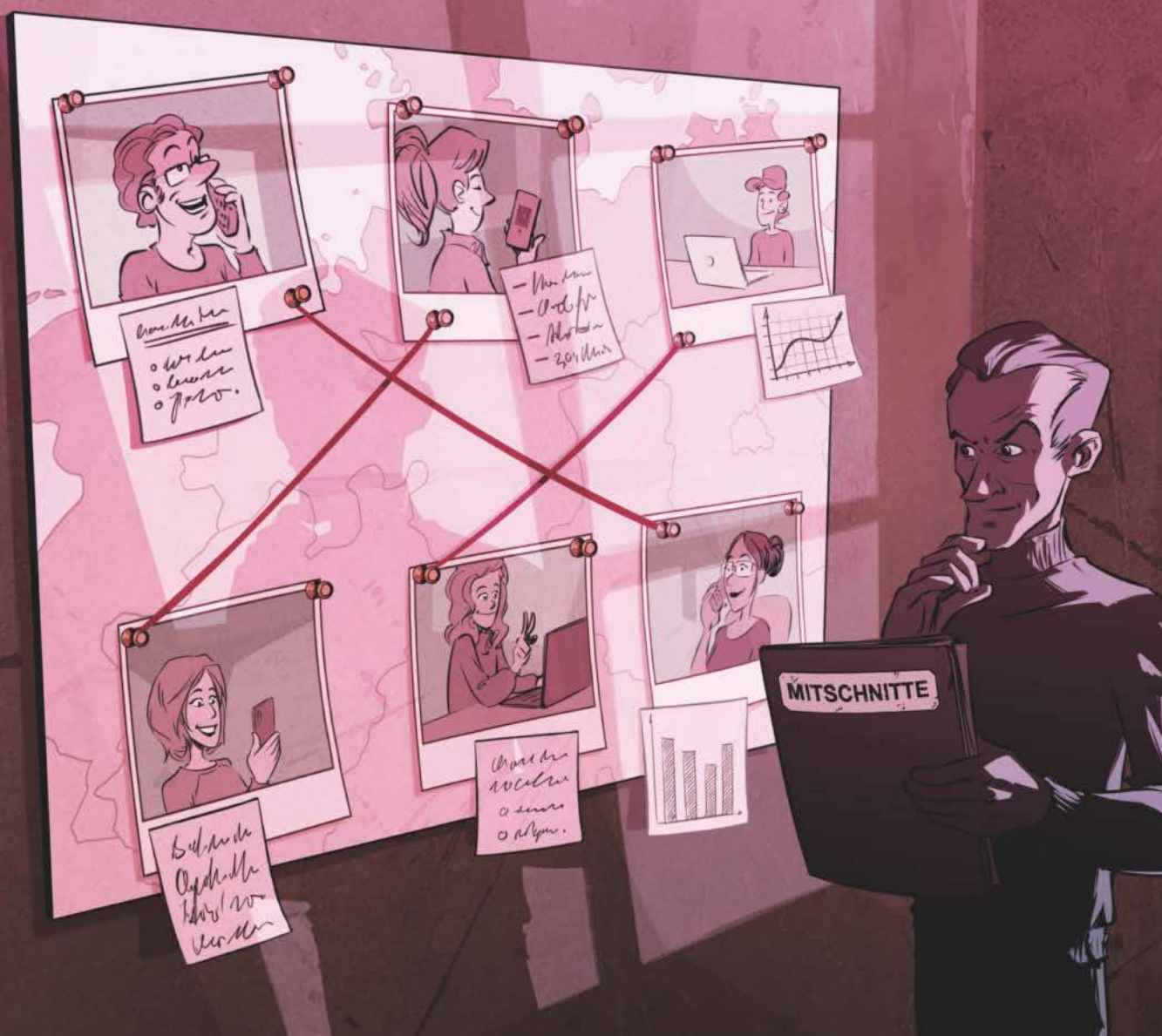


Nichts zu verbergen?

Sicher und vertraulich kommunizieren:
Ein Grundrecht



Ein Grundrecht: Vertraulich kommunizieren	Seite 50
E-Mails: Ein altes Medium bestmöglich absichern	Seite 54
Verschlüsselnde Messenger: Wo liegen die Unterschiede?	Seite 56
Abhörsicher telefonieren: Von Festnetz bis Videotelefonie	Seite 58
Folgenlos, selbstheilend, abstreitbar – wie moderne Kryptografie funktioniert	Seite 60

Zum Recht auf informationelle Selbstbestimmung gehört auch vertrauliche Kommunikation. Angriffe auf dieses Grundrecht gibt es traditionell nicht nur von Kriminellen, sondern auch von Staaten – einschließlich solchen, die sich gern als freiheitlich-demokratisch einordnen. Jeder Einzelne kann viel tun, um vertraulich zu mailen, zu chatten und zu telefonieren. Oft ganz ohne Komfortverlust.

Von Jan Mahn

Deutschland ist ein freies Land – zu dieser Erkenntnis kommen seit Jahren auch die Politikwissenschaftler der unabhängigen Forschungsorganisation Freedom House. Sie machen sich alljährlich die Mühe, die Freiheit aller Staaten der Welt zu erforschen. Für jedes Land schreiben sie einen Bericht und vergeben Punkte in 25 Kategorien (siehe ct.de/ypbr). Darin geht es um Wahlen, Presse- und Demonstrationsfreiheit und auch um die Freiheit im Internet. Mit 94 von 100 möglichen Punkten schneidet Deutschland vergleichsweise gut ab, Österreich kommt auf 93 Punkte, die Schweiz auf 96.

In Kategorie D4 geht es in den Länderberichten um die Freiheit, keine Überwachung fürchten zu müssen. Diese Freiheit ist in Deutschland gesetzlich verankert: Das Grundgesetz kennt das Post- und Fernmeldegeheimnis, die Europäische Menschenrechtskonvention nennt in Artikel 8 das Recht auf Achtung des Privatlebens und den Schutz der Korrespondenz. Es ist also ein Grundrecht, vertraulich mit anderen kommunizieren zu können – auch dann, wenn sich die Gesprächspartner nicht gegenüber sitzen und ein elektronisches Medium die Übertragung übernimmt.

Vertrauliche Kommunikation ist nicht nur für die wenigen Berufsgruppen wichtig, die immer wieder genannt werden, wenn es um verschlüsselte Kommunikation geht: Journalisten, Whistleblower und Dissidenten in unfreien Staaten müssen natürlich besonders auf Vertraulichkeit achten, jeder andere sollte von seinem

Grundrecht aber ebenfalls großzügig Gebrauch machen.

Denn auch als Normalbürger hat man eine Menge zu verlieren, wenn man sich auf die Vertraulichkeit des Geschriebenen nicht verlassen kann. Wer meint, er habe nichts zu verbergen, sollte am besten von einem Messenger direkt auf Twitter wechseln und die nächste Kneipentour nach der Pandemie mit Freunden in aller Öffentlichkeit planen und im Anschluss auch dort nachbesprechen. Spätestens, wenn man mit Kollegen oder Kunden über dienstliche Inhalte kommuniziert, ist Vertraulichkeit oft entscheidend. Wer mit Kundendaten fahrlässig umgeht, muss die DSGVO fürchten, wer Firmengeheimnisse ungeschützt übermittelt, muss Angst vor Industriespionen haben.

Mühsame Angriffe

Die Gefahr, von staatlichen Stellen abgehört zu werden, wirkt in Europa nicht so groß. Doch auch Deutschland bekommt in dieser Kategorie von den Freedom-House-Forschern Punktabzüge unter anderem für die Quellen-Telekommunikationsüberwachung (TKÜ). Im Visier sind dabei vor allem die Messaging-Dienste. Strafverfolgungsbehörden dürfen auf richterliche Anordnung einen Trojaner auf dem Mobiltelefon einer verdächtigen Person installieren, der zum Beispiel Screenshots der Nachrichten aufzeichnet und diese an die Strafverfolger verschickt. Das Verfahren ist aber mühsam, meist muss ein Ermittler meh-

rere Minuten Zugriff auf das Telefon des Verdächtigen haben.

Die beschwerliche Quellen-TKÜ ist für die Strafverfolger auch nur eine Notlösung – das Problem für alle, die vertrauliche Kommunikation mitlesen wollen, ist

die Ende-zu-Ende-Verschlüsselung. Sie stellt sicher, dass nur die Gesprächspartner einen Schlüssel besitzen, um die Nachrichten lesen zu können. Alle anderen auf dem Weg, also der Betreiber des WLANs, die Internetanbieter, Knotenpunkte, abzapfende Geheimdienste, aber auch

zum Beispiel die Betreiber der Messenger selbst, sehen nur verschlüsselten Datensalat. Ende-zu-Ende-Verschlüsselung schützt die Kommunizierenden nicht nur vor individueller Überwachung. Vor allem schützt sie zuverlässig vor der Massenüberwachung ganzer Gesellschaften. Eine solche haben unter anderem die Geheimdienste der USA und Großbritanniens weltweit eingerichtet, indem sie an Internetknotenpunkten große Teile des Internetverkehrs ausleiten und auswerten. Gegen Ende-zu-Ende-verschlüsselte Nachrichten kommen aber auch BND, GCHQ und NSA nicht an.

Das liegt schlicht daran, dass Ende-zu-Ende-Verschlüsselung durch die einzigen Gesetze geschützt wird, die Geheimdienste nicht beugen und Politiker nicht durch Verordnungen aushöhlen können: durch die Gesetze der Mathematik. Die stellen sicher, dass es beim Knacken der Verschlüsselung aktuell keine Abkürzungen gibt und man auch mit viel teurer Hardware nicht effizient entschlüsseln

Es ist also ein Grundrecht, vertraulich mit anderen kommunizieren zu können.

kann, wenn man den Schlüssel nicht kennt. Warum Ende-zu-Ende-verschlüsselte Übertragung kryptografisch sicher ist und was es mit Selbstheilung und Abstreitbarkeit auf sich hat, erfahren Sie auf Seite 60. Wie verschiedene Messenger-Anbieter die Ende-zu-Ende-Verschlüsselung umsetzen und welche Auswirkungen das auf den Komfort hat, lesen Sie ab Seite 56.

Schwere Geschütze

Mit diesem für Überwacher unbefriedigenden Zustand wollen sich auch in Deutschland einige Politiker aber nicht abfinden – allen voran das CSU-geführte Innenministerium. Zusammen mit den europäischen Amtskollegen haben sie eine Resolution auf den Weg gebracht, in der sie Zugriffe für Strafverfolger und zuständige Stellen auf verschlüsselte Kommunikation fordern. Ausführlich berichtet haben wir darüber Mitte Dezember 2020 [1]. Wie die Zugriffe auf die Nachrichten technisch aussehen sollen, ist mehr als unklar. Funktionieren kann das nur, indem man Lücken in die Software einbauen lässt, die Ende-zu-Ende-Verschlüsselung stellenweise deaktiviert, die Kommunikationspartner aber nicht darüber informiert. Ein mathematischer oder informationstechnischer Weg, Verschlüsselung nur ein bisschen zu brechen, existiert nicht. Problematisch sind solche Zugriffe unter anderem rechtlich: In Deutschland muss man keine Strafverfolgung fürchten, wenn man den ungarischen Ministerpräsidenten Viktor Orbán als Diktator und Faschisten bezeichnet, in Ungarn sieht das möglicherweise anders aus. Gäbe es nun eine richterliche Anordnung aus Ungarn an einen Messenger-Betreiber, die Inhalte einer Unterhaltung von zwei Deutschen offenzulegen und die Verschlüsselung zu umgehen – wer sollte entscheiden, welches Recht jetzt schwerer wiegt? Was, wenn die Unterhaltung von einem Deutschen und einem Ungarn geführt wurde?

Davon lassen sich Seehofer und seine Kollegen aber nicht abhalten und sprechen von einem Dialog mit den Anbietern, der nötig sei, um technische Lösungen zu finden. Sollten sie mit ihren Grundrechtseinschnitten im EU-Parlament und später in

den nationalen Parlamenten durchkommen, müssten die Messenger-Anbieter dem auch Folge leisten. Tun sie das nicht, droht ihnen der Rauswurf aus den Stores von Apple und Google. Das trifft allerdings vor allem die Mehrheit der Bürger, deren Grundrecht beschnitten wird. Kriminelle würden dann auf andere Kanäle ausweichen. Mit solchen Hintertüren wäre

außerdem nicht nur die gezielte Überwachung von Verdächtigen auf richterliche Anordnung möglich. Auch Massenüberwachung, wie sie Europa in den USA immer scharf kritisiert hat, wäre dann technisch kein Problem mehr. Die Geschichte der Hintertüren und Zweitschlüssel zeigt leider: Noch nie ist ein solches Instrument langfristig nur einem

kleinen Kreis zugänglich geblieben. Zu den größten Fehlgriffen zählten die Hintertüren, die Netzwerkausrüster Juniper in seine Geräte auf Veranlassung der NSA einbauen musste. Genutzt wurden sie schnell auch vom chinesischen Geheimdienst.

Im Freedom-House-Index dürften solche gesetzlich vorgeschriebenen Hintertüren zu massivem Punktabzug führen, Deutschland und die EU, einst Vorreiter bei der Freiheit, würden ins Mittelfeld abrutschen. Gleichzeitig schwächt man damit auch Argumente für die eigene Weltsicht: Unternehmen werden von der DSGVO aktuell dazu gebracht, personenbezogene Daten nur in Europa zu verarbeiten und nicht in den USA – dort erlaubt es der Cloud Act den Geheimdiensten, auf die Daten in den Rechenzentren zuzugreifen. An diesem Streitpunkt scheiterte zuletzt das Datenschutzabkommen Privacy Shield und Europa konnte immer aus der Position moralischer Überlegenheit argumentieren. Mit eigenen Hintertürgesetzen wäre damit Schluss.

Andere Wege

Möchte man auch dann noch abhörsicher kommunizieren, wenn die Innen- und Sicherheitspolitiker mit ihrer Grundrechtseinschränkung erfolgreich waren, kann man auf dezentrale Kommunikationssysteme umsteigen. Bei der populärsten dezentralen Kommunikationslö-

sung gibt es keinen Anbieter, den man per Gesetz zu Hintertüren zwingen kann: Die gute alte E-Mail wird seit Jahrzehnten aber meist unverschlüsselt verschickt. Das liegt daran, dass Ende-zu-Ende-Verschlüsselung nicht Teil der Protokolle ist, nicht jeder Mailclient mitspielt und die Einrichtung durchaus mit Komfortverlusten verbunden ist. Auf Seite 54 erfahren Sie, was trotzdem möglich ist und wie Sie vertrauliche E-Mails versenden.

Vertraulichkeit ist nicht nur beim geschriebenen Wort oft wünschenswert. Telefonate sind schon seit vielen Jahrzehnten im Fokus von Mithörern. Was Sie tun können, um möglichst große Teile der Verbindung zwischen Ihrem Telefonhörer und dem Hörer Ihres Gesprächspartners zu verschlüsseln, und ob es wahre Ende-zu-Ende-Verschlüsselung bei Telefonaten überhaupt gibt, erfahren Sie ab Seite 58.

Datenbeiwerk

Nicht nur die Inhalte der Nachrichten sind für alle Arten von Mithörern interessant. Strafverfolger, Geheimdienste, aber auch die Werbewirtschaft interessieren sich brennend dafür, wer mit wem zu welcher Uhrzeit und von welchem Gerät kommuniziert. Mit solchen Metadaten kann man, sofern man genug davon hat, eine Menge über Personen, Netzwerke und Beziehungen erfahren. Scrollen Sie einfach mal durch Ihre letzten Chatverläufe, achten nur auf die Uhrzeiten und überlegen Sie, welche Schlüsse man allein daraus über Sie und Ihre Gesprächspartner ziehen könnte, wenn man diese Informationen systematisch auswertet. Wenn man dann noch einbezieht, wer mit wem in welcher Gruppe ist, wird das Bild komplett.

In den folgenden Artikeln geht es daher nicht nur um die reine Verschlüsselung der Inhalte, sondern auch um den Schutz und die Vermeidung von Metadaten. Das Recht auf private Korrespondenz beschränkt sich schließlich nicht nur auf die reinen Gesprächsinhalte.

(jam@ct.de) **ct**

Literatur

- [1] Jan Mahn, Niemand hat die Absicht ..., Innenminister wollen Verschlüsselung umgehen, c't 26/2020, S. 16

Länderberichte von Freedom House:
[ct.de/ypbr](https://www.freedomhouse.org/de/ct.de/ypbr)

TECHNIKUNTERRICHT MACHT ENDLICH SPAß!



Spannende
Unterrichts-
materialien
GRATIS

Make: *Education*

Mit **Make Education** erhalten Sie jeden Monat kostenlose Bauberichte und Schritt-für-Schritt-Anleitungen für einen praxisorientierten Unterricht:



Für alle weiterführenden
Schulen



Digital zum Downloaden



Fächerübergreifend



Monatlicher Newsletter

Jetzt kostenlos downloaden: make-magazin.de/education

E2EE-Mail

E-Mails bestmöglich absichern

„E-Mails sind nicht sicher“, hat vermutlich jeder schon mal gehört. Benutzt werden sie trotzdem und ganz so schlimm ist die Situation auch nicht: Die wichtigsten Sicherungen lassen sich nachrüsten.

Von Sylvester Tremmel

Als E-Mails aufkamen, galt es, Computernetzwerke gegen atomare Erstschläge zu sichern. Seither hat sich einiges geändert – die Gefahren sind eher Malware und Industriespionage, womit das Medium leider kaum Schritt hielt: Mails sind standardmäßig weder verschlüsselt noch authentifiziert – von fortschrittlicheren kryptografischen Eigenschaften ganz zu schweigen.

Unterwegs verschlüsselt

Relativ weit gekommen sind E-Mails bei der Transportverschlüsselung. Heutzutage ist es üblich, seine Mails nur transportverschlüsselt abzuholen, egal ob per IMAP oder POP3. Das geschieht, indem der Mail-Client eine verschlüsselte Verbindung aufbaut (TLS) oder eine normal aufgebaute Verbindung nachträglich verschlüsselt (STARTTLS). Beides beherrschen praktisch alle Clients und Mailserver, Sie müssen nur sicherstellen, dass Ihr Mailprogramm in den Servereinstellungen TLS oder STARTTLS nutzt. Auf diese Weise verhindern Sie zumindest, dass WLAN-Betreiber oder andere Gäste im öffentlichen Hotspot mitlesen.

Schwieriger wird es schon beim Versand von E-Mails. Hier sind zwar ebenfalls TLS und STARTTLS verbreitet, aber die so initiierte Transportverschlüsselung reicht naturgemäß nur bis zum eigenen Mailprovider. Von dort muss die E-Mail weiter zum Provider des Adressaten und diese Übertragung geschieht unter Umständen unverschlüsselt, je nachdem ob

die beteiligten Mailserver angeben, Verschlüsselung zu unterstützen. Zwischengeschaltete Angreifer (Man-in-the-Middle, MITM) können diese Angaben sogar manipulieren und so eine unverschlüsselte Verbindung erzwingen, auch wenn eigentlich TLS verfügbar wäre.

Als Endnutzer können Sie dagegen nicht viel ausrichten. Es gibt Ansätze, solche Attacken zu verhindern (zum Beispiel via DANE oder den Standard MTA-STS), aber sie werden noch nicht universell unterstützt. Letztlich hängt es von den beteiligten Mail-Providern ab, ob Transportverschlüsselung zum Einsatz kommt. Initiativen wie „E-Mail made in Germany“ garantieren Verschlüsselung zumindest bei Übertragungen zwischen ihren Mitgliedern. Es gibt auch Mailserver, etwa die des Landes Niedersachsen, die Mails nur annehmen, wenn sie transportverschlüsselt eingeht. Manche Mail-Provider – zum Beispiel mailbox.org oder posteo.de – bieten auch die Option, E-Mails gar nicht erst zu versenden, wenn sie keine Transportverschlüsselung aufbauen können. Die Option finden Sie – falls Ihr Provider sie anbietet – in dessen Webmail- oder Account-Verwaltung.

Aber auch mit durchgehender Transportverschlüsselung werden E-Mails nicht zum absolut sicheren Medium. Zum einen können immer noch alle beteiligten Mail-Provider mitlesen. Die Verschlüsselung besteht nur zwischen ihnen, um Lauschern auf der Leitung einen Strich durch die Rechnung zu machen. Die Provider-Systeme sehen die E-Mails im Klartext. Wenn es um unternehmensinterne Mails geht und der firmeneigene Mailserver der einzige beteiligte „Provider“ ist, dann mag dieser Zustand akzeptabel sein.



Bild: Albert Hulm

Erstrebenswert ist er jedenfalls nicht. Vielleicht verlassen die Mails ja doch irgendwann den Firmenserver – zum Beispiel wenn das Unternehmen sich für ein Cloud-Backup entscheidet.

Zum anderen gibt es auch bei transportverschlüsselten Mails keinerlei Authentifizierung: Eine Mail von `chef@example.com` muss keineswegs wirklich vom Account „chef“ und den Servern in der Domain `example.com` stammen – ein Grund, warum E-Mail-Spam so alltäglich ist. Mit SPF, DKIM und DMARC gibt es wieder verschiedene Ansätze, die die Situation verbessern. Sie setzen sich aber (wie DANE und MTA-STS) nur langsam durch und sind nichts, was Sie als Endnutzer in der Hand haben [1].

Immer verschlüsselt

Sie können die Probleme allerdings angehen, indem Sie Ende-zu-Ende-Verschlüsselung nutzen (End-to-end encryption, E2EE). Dann kann niemand auf dem Weg mehr mitlesen, auch nicht die Mail-Provider. Gängige E2EE-Methoden erlauben außerdem, Nachrichten zu authentifizieren, indem der Versender sie digital signiert. Zwei Varianten von E2EE sind im E-Mail-Universum verbreitet: S/MIME und OpenPGP. „Verbreitet“ ist allerdings relativ zu verstehen – die allermeisten E-Mails nutzen keine Ende-zu-Ende-Verschlüsselung.

Wie E-Mail selbst sind auch S/MIME und (Open-)PGP recht betagt und haben mit Alterserscheinungen zu kämpfen. Manche Designentscheidung würde man heutzutage anders treffen und fortschrittlichere Eigenschaften wie perfect forward secrecy oder post-compromise security

(siehe Seite 60) lassen sich damit kaum realisieren. Das sollte Sie aber nicht davon abhalten, S/MIME oder OpenPGP zu nutzen. Besser als Mails ohne E2EE sind die Systeme allemal.

S/MIME ist vor allem im Firmenumfeld verbreitet. Um es zu nutzen braucht man ein kostenpflichtiges Zertifikat. Dafür unterstützen die meisten E-Mail-Clients S/MIME out-of-the-box. Wie Sie S/MIME einrichten und wo es Zertifikate zu annehmbaren Preisen gibt, haben wir in c't 14/2020 beschrieben [2]. Kostenlos und gerade im privaten Umfeld verbreiteter ist PGP. Auch das haben einige Clients eingebaut, für diverse andere (inklusive Outlook) gibt es Plug-ins. Mit Mailvelope existiert sogar ein Browser-Add-on, das OpenPGP für Webmailer nachrüstet und von verbreiteten Mail Providern wie GMX oder Web.de unterstützt wird.

Einfach ist was anderes

OpenPGP wird – leider aus guten Gründen – nachgesagt, dass es kompliziert und lästig in der Handhabung sei. Die verschiedenen Implementierungen versuchen auf unterschiedliche Weise, diese Komplexität zu verbergen oder zugänglich zu machen.

Vergleichsweise einfach ist es beim Mail-Client Thunderbird, der seit Version 78 OpenPGP eingebaut hat. Langjährige Nutzer des zuvor verfügbaren Plug-ins Enigmail üben an der Neuimplementierung durchaus Kritik, aber gerade für PGP-Neulinge bietet sich der Mailer an: Man bekommt alles Nötige aus einer Hand, kann nicht allzu viel falsch machen und im Fall von Problemen ist die Community groß. Eine Einführung in Thunderbirds PGP-Funktionen, finden Sie in c't 19/2020 [3].

Man muss auch nicht vollständig auf Thunderbird umsatteln, nur weil man gelegentlich Mails verschlüsseln will (und mit der PGP-Unterstützung des eigenen Clients nicht zurande kommt). E-Mail basiert auf offenen Standards und nichts spricht dagegen, zwei oder mehr Clients parallel zu nutzen – zumindest für IMAP-Nutzer. Auch proprietäre Systeme wie Microsofts Exchange bieten IMAP- und SMTP-Schnittstellen, über die Thunderbird parallel genutzt werden kann.

Schlüsselverwaltung

Einige Probleme von OpenPGP kann aber kein Client übertünchen, etwa das der Schlüsselverwaltung. Ihren privaten PGP-Schlüssel müssen Sie hüten wie Ihren Augapfel: Gerät er in die falschen Hände, kann jeder in Ihrem Namen E-Mails signieren und aktuelle sowie in der Vergangenheit aufgezeichnete Kommunikation entschlüsseln. Schützen Sie den Schlüssel daher mit einem Passwort (Thunderbird macht das über das Master-Passwort) und lassen Sie nicht jedermann an Ihren Mail-Client.

Auch vor Verlust müssen Sie den privaten Schlüssel schützen, um alte Nachrichten für immer lesen zu können. Wichtig ist das auch bei Nachrichten, die archiviert werden sollen. Am besten exportieren Sie den privaten Schlüssel in ein sicheres Backup.

Ihren öffentlichen PGP-Schlüssel müssen Sie dagegen publizieren, damit Gesprächspartner mit Ihnen verschlüsselt Kontakt aufnehmen können. Idealerweise kann auch niemand gefälschte Schlüssel in Ihrem Namen publizieren und so Korrespondenten in die Irre führen. Das von OpenPGP dafür vorgesehene Konzept namens Web-of-Trust hat aber eklatante Mängel. Eine verbreitete

Notlösung ist der Server keys.openpgp.org. Für dort publizierte Schlüssel wird allerdings nur sichergestellt, dass die E-Mail-Adresse stimmt. Manche Clients – inklusive Thunderbird – können direkt bei keys.openpgp.org suchen, wenn kein passender Schlüssel lokal vorhanden ist.

Es gibt Projekte wie Pretty Easy Privacy (pEp), Autocrypt oder Web Key Directories (WKD), die OpenPGP-Verschlüsselung und insbesondere die problematische Schlüsselverwaltung weiter vereinfachen wollen. Zumindest aktuell ist ihre Unterstützung bei Clients aber so eingeschränkt, dass sie sich nicht allgemein nutzen lassen. Thunderbird unterstützt immerhin WKD und Teile der Autocrypt-Spezifikation.

Metadaten

Ein weiteres Problem von E-Mails können auch die E2EE-Lösungen nicht beheben: Es fallen massenweise Metadaten an. Absurderweise ist sogar der Betreff einer E-Mail technisch gesehen ein Metadatum und wird deswegen üblicherweise nicht verschlüsselt. Das zumindest ändert sich langsam, Mailer wie Thunderbird verschlüsseln auch den Betreff. Dadurch zeigen allerdings Clients, die zwar OpenPGP kennen, aber nicht diese Betreffverschlüsselung, immer „...“ als Betreff an.

Echte Metadaten wie Adressaten und Sende- oder Empfangszeitpunkte lassen sich bei E-Mails grundsätzlich nicht verschlüsseln, sie werden zur Zustellung benötigt beziehungsweise fallen dabei an. Um das zu ändern, müsste man ein neues Protokoll einführen, mit dem normale E-Mail-Clients und -Server nicht kompatibel wären. Wer wann mit wem redet, wissen also auch mit E2EE alle beteiligten Mailserver (bei durchgängiger Transportverschlüsselung immerhin nur die). Nicht alles lässt sich nachträglich in ein 50 Jahre altes Protokoll einbauen. Wer mehr will – oder sich einfach nur möglichst wenig mit Verschlüsselung beschäftigen möchte –, sollte seine Kommunikation auf Messenger umstellen (siehe nächste Seite). (syt@ct.de) ct

Literatur

- [1] Leo Dessani und Jan Mahn, DKIM-Fail, Fehler bei Hostern gefährden die Sicherheit von DKIM, c't 01/2021, S. 126
- [2] Holger Bleich, Einfach vertraulich, Unkomplizierte Verschlüsselung und Signierung von E-Mails mit S/MIME, c't 14/2020, S. 140
- [3] Sylvester Tremmel, Eingebaute Verschlüsselung, OpenPGP-Unterstützung in Thunderbird 78, c't 19/2020, S. 154



Verschlüsselt und signiert, alles grün. Leider beherrscht das abgebildete Evolution keine Betreffverschlüsselung und zeigt nur drei Punkte an.

Spurlos verschlüsselt

Instant Messages ohne Datenlecks

Über Chats können Sie bequem mit fast jedem Partner plauschen. Aber dass Sie das tun, und was Sie sich da erzählen, bleibt nicht immer privat. Entscheidend dafür ist die Wahl des Werkzeugs.



Bild: Albert Hujm

Von Hans-Peter Schüler

Mit WhatsApp erreichen Absprachen zur geplanten Fahrradtour und spontane Fotos der Protestdemo vor dem Rathaus auf Anhieb fast jeden gewünschten Adressaten [1]. Das ist höchst bequem, und die Ende-zu-Ende-Verschlüsselung bei diesem Messenger könnte man als Garantie für den perfekten Datenschutz ansehen – doch das ist zu kurz gedacht.

Beim Gedankenaustausch über Instant Messages sind nämlich dreierlei Risiken zu beachten. Nur eines davon, dass jemand heimlich mitliest, lässt sich mit der Ende-zu-Ende-Verschlüsselung eindämmen.

Was Sie Ihren Partnern mitteilen, ist nur dann zuverlässig geschützt, wenn es

noch vor der Übergabe ins Internet auf Ihrem Gerät verschlüsselt und erst nach dem Verlassen des Internets auf den Geräten Ihrer Partner entschlüsselt wird. Beim viel gerühmten Dienst Telegram etwa gilt dieses Prinzip nur für wählbare Geheimchats mit eingeschränkten Möglichkeiten. Bei Microsoft Teams, das alle Nachrichten auf dem Server entschlüsselt und erst zur Zustellung wieder verschlüsselt, ist der Datenschutz immer eine Mogelpackung.

Schutz von Inhalten

Bei WhatsApp und insbesondere den quelloffenen Konkurrenten Signal und Threema sind die Inhalte als sicher zu betrachten. Einzelheiten dazu erläutert der Beitrag auf Seite 60, in dem wir auch darauf eingehen, dass selbst ein durchgesickter Kryptoschlüssel nicht unbedingt

die Entschlüsselung früherer Nachrichten ermöglicht.

Offenes Buch: Metadaten

Der zweite Gesichtspunkt sind Informationen darüber, wann wer mit wem gepocht hat. Das mag Ihnen bei der Fahrradtour egal sein. Dagegen taugen am Ort und Zeitpunkt der Rathaus-Demo geteilte Fotos durchaus als Anhaltspunkt, um deren Empfänger zu recht oder zu unrecht als Sympathisant einer politischen Gruppierung abzustempeln. Sie sollten deshalb auch darauf achten, wie gut Ihre Kontaktdaten und die Ihrer Gesprächspartner geschützt sind.

WhatsApp möchte schon zur Installation Lesezugriff auf Ihr komplettes Adressbuch, und wenn Sie den nicht ausdrücklich verweigern, landen die Daten postwendend beim Anbieter Facebook. Vorgeblich dient

Datenschutz bei Messengerdiensten

Messenger	Signal	Telegram	Threema	WhatsApp	Slack	Stackfield	Teams
Anbieter	Signal Foundation	Telegram LLC	Threema GmbH	Facebook	Salesforce	Stackfield	Microsoft
Serverstandort	USA	veränderlich	CH	USA	USA	D	USA, EU
Plattformen	Android, iOS, Windows, macOS, Linux	Android, iOS,	Android, iOS, Browser	Android, iOS, Windows	Windows, macOS, Linux (Beta), Android, iOS	Windows, macOS, Android, iOS	Windows, macOS, Linux, Browser, Android, iOS
auf mehreren Geräten nutzbar	✓ ⁵	✓	✓ ²	✓ ⁶	✓	✓	✓
Client/Server quelloffen	✓ / ✓	✓ / –	✓ / –	– / –	– / –	– / –	– / –
Nutzung							
Funktionen ¹	Zensieren von Gesichtern in Bildern	Add-ons, Bots, Bezahldienst ²	Umfragen in Chatgruppen	Bezahldienst	Bildschirmfreigabe, programmierbare Abläufe, cloudgestützte Filterfunktionen, API für externe Dienste	Aufgabenverwaltung	Bildschirmfreigabe, Add-ons
E2E-Verschlüsselung	✓	nur in Sonderfällen	✓	✓	✓ ⁴	✓	–
Kontaktdaten in der Cloud	Nutzer-IDs + Telefonnummern, weitgehend verschlüsselt	Nutzer-IDs + Telefonnummern, unverschlüsselt	nur anonyme Threema-IDs	komplette Nutzer-Adressbücher inkl. Telefonnummern, unverschlüsselt	Nutzer-IDs, unverschlüsselt ⁷	Nutzer-IDs, unverschlüsselt ⁷	Nutzer-IDs, unverschlüsselt ⁷
Schutzfunktionen	PIN oder QR-Code	optischer Code	2FA	2FA	2FA	2FA	MFA über Active Directory

¹ alle Dienste bieten Einzel- und Gruppenchats, Audio- und Videoanrufe und -konferenzen sowie Dateiaustausch ² angekündigt ³ Dateiablage per Webbrowser ⁴ nur über EKM (externe Schlüsselverwaltung)
⁵ 1 Mobil- + max. 5 Desktop-Clients ⁶ max. 4 Clients (Beta) + Fernsteuerung unter Windows und macOS ⁷ vertraglich regelbar ⁸ ja ⁹ – nein

das dazu, die WhatsApp-Nutzer unter Ihren Bekannten für Sie ausfindig zu machen, aber Facebook hat ein profundes Interesse am Besitz dieser Informationen: Sein ganzes Geschäftsmodell beruht darauf, das weltweite soziale Netz mit allen erdenklichen Informationen als perfekte Werbepattform zu vermarkten und Sie als Adressaten für gezielte Werbung zu charakterisieren.

Man kann WhatsApp zwar auch verwenden, ohne das Adressbuch freizugeben, aber dann kann man nur mit Kunstgriffen Partner anschatten, von denen man noch nie eine WhatsApp-Message erhalten hat [2]. Für dieses Setup lässt man sich zum Beispiel von einem Radtour-Partner eine Nachricht schicken und sich in die Radtour-Absprachegruppe eintragen. Danach kann man sich ohne weltweites Outing an diesen Absprachen beteiligen.

Trau, schau, wem

Der dritte Knackpunkt betrifft die Identität Ihrer Gesprächspartner. Ein guter Messenger macht es nicht nur schwer, sich im Chat als jemand anderes auszugeben, sondern gibt Teilnehmern auch die Gelegenheit, die Authentizität eines Gesprächspartners zu prüfen. Dieser Schutz ist wichtiger, als man auf Anhieb erkennt: Eine E-Mail, die Sie nach der PIN Ihrer EC-Karte fragt, wird vermutlich sofort Ihren gesunden Menschenverstand alarmieren. Dagegen ist die Situation beim Messenger-Dienst nicht ganz so offensichtlich. Die Nachricht, in der sich angeblich ein guter Freund nach Ihrem WhatsApp-Verifizierungscode erkundigt, lässt sich nach dem Erhalt kaum auf ihre Herkunft prüfen, und scheinbar dient sie nur einer legitimen Sicherheitskontrolle. Doch wenn sich dadurch ein Gauner unter falschem Namen den gewünschten Code erschleicht, kann er damit Ihr WhatsApp-Konto übernehmen, Sie davon aussperren und fortan unter Ihrem Namen auftreten.

Immerhin bemühen sich alle gängigen Messenger, die Zugänge ihrer Nutzer gegen Missbrauch abzusichern. Bei Signal und Telegram können Sie zum Beispiel im Chat einen grafischen Code vom Partner anfordern und mit einer Referenz vergleichen. Für den Fall, dass Sie Ihr Mobilgerät verlieren, lässt sich Missbrauch vorsorglich ausschließen, indem Sie Logins an eine 2FA oder MFA (Zwei-Faktor- oder Multi-Faktor-Authentifizierung) binden.

Sprenu und Weizen

Dienste aus der Mobilfunkszene wie WhatsApp, Telegram, Signal oder Three-

ma unterscheiden sich nur oberflächlich von anderen wie Teams, Slack oder Stackfield, die zuerst als Desktop-Browseranwendungen bekannt geworden sind. Auch wenn sich die Anmeldeprozesse unterscheiden, verschmelzen beide Kategorien miteinander und sind nach denselben Kriterien zu bewerten.

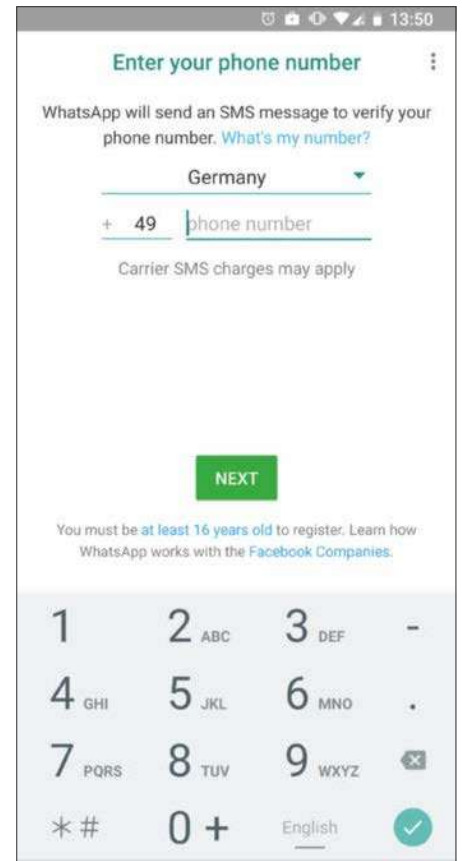
Für WhatsApp, Telegram & Co. registriert man sich mit seiner Telefonnummer per Smartphone, und aus dessen Geräteerkennung wird das Benutzerkonto des Dienstes abgeleitet. Wechseln Sie das Handy, womöglich auch ohne Vertragswechsel beim Handy-Provider, müssen Sie den Messaging-Dienst auf das neue Gerät ummelden. Die Einzelheiten variieren von Plattform zu Plattform und von Messenger zu Messenger. Den Prozess starten Sie zum Beispiel aus der auf dem neuen Gerät installierten App heraus und erhalten daraufhin auf dem alten Gerät einen Bestätigungscode, den Sie am neuen Gerät eingeben müssen. Threema ist eine Ausnahme: Es funktioniert ohne personenbeziehbares Benutzerkonto über eine zufällig generierte ID, ohne dass man jemals Rückschlüsse auf seine Person ermöglichen müsste.

Besitzen Sie kein Smartphone oder möchten Ihr privates Smartphone nicht für einen beruflich genutzten Dienst registrieren, sind Sie mit diesen Messengern (abgesehen von Threema) schlecht bedient. In diesem Fall fahren Sie besser mit Diensten wie Teams, Stackfield oder Slack, bei denen Sie sich per Webseite und Passwort registrieren und die Anmeldung in Reaktion auf eine SMS oder E-Mail vom Provider bestätigen.

Unabhängig von Geräte-IDs können Sie alle gängigen Mobil-Messenger schon jetzt oder in Kürze parallel auf mehreren Geräten nutzen – Details finden Sie in der Tabelle. Telegram bietet zusätzlich die Option, die App mit bis zu drei Konten vom selben Gerät aus zu verwenden.


Jenseits des Tellerrands

Messenger wie Rocket.Chat nach dem Jabber-Nachfolgestandard XMPP oder das dezentralisierte Kommunikationssystem Matrix ermöglichen noch weiter reichende Sicherheitsmerkmale: Für diese Dienste können Sie mit quelloffener Software einen eigenen Server einrichten und autark betreiben. Der Ansatz geht allerdings zulasten der Reichweite: Auch wenn sie einen Standard wie XMPP umsetzen, enthalten die meisten dieser Dienste indivi-



Viele Messenger nutzen die bestehende Telefonnummer als Geräteerkennung und prüfen bei der Installation, dass man die korrekte Nummer eingibt.

duelle Erweiterungen und kooperieren nur unvollständig miteinander.

Wenn Sie mit Dissidenten unter einem totalitären Regime chatten möchten, können Sie den Datenschutz mit dem Briar Project auf die Spitze treiben. Das baut auf Ende-zu-Ende-verschlüsselte Verbindungen über das Tor-Netzwerk oder funktioniert sogar ganz ohne durchgehende Internetverbindung, etwa über Zwischenschritte mit geschmuggelten USB-Sticks. Damit lassen sich nur Text-Nachrichten austauschen und die Partner müssen sich auch über einen anderen Kanal auf einen Gesprächstermin einigen, weil nichts gespeichert wird. Dafür stellen sie einen Angreifer aber selbst dann vor Probleme, wenn er auch nur die Gesprächsteilnehmer ausmachen will. (hps@ct.de) 

Literatur

- [1] Peter Schüler, Keywan Tonekaboni, Harter Wettbewerb, Sieben Messenger gegen WhatsApp, c't 11/2019, S. 72
- [2] WhatsApp-Kontakt per Telefonnummer: heise.de/s/kZpQ

Sichere Leitung

Verschlüsselt telefonieren und konferieren

Der Ausbruch von Corona war der Durchbruch für viele Kommunikations-Apps: Sie sind als Ersatz für persönliche Treffen mit Familie, Freunden und Kollegen eingesprungen. Doch Anrufe und Videotelefonate lassen sich in vielen Fällen leicht abhören. Mit der richtigen App haben Lauscher jedoch keine Chance.

Von Ronald Eikenberg

Wenn man Familie, Freunde und Kollegen nicht persönlich treffen kann, dann bleibt man zumindest per Ton und Bild in Kontakt – der modernen Technik sei Dank. Doch diese Kommunikationswege bergen Tücken, denn anders als beim Vieraugengespräch vor Ort ist die Vertraulichkeit oft nicht gegeben. Schlimmstenfalls kann jeder die Gespräche belauschen, der den Datenverkehr abzwacken kann.

Doch auch modernere Kommunikationsmittel wie Microsoft Teams oder Telegram sind nicht automatisch sicher. Dabei kommt zwar eine Transportverschlüsselung zum Einsatz, diese sorgt aber nur dafür, dass die Gespräche jeweils zwischen Gesprächsteilnehmer und Anbieter verschlüsselt sind. Wenn der Anbieter wollte – oder im Falle einer behördlichen Anordnung muss – kann er die Telefonate und Videogespräche seiner Nutzer also problemlos aufzeichnen.

Die gute Nachricht ist, dass Sie sich leicht schützen können, indem Sie vorhandene Verschlüsselungsfunktionen aktivieren oder einen anderen Dienst nutzen. Denn bei vielen Anbietern ist eine gute, nach-

vollziehbare Verschlüsselung längst Standard. Im Idealfall kommt eine Ende-zu-Ende-Verschlüsselung (E2E) zum Einsatz, die gewährleistet, dass nur die Gesprächsteilnehmer den Anruf entschlüsseln können. Damit kommunizieren Sie annähernd so sicher, als würden sie sich im gleichen Raum wie Ihr Gesprächspartner befinden.

Eine der meistverbreiteten Apps ist ohne Zweifel **WhatsApp** (siehe S. 56). Es ist also naheliegend, die Chat-App auch für Telefonate und Videochats zu verwenden. In puncto Verschlüsselung spricht auch nichts dagegen: WhatsApp nutzt das Secure Real-Time Transport Protocol (SRTP) für die Audio- und Videokommunikation. Die Gespräche sind E2E-verschlüsselt und lassen sich nachzeitigem Stand nicht belauschen. Im einfachsten Fall rufen Sie besser über WhatsApp an als vollkommen unverschlüsselt über Festnetz oder Handy-Telefonat. Das funktioniert sogar in Gruppen mit bis zu 8 Teilnehmern.

Doch die Sache hat auch zwei Haken: Die Anruf-Funktion funktioniert derzeit nur am Smartphone oder Tablet, nicht per WhatsApp Web am Rechner. Und dann ist da auch noch der Megakonzern Facebook, der sich WhatsApp vor einiger Zeit einverleibt hat und sein Geld bekanntlich mit den Daten seiner Nutzer verdient. Die Versuchung, sich zumindest an den Metada-



Bild: Albert Hulm

ten der Nutzer zu bedienen und zum Beispiel das Telefonbuch auszuwerten, ist groß. Und falls eines Tages eine Krypto-Backdoor angeordnet werden sollte, dann wäre WhatsApp vermutlich der erste Dienst, der sie umsetzen muss.

Sicheres Signal

Wer Wert auf Datenschutz legt, greift daher zu **Signal**. Die App funktioniert wie WhatsApp und nutzt die gleiche Verschlüsselung, versucht aber möglichst wenig Metadaten anfallen zu lassen und ist Open Source. Wer möchte, kann also eigenhändig im Quellcode nach Backdoors suchen. Auch über Signal kann man in Ton und Bild telefonieren, das klappt auch am Rechner. Vor Kurzem wurden die Videocalls für Gruppen mit bis zu fünf Teilnehmern freigeschaltet.

Viele weitere Chat-Apps eignen sich inzwischen ebenfalls für verschlüsselte Anrufe, darunter etwa **Threema** und **Wire**. Während man bei Threema aktuell nur mit einer Person gleichzeitig sprechen kann, unterstützt Wire bereits Gruppenanrufe mit bis zu 25 Teilnehmern. Bei Videocalls liegt das Limit bei 12 Teilnehmern. Grundsätzlich gilt: Wählen Sie am besten den Messenger, den die meisten Ihrer Kontakte bereits einsetzen. Apple-Nutzer können über **FaceTime** durchgängig Ende-zu-Ende-verschlüsselt kommunizieren, erreichen darüber allerdings ausschließlich andere Apple-Nutzer. Das Limit liegt hier bei 32 Teilnehmern.

Googles Pendant heißt **Google Duo** und setzt ebenfalls auf E2E, das Limit liegt ebenfalls bei 32 Personen. Passende Apps gibt es für Android und iOS, am Rechner kann man auf die Web-App per Browser zurückgreifen. Google macht auf seiner

FRITZ!Box 7580

Rufnummer eintragen

Weitere Einstellungen zur Verbindung

Internettelefonie-Anbieter kontaktieren über IPv4 und IPv6, IPv4 bevorzugt

Verschlüsselte Telefonie aktivieren

Fritzboxen können Festnetzgespräche (VoIP) seit Kurzem verschlüsselt übertragen. Sie müssen die Option nur noch einschalten.

Website kein Geheimnis daraus, dass Metadaten wie Telefonnummern und Geräte-IDs der Gesprächsteilnehmer „ungefähr einen Monat lang sicher auf Google-Servern“ gespeichert werden, „um Fehler zu beheben und Funktionen zu verbessern“.

Berufsgeheimnis

Im beruflichen Umfeld muss eine Videochat-Lösung für virtuelle Meetings gruppentauglich und am Rechner nutzbar sein. **Microsoft Teams** ist zwar komfortabel und dockt nahtlos an andere Microsoft-Produkte an. Doch dieser Komfort hat einen hohen Preis: Teams beherrscht aktuell keine E2E-Verschlüsselung. Vertrauliche Gespräche, die vormalig in Konferenzräumen von Angesicht zu Angesicht geführt wurden, lassen sich somit prinzipiell belauschen, wenn man Zugriff auf die Microsoft-Server erlangt. **Skype**-Anrufe sind nur dann E2E-verschlüsselt, wenn man explizit einen „privaten Anruf“ startet. Das klappt allerdings noch nicht mit der Web-Version des Tools.

Die Videokonferenz-Plattform **Zoom** ist schon einen großen Schritt weiter und beherrscht E2E-verschlüsselte Videokonferenzen mit bis zu 200 Teilnehmern (siehe Whitepaper unter ct.de/yqb5). Derzeit befindet sich die E2E-Verschlüsselung von Zoom noch im Testbetrieb, sie kann aber bereits von jedem Gastgeber aktiviert werden. Klicken Sie hierzu auf der Zoom-Website nach dem Einloggen auf „Mein Account/Einstellungen“ und schalten Sie die Option „Durchgehend (E2E) verschlüsselte Meetings“ ein. Zudem sollten Sie darunter den „Default encryption type“ auf „End-to-end encryption“ stellen, damit Ihre Meetings bestmöglich geschützt sind. Verwechseln Sie die Funktion jedoch nicht mit der „Enhanced encryption“: Diese ist weniger sicher, da hier auch Zoom die Schlüssel für die E2E-Verschlüsselung kennt.

Innerhalb eines Meetings erkennen Sie die E2E, indem Sie auf den grünen Schutzschild oben links klicken. Steht dort „Verschlüsselung: Durchgehend“, dann haben Sie alles richtig gemacht. Darunter können Sie mit „Verifizieren“ einen Sicherheitscode anzeigen, dieser muss bei allen Gesprächsteilnehmern identisch sein. Eine E2E-Verschlüsselung gibt es auch für andere professionelle Videokonferenz-Programme wie **Cisco WebEx**. Erkundigen Sie sich am besten direkt beim Anbieter nach dem aktuellen Stand der Dinge.

Im Idealfall nutzen Sie für vertrauliche Kommunikation keine fremde Infrastruktur, sondern betreiben den Server im eigenen Haus. Das hat den Vorteil, dass sie alles unter Ihrer Kontrolle haben, einschließlich der Metadaten. Die Gespräche verlassen das Firmennetz bestenfalls erst gar nicht und die Mitarbeiter im Homeoffice werden verschlüsselt über VPN angebunden. Gute Fortschritte macht die quelloffene Videokonferenz-Lösung **Jitsi**. Sie können den Server selbst betreiben, passende Clients gibt es für iOS und Android und als Web-Version. Das Entwicklerteam ist gerade dabei, eine E2E-Verschlüsselung zu implementieren. Sie können die Funktion schon jetzt ausprobieren. Wer eine Nextcloud betreibt, der kann mit **Nextcloud Talk** ebenfalls Ende-zu-Ende-verschlüsselt in Echtzeit kommunizieren.

Festnetz verschlüsselt

Wie eingangs erwähnt, ist auch die Festnetztelefonie problematisch: Die meist per VoIP übertragenen Gespräche sind vollkommen unverschlüsselt. Wer die Daten auf dem Transportweg zum Ziel abgreift, kann die Gespräche problemlos mithören und manipulieren. Eine E2E-Verschlüsselung ist zwar nicht ohne Weiteres umsetzbar, jedoch ist zumindest eine Transport-

verschlüsselung zum VoIP-Anbieter drin: Bei den **AVM-Fritzboxen** können Sie seit FritzOS-Version 7.20 die verschlüsselte Telefonie aktivieren. Spielt Ihr VoIP-Anbieter mit, dann werden die Gespräche verschlüsselt zu ihm übertragen – und im Idealfall auch von dort aus weiter verschlüsselt zum Gesprächspartner. Hierbei kommt SIP-over-TLS (SDES-sRTP) zum Einsatz. Eine ausführliche Anleitung mit weiteren Details finden Sie in [c't 22/2020](https://ct.de/2020/02/22) [1].

Fazit

Ganz gleich, ob es um die Alltagskommunikation mit Familie und Freunden oder virtuelle Meetings im Homeoffice geht: Mit der Wahl des richtigen Kanals können Sie schon jetzt in allen Fällen komfortabel und verschlüsselt kommunizieren. Es gibt keinen Grund, es nicht zu tun und auch das Argument „Ich habe doch nichts zu verbergen“ zählt schon lange nicht mehr. Gerade in Zeiten, in denen Apps das persönliche Treffen ersetzen, sollten Sie so viel verschlüsseln, wie Sie können. (rei@ct.de) **ct**

Literatur

- [1] Alexander Traud, Chiffriert fernsprechen, FritzOS 7.20: Verschlüsselt telefonieren, Grenzen der Methode kennen, [c't 22/2020](https://ct.de/2020/02/22), S. 18

Apps & Hintergrundinfos: ct.de/yqb5

The screenshot shows the Zoom settings interface. At the top, there are buttons for 'BEITRETEN' and 'VERANSTALTEN', and a hamburger menu icon. The main heading is 'Durchgehend (E2E) verschlüsselte Meetings' with a 'Technical Preview' badge. Below this, a text block explains that end-to-end encryption provides additional security, allowing only participants to decrypt the meeting. A toggle switch is currently turned on. To the right of the toggle are links for 'Geändert' and 'Zurücksetzen'. Below this, there is a section for 'Default encryption type' with a descriptive text: 'If the admin locks this setting, users will not be able to change the encryption type for meetings (i.e. scheduled, instant, PMI)'. At the bottom, there are two radio button options: 'Enhanced encryption' (which is unselected) and 'End-to-end encryption' (which is selected). Both options have a help icon next to them.

Zoom bietet auch Gratis-Nutzern eine Ende-zu-Ende-Verschlüsselung für Videomeetings. Die Funktion befindet sich noch im Teststadium, lässt sich aber bereits nutzen.

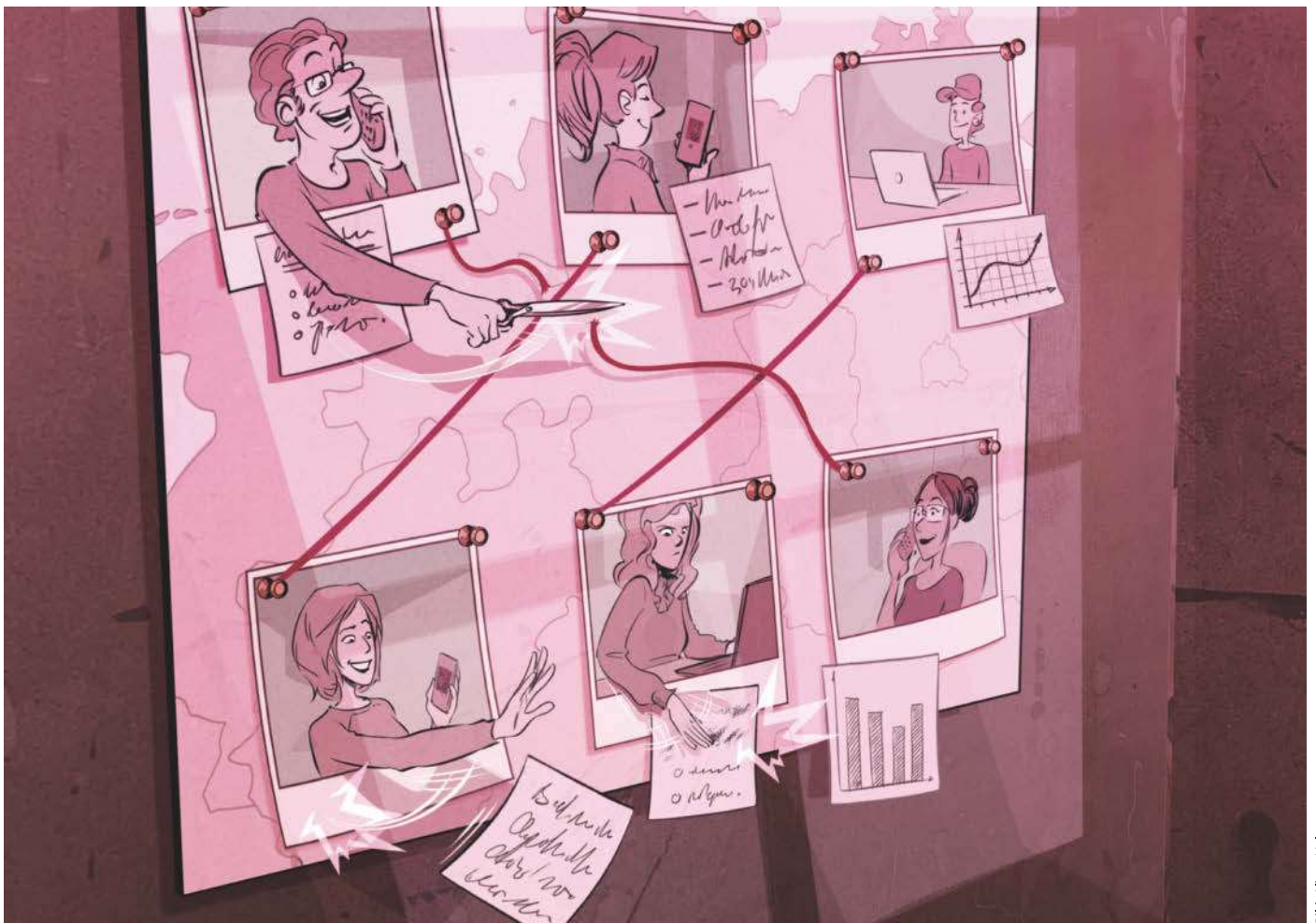


Bild: Albert Hulm

Für immer unlesbar

Wie moderne Kommunikationsverschlüsselung funktioniert

Ende-zu-Ende-Verschlüsselung klingt nach absoluter Sicherheit, aber bei vielen Implementierungen gibt es noch Luft nach oben. Mit dem Boom von Messengern kamen neue Verfahren auf, die sogar dann noch Sicherheiten bieten, wenn Kommunikationspartner unterwandert werden.

Von Sylvester Tremmel

Eine Nachricht abhör- und manipulationssicher zu verschicken, ist eigentlich gar nicht kompliziert: Man einigt sich mit dem Korrespondenten auf

einen Schlüssel und chiffriert damit die Nachricht. Passende Verfahren sind altbekannt. Aber wie einigt man sich mit seinem Gesprächspartner auf einen Schlüssel? Das muss ebenfalls abhör- und manipulationssicher geschehen und die Katze beißt sich in den Schwanz.

Über Jahrtausende wurden verschiedenste Tricks angewandt, um den Schlüssel zu transportieren. Seit den 1970er-Jahren sind bestimmte mathematische Tricks beliebt: Asymmetrische Kryptosysteme, auch Public-Key-Verfahren genannt, funktionieren mit zwei verschiedenen Schlüsseln – einem öffentlichen zum Verschlüsseln und einem dazu passenden privaten Schlüssel zum Entschlüsseln. Man

kennt solche Systeme zum Beispiel von der Mailverschlüsselung OpenPGP (siehe ct.de/yvbv). Nachrichten, die mit dem öffentlichen Schlüssel chiffriert wurden, können nur mit dem privaten entschlüsselt

werden. Außerdem lässt sich der private Schlüssel nicht aus dem öffentlichen rekonstruieren. Das ist der entscheidende

Punkt, weil man so seinen öffentlichen Schlüssel ruhigen Gewissens an potenzielle Gesprächspartner verteilen kann.

Die fortschreitende Verbesserung von Computern erzwingt zwar gelegentliche Anpassungen an den Krypto-Verfahren und Quantencomputer bedrohen manche Verfahren grundsätzlich. Aber in der Praxis lösen Public-Key-Verfahren das Prob-



lem des Schlüsselaustauschs. Man kann die beiden Schlüssel nutzen, um Nachrichten sicher zu (de-)chiffrieren, oder um sich über Verfahren wie einen Diffie-Hellman-Schlüsselaustausch abhörsicher auf ein gemeinsames Geheimnis zu einigen und es als Schlüssel für herkömmliche – symmetrische – Verschlüsselungsverfahren zu nutzen. Durch Standards wie OpenPGP sind Public-Key-Verfahren für jedermann verfügbar. Also gibt es nichts mehr zu tun?

Identitätsfragen

Leider doch: Über die Jahre und mit der zunehmenden Verbreitung von Public-Key-Verfahren haben sich diverse Unzulänglichkeiten herauskristallisiert. Eine davon ist **Authentifizierung**. Also die Garantie, dass man mit dem beabsichtigten Gegenüber spricht und nicht einem Angreifer, der sich zwischen die Korrespondenten geschaltet hat. Public-Key-Verfahren bieten dafür digitale Signaturen, die beweisen, dass eine Nachricht vom Besitzer eines bestimmten privaten Schlüssels kommt. Üblicherweise kombiniert man die Signatur mit der Verschlüsselung der Nachricht, sodass nur der Kommunikationspartner den Ursprung der Nachricht sicher nachweisen kann.

Dafür müssen die beiden Korrespondenten aber sicher den öffentlichen Schlüssel ihres Gegenübers kennen. Wenn ein Angreifer es schafft, seinen eigenen öffentlichen Schlüssel als den eines Partners auszugeben, dann kann er natürlich auch die passenden Signaturen erstellen. Eine Möglichkeit dieses Problem anzugehen, sind vertrauenswürdige Zertifizierungsstellen, die für die Korrektheit des Schlüssels bürgen. Diese Methode kommt zum Beispiel bei der HTTPS-Verschlüsselung von Webseiten oder der S/MIME-Verschlüsselung von E-Mails zum Einsatz.

Allerdings muss man der Zertifizierungsstelle vertrauen. Das ist grundsätzlich schlecht – Verschlüsselung soll Vertrauen unnötig machen – und auch praktisch haben Zertifizierungsstellen schon mehrfach grobe Fehler gemacht. Viele Messenger und auch manche Systeme für PGP-verschlüsselte E-Mails setzen daher auf eine andere Methode: TOFU und das Prüfen von Fingerabdrücken. „TOFU“ steht für „Trust on first use“ und bedeutet, anfänglich einfach anzunehmen, dass der öffentliche Schlüssel korrekt ist. So kann sich ein Angreifer immerhin nicht nachträglich in eine Kommunikation einschalten, er muss schon beim erstmaligen

Nachschießen des öffentlichen Schlüssels eine Fälschung untergeschoben haben.

Um auch das zu verhindern, kann man – wenn man sich einmal real sieht – die Fingerabdrücke von Schlüsseln vergleichen. Stimmen sie überein, dann hat man sicher den wahren Schlüssel. Um den Abgleich möglichst einfach zu machen, können ihn viele Messenger semiautomatisch durchführen – zum Beispiel über das gegenseitige Scannen von QR-Codes – und merken sich, welche Kontakte verifiziert wurden. Ändert sich ein Fingerabdruck später, schlägt der Messenger Alarm.

Ich wars nicht

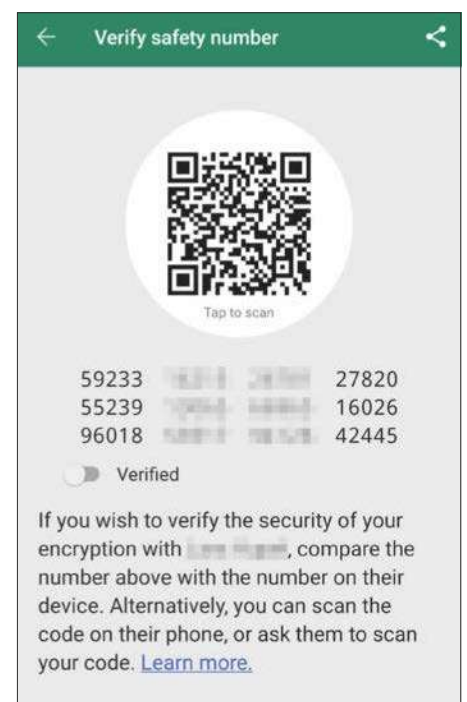
Mit der Authentifizierung geht allerdings eine häufig unerwünschte Eigenschaft einher: Kommunikation kann nicht bestritten werden. Eine mit einem privaten Schlüssel signierte Nachricht kommt ohne jeden Zweifel vom Besitzer dieses Schlüssels. Das lässt sich auch nachträglich prüfen und wird problematisch, wenn zum Beispiel staatliche Stellen einen Kommunikationspartner unterwandern und so an alte Nachrichten im Klartext gelangen. Die tragen Signaturen vom privaten Schlüssel des Absenders und liefern so auch Beweismaterial gegen ihn. Der Angreifer kann die Signaturen leicht prüfen, weil er dazu nur den öffentlichen Schlüssel des Absenders braucht – und der ist eben öffentlich. Es ist umstritten, ob **Abstreitbarkeit** einen praktischen Nutzen hat, gerade gegenüber Stellen, die im Zweifel nicht an gerichtsfesten Beweisen interessiert sind. Zumindest in Rechtsstaaten hilft es aber, Kommunikation bestreiten zu können.

Authentifizierung und Abstreitbarkeit scheinen sich nur auf den ersten Blick zu widersprechen: Tatsächlich wollen Gesprächspartner vornehmlich, dass sie in einer Konversation *aktuell* sicher sein können, mit dem richtigen Korrespondenten zu reden. Sie wollen es nicht nachträglich für bereits vergangene Gespräche beweisen. Die Lösung ist daher ein System, das den Signaturschlüssel regelmäßig wechselt, und zwar so, dass sich keine Rückschlüsse auf frühere Schlüssel ziehen lassen. Man spricht auch von Schlüsselrotation. Wenn ein Gesprächspartner kompromittiert wird, können so aus dem aktuellen Schlüssel keine früheren abgeleitet werden, und alte, vom Angreifer aufgezeichnete Konversationen, lassen sich nicht sicher zuordnen. Voraussetzung dafür ist, dass ausgediente Schlüssel auch gelöscht werden.

Perfekte Geheimhaltung

Wenn Schlüsselrotation nicht (nur) bei Signaturen, sondern auch bei der Verschlüsselung selbst zum Einsatz kommt, kann sie eine noch wichtigere Eigenschaft garantieren: **Folgenlosigkeit**, oft auch (**Perfect Forward Secrecy** (PFS oder FS) genannt. PFS schützt vor dem oben bereits skizzierten Szenario: Ein Angreifer kann die Verschlüsselung nicht brechen, zeichnet die Chiffre aber trotzdem auf. Geheimdienste wie die NSA tun das in großem Stil. Wenn nun, vielleicht Jahre später, der private Schlüssel eines Kommunikationspartners bekannt wird, können damit die jahrelang aufgezeichneten Übertragungen allesamt entschlüsselt werden. PFS verhindert das, weil die Schlüssel wechseln. Der Jahre später kompromittierte Schlüssel verrät nichts über frühere Schlüssel und die von ihnen geschützten Nachrichten bleiben sicher verschlüsselt.

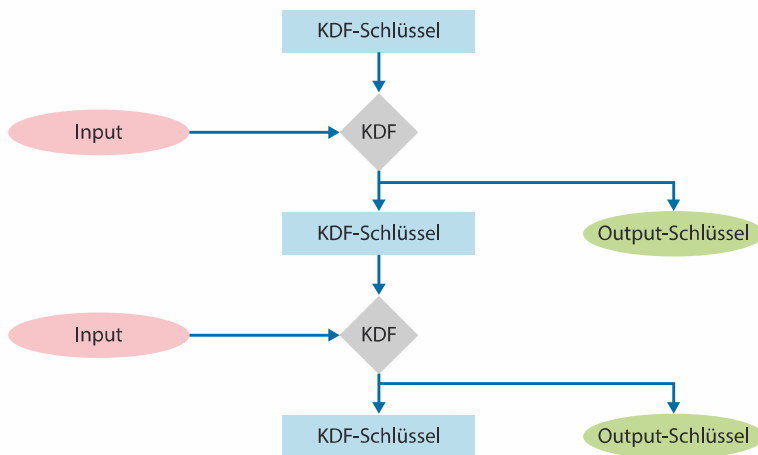
PFS kommt heutzutage bei TLS zum Einsatz und damit automatisch bei vielen Transportverschlüsselungen. Bei Ende-zu-Ende-Verschlüsselungen ist es weniger selbstverständlich: Bei den E-Mail-Verschlüsselungen S/MIME und OpenPGP sind häufige Schlüsselrotationen umständlich und bleiben dem Benutzer überlassen. In der Praxis kommen sie daher kaum vor und E-Mails sind nicht durch PFS geschützt. Manche Messengerprotokolle



Viele Messenger erlauben Fingerabdrücke – Signal nennt sie „safety numbers“ – semiautomatisch abzugleichen.

KDF-Kette

Aus einer Schlüsselableitungsfunktion (key-derivation function, KDF) lässt sich eine Kette knüpfen. Jede Anwendung der KDF generiert einen neuen Output-Schlüssel, der etwa genutzt werden kann, um Nachrichten zu verschlüsseln, und einen neuen Schlüssel für die Kette selbst. KDFs sind wie Hash-Funktionen nicht umkehrbar: Aus einem bekannten Kettenstand lassen sich keine früheren Output- oder KDF-Schlüssel errechnen. Falls die Inputs nicht vorhersagbar sind, lassen sich aus einem bekannten Zustand auch keine zukünftigen Zustände errechnen.



unterstützen PFS ebenfalls nicht, Threema etwa nutzt PFS nur in der Transportverschlüsselung zwischen Client und Server, nicht in der Ende-zu-Ende-Verschlüsselung zwischen den Clients.

Double Ratchet

Der Messenger Telegram unterstützt PFS in seinen geheimen Chats, in denen etwa alle 100 Nachrichten oder einmal pro Woche der Schlüssel gewechselt wird. Bei den meisten anderen Messengern hat sich das Signal-Protokoll (oder Abwandlungen davon) als Quasi-Standard durchgesetzt. Das Protokoll verschlüsselt jede einzelne Nachricht mit einem neuen Schlüssel. Zentrales Element dafür ist der Double-Ratchet-Algorithmus. Er besteht aus symmetrischen und asymmetrischen Ratschen, also Komponenten, die sich nur in eine Richtung bewegen können.

Die symmetrischen Ratschen basieren auf KDF-Ketten (siehe Grafik oben). Für die Inputs der Ketten werden feste Werte genutzt. Für jede zu übermittelnde Nachricht vollzieht der Sender einen Kettenschritt und nutzt den Output-Schlüssel zum Verschlüsseln der Nachricht. Der ebenfalls entstandene neue KDF-Schlüssel ersetzt den alten. Der Empfänger hat eine Kopie der Kette, vollzieht ebenfalls einen Schritt und nutzt den entstandenen identischen Output-Schlüssel zum Ent-

schlüsseln. Alte Schlüssel werden verworfen und die Ketten lassen sich nicht zurückrechnen, was PFS herstellt.

Zum Senden in die andere Richtung nutzen die Partner ein zweites Kettenpaar, sodass sich überschneidend gesendete Nachrichten nicht stören. Bleibt die Frage, wie Kommunikationspartner zu den identischen KDF-Ketten kommen. Dafür ist die asymmetrische Diffie-Hellman-Ratsche (DH-Ratsche, siehe Grafik gegenüber) zusammen mit einer weiteren KDF-Kette – der Root-Chain – zuständig. Beide Partner haben dieselbe Root-Chain. Jedes Mal, wenn die Kommunikationsrichtung wechselt, denkt sich der Sender in der DH-Ratsche ein neues Schlüsselpaar aus und nutzt es als Input, um einen Schritt mit der Root-Chain zu machen. Mit dem Output-Schlüssel der Root-Chain beginnt er eine neue KDF-Kette zum Senden. Über die DH-Ratsche kann der Empfänger ebenfalls denselben Input in seine Kopie der Root-Chain geben und so eine passende neue KDF-Kette zum Empfangen erstellen.

Mit jeder Umkehr der Kommunikationsrichtung wechseln Sender und Empfänger also die genutzten KDF-Ketten. Das DH-Ratchet garantiert so PFS, aber das konnten ja schon die Ketten selbst bereitstellen. Wichtiger ist etwas anderes: **Post-Compromise Security (PCS)**. Diese auch als **Selbstheilung** oder **Future Secre-**

cy bezeichnete Fähigkeit ist das Gegenstück zu PFS. Falls ein Kommunikationsteilnehmer kompromittiert wird, schützt PFS vergangene Kommunikation. Zukünftige kann der Angreifer aber für alle Zeit mitlesen (sofern er nicht bemerkt wurde), selbst wenn er den Zugriff auf den Gesprächsteilnehmer wieder verliert. Schließlich lassen sich die symmetrischen Ratschen (und andere Schlüsselrotationssysteme) leicht „nach vorne“ bewegen. Aus einem einmal bekannten Kettenzustand kann der Angreifer alle zukünftigen Output-Schlüssel selbst errechnen.

Die neuen Schlüsselpaare im DH-Ratchet denken sich die beiden Partner aber aus, sie lassen sich nicht vorhersagen. Wenn ein Angreifer also den Zugriff auf einen Kommunikationspartner verliert, so kann er nur so lange weiter mitlesen, wie die ihm bekannten symmetrischen Ratschen genutzt werden. Sobald aber ein ganzer DH-Schritt erfolgt, sind beide Kettenpaare ausgetauscht und der Angreifer ist wieder ausgesperrt. Die Verschlüsselung hat sich selbst geheilt.

Jenseits der Verschlüsselung

Der Double-Ratchet-Algorithmus nutzt die wechselnden Schlüssel auch zur Authentifizierung und erreicht so Abstreitbarkeit, zumindest in Bezug auf den Nachrichteninhalte. Angreifer könnten aber zum Beispiel den Anbieterserver kompromittieren und dadurch immerhin erfahren, wer mit wem Nachrichten austauscht. Manche Messenger – etwa WhatsApp oder Telegram – analysieren sogar das komplette Telefonbuch ihrer Nutzer und schaffen damit attraktive Angriffsziele. Diverse Messenger versuchen aber, möglichst wenig Metadaten zu sammeln und gesammelte Daten möglichst schnell zu löschen. Löschversprechen muss man als Nutzer allerdings vertrauen, weswegen es besser ist, wenn Messenger Daten gar nicht erheben. Zum Beispiel Threema, Conversations (XMPP) oder Element (Matrix) nutzen IDs, statt die Nutzer um ihre Telefonnummer zu bitten. Signal treibt dagegen viel Aufwand, damit ihre Server die Telefonnummern nicht erfahren (alle Links unter ct.de/yvbv).

Grundsätzlich schreitet die Entwicklung bei der Vermeidung von Metadaten rasch voran. Messenger wie Briar nutzen dezentrale Verbindungen über das Tor-Netzwerk, um Metadaten zu verschleiern; Signal hat „Sealed Sender“ erfunden, damit der Signal-Server Absender

und Empfänger nicht zuordnen kann; XMPP oder Matrix föderieren ihre Server, damit zumindest keine einzelne zentrale Instanz existiert, bei der alle Metadaten anfallen.

Viel Bewegung gibt es auch bei Gruppenchats. Auf der einen Seite des Spektrums an Kompromissen steht Telegram, dessen Gruppen lediglich transportver-

schlüsselt sind. Der Server kennt Metadaten und Inhalte, aber dafür unterstützen Telegram-Gruppen bis zu 200.000 Mitglieder. Das andere Extrem ist Signal, das Gruppen über den Double-Ratchet-Algorithmus abwickelt und den Server nicht mal wissen lässt, wer in welcher Gruppe ist. Signal-Gruppen skalieren aber nur schlecht und sind daher auf 150 Mitglieder

beschränkt. Dazwischen liegt zum Beispiel WhatsApp, das Gruppenzugehörigkeiten vom Server verwalten lässt und in ihnen nur die symmetrischen Ratschen nutzt. Das skaliert besser, kostet aber die Selbstheilung und erzeugt Metadaten auf dem Server. (synt@ct.de) **ct**

Weitere Infos: ct.de/yvbw

Diffie-Hellman-Ratchet

Die Diffie-Hellman-Ratsche ist die übergeordnete Ratsche des Double-Ratchet-Algorithmus. Die sekundären Ratschen befinden sich in den angedeuteten Sending und Receiving Chains.

