Jenseits des zentralen Servers: Ende-zu-Ende-geschützte Kommunikation und Zusammenarbeit

KI-gestützte Angriffe und Quantenrisiko, Gestaltungsprinzipien und zwei realisierte Technologiedemonstratoren: HeyAppPro und CollabNowPro

Beat W. Meier *

Buchautor · Unternehmer · Visionär · Ingenieur — beat-w-meier.ch, Schweiz

ARTIKELINFO

Artikelhistorie:

Erstellt am 11. November 2026

Datenstand: 11. November 2026

Version 1.0

Quellen: Standards, Behördenberichte, Gesetzestexte, begutachtete Fachliteratur, Herstellerangaben sowie eine Code- und Testdurchsicht beider Projekte

Schlüsselwörter:

dezentrale Architektur

Ende-zu-Ende-Verschlüsselung

anonymisiertes Netzwerk

segmentierte Datenhaltung

KI-gestützte Schwachstellensuche

Post-Quanten-Umstellung

digitale Souveränität

ABSTRACT

Drei Entwicklungen verändern die Risikorechnung für zentral betriebene digitale Dienste. KI-Systeme finden und verwerten Software-Schwachstellen heute in einem Tempo, mit dem menschliche Prüfung nicht mithalten kann: An einem einzigen Tag im August 2026 wurden 848 CVEs zum Linux-Kernel veröffentlicht, und eine einzige KI-Kampagne erzeugte 948 funktionierende Exploits zur Rechteausweitung für denselben Kernel. Quantencomputer bedrohen die Public-Key-Verfahren, die heutigen Datenverkehr schützen, und verschlüsselte Daten lassen sich heute aufzeichnen und später entschlüsseln. Gesetze wie der US-amerikanische CLOUD Act verschaffen Behörden Zugriff auf Daten bei Anbietern, unabhängig davon, wo das Rechenzentrum steht. Alle drei Kräfte treffen auf die zentrale Plattform, die Identitäten, Inhalte, Schlüssel und Metadaten an einem Ort hält. Die Studie leitet sechs Gestaltungsprinzipien für eine Architektur ab, die nicht auf eine solche Plattform angewiesen ist, und veranschaulicht sie an zwei Technologiedemonstratoren, die als funktionierende Software bestehen. HeyAppPro ist ein Messenger ohne Teilnehmerregister, der ausschliesslich Ende-zu-Ende-verschlüsselten Verkehr über ein anonymisiertes Netzwerk transportiert und Nachrichten für abwesende Empfänger als Chiffretext auf kleinen, wechselnden Gruppen von Knoten ablegt. CollabNowPro vereint Mail, Kalender, Kontakte, Aufgaben, Notizen, Dateien und einen KI-Assistenten in einer Anwendung, die mit Infrastruktur unter eigener Kontrolle der Organisation arbeitet und diese über ein privates Mesh erreicht. Die Studie beschreibt Vorteile und Funktionsprinzipien, lässt alles weg, was einen Nachbau ermöglichen würde, und benennt die Grenzen: Keiner der beiden Demonstratoren verwendet bisher Post-Quanten-Algorithmen, Anonymität ist nicht absolut, und unabhängige Sicherheitsaudits stehen aus.

Kontakt: beat-w-meier.ch/kontakt · © 2026 Beat W. Meier. Alle Rechte vorbehalten.

Management Summary

Seit zwei Jahrzehnten ist die zentrale Plattform der übliche Ort digitaler Kommunikation. Ein Betreiber führt die Server, verwaltet die Konten, speichert die Inhalte und hält die Schlüssel oder zumindest die Metadaten. Wer diese Plattform kompromittiert, ob technisch, organisatorisch oder per behördlicher Anordnung, erreicht alles auf einmal.

Drei Entwicklungen machen diese Konzentration gefährlicher als bisher. Erstens haben KI-Systeme die Suche nach Schwachstellen in einen industriellen Prozess verwandelt. Ingenieure, die den Linux-Kernel für einen grossen Cloud-Anbieter betreuen, berichten, dass die Zahl der Kernel-CVEs von rund

zwei pro Woche vor 2024 auf rund sechzehn pro Tag gestiegen ist; allein am 15. August 2026 wurden 848 veröffentlicht. [Q01] Im November 2026 meldete ein KI-Anbieter eine einzige Kampagne, die 948 funktionierende Exploits mit Root-Zugriff auf Linux ergab. [Q02]

Zweitens wird das US-amerikanische National Institute of Standards and Technology (NIST) die heutige quantenanfällige Public-Key-Kryptografie nach 2030 als veraltet einstufen und nach 2035 nicht mehr zulassen; es warnt, dass Angreifer bereits heute verschlüsselte Daten sammeln, um sie später zu entschlüsseln. [Q03] Drittens verpflichtet der CLOUD Act Anbieter unter US-Rechtshoheit, Daten in ihrem Besitz, ihrer Verwahrung oder unter ihrer Kontrolle herauszugeben, unabhängig davon, ob sich die Daten innerhalb oder ausserhalb der Vereinigten Staaten befinden. [Q04]

Dass die Gefahr real ist, zeigen allein die Vorfälle des Jahres 2026. In der Schweiz wurden bei einem Lieferanten von Pensionskassensoftware Datensätze von mehr als 100’000 aktiven und ehemaligen Bundesangestellten entwendet. [Q05] In den Vereinigten Staaten wurden bei einem Medizintechnikhersteller Zehntausende Geräte auf einen Schlag gelöscht [Q06], und das FBI verzeichnete für 2025 gemeldete Schäden durch Cyberkriminalität von 20,9 Milliarden US-Dollar. [Q07]

Die hier vorgeschlagene Antwort versucht nicht, die zentrale Plattform weiter zu härten. Sie nimmt die Plattform aus dem Weg. Informationen laufen Ende-zu-Ende-verschlüsselt zwischen den Geräten der Beteiligten, der Transport erfolgt über ein anonymisiertes Netzwerk, das verbirgt, wer mit wem spricht, und was gespeichert werden muss, wird segmentiert: Kein einzelnes System hält alle Daten, und kein Speicherort hält etwas anderes als Chiffretext.

Kernaussage

HeyAppPro und CollabNowPro zeigen, dass diese Architektur keine Forschungsvision ist. Beide bestehen als funktionierende Software auf realen Geräten. HeyAppPro tauscht Nachrichten über eine laufende Flotte von Knoten aus, ohne zentrales Teilnehmerregister. CollabNowPro betreibt Mail-, Kalender- und Kollaborationsdaten mit den eigenen Servern der Organisation, die nur über ein privates Mesh erreichbar sind. Beide sind Technologiedemonstratoren, keine fertigen Produkte: Unabhängige Sicherheitsaudits, Post-Quanten-Kryptografie und die vollständige Geräteabnahme stehen noch aus.

Die Studie benennt den Preis des Ansatzes. Ein anonymisiertes Netzwerk macht Verkehrsanalyse aufwendig, nicht unmöglich. Segmentierte Speicherung verkraftet Ausfälle und begrenzt den Schaden einer Kompromittierung, übersteht aber keine böswillige Mehrheit der Speicherknoten. CollabNowPro ist weiterhin auf Server angewiesen, wenn auch auf solche der Organisation selbst. Und Kryptografie, die heute sicher ist, muss ersetzt werden, bevor grosse Quantencomputer verfügbar sind.

1. Auftrag, Gegenstand und Abgrenzung

1.1 Forschungsfragen

Die Studie beantwortet drei Fragen. Welche Entwicklungen erhöhen das Risiko zentral betriebener Kommunikations- und Kollaborationsdienste? Welche Gestaltungsprinzipien folgen daraus für Systeme, die unter diesen Bedingungen vertraulich bleiben sollen? Und wie setzen die beiden Technologiedemonstratoren HeyAppPro und CollabNowPro diese Prinzipien um, mit welchen Vorteilen und welchen Grenzen?

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Öffentlich.

1.2 Methode und Belegbasis

Die Bedrohungsanalyse stützt sich auf amtliche Standards und Behördenberichte, Gesetzestexte, begutachtete Fachliteratur, Konferenzmaterial und Primärangaben von Herstellern. Herstellerangaben sind Selbstauskünfte und als solche gekennzeichnet. Wo eine Originalpublikation eines Herstellers nicht direkt abrufbar war, zitiert die Studie die darüber berichtende Fachpublikation und vermerkt dies in der Quellenangabe. Jüngste Vorfälle, zu denen noch kein amtlicher Bericht vorliegt, sind über etablierte Fachmedien belegt.

Die Beschreibung der beiden Demonstratoren beruht auf einer Durchsicht ihrer aktiven Quellcode-Repositorien, Anforderungs- und Architekturdokumente, Fortschrittsaufzeichnungen und erfassten Testergebnisse, durchgeführt am 11. November 2026. Aussagen zum Umsetzungsstand unterscheiden drei Stufen: umgesetzt und auf realen Geräten beobachtet, umgesetzt und lokal getestet sowie lediglich spezifiziert. Ein Gestaltungsziel wird nie als nachgewiesene Eigenschaft dargestellt. Für diese Studie wurden keine neuen Tests durchgeführt.

1.3 Bewusste Abstraktion

Die Studie beschreibt das Problem, die Gestaltungsprinzipien und die grundsätzliche Funktionsweise der Demonstratoren. Sie lässt bewusst alle Informationen weg, die einen Nachbau ermöglichen würden. Dazu gehören Nachrichtenformate und Protokollabläufe, Schlüsselhierarchien und Schlüsselableitungen, Zeitgeber, Kontingente und Grenzwerte, die Algorithmen für Knotenauswahl, Zulassung, Auffindung und Speicherplatzierung, Software-Bibliotheken und Versionen, Isolationskonfigurationen sowie die Betriebstopologie. Die Namen HeyAppPro und CollabNowPro werden als Bezeichnungen von Technologiedemonstratoren verwendet. Die Abstraktion schränkt die Überprüfbarkeit der Argumentation nicht ein, denn diese stützt sich auf veröffentlichte Verfahren mit bekannten Eigenschaften.

1.4 Begriffe

Ende-zu-Ende-Verschlüsselung bedeutet, dass nur die Geräte der Kommunizierenden die Schlüssel besitzen, die zum Lesen der Inhalte nötig sind. Ein **anonymisiertes Netzwerk** ist ein Overlay-Netz, das den Verkehr in mehrschichtiger Verschlüsselung über mehrere unabhängige Stationen weiterleitet, sodass keine einzelne Station zugleich Herkunft und Ziel kennt. [Q08] **Metadaten** sind alle Umstände einer Kommunikation ausser dem Inhalt: Identitäten, Kontaktbeziehungen, Zeitpunkte, Grössen und Netzwerkadressen. **Segmentierte Datenhaltung** bedeutet, dass Daten nach Funktion, Eigentümer und Ort so aufgeteilt sind, dass kein einzelnes System ein vollständiges Bild enthält. Ein **privates Mesh** ist ein verschlüsseltes Overlay-Netz, dem nur einzeln zugelassene Geräte angehören. Ein **Technologiedemonstrator** ist funktionierende Software, die die Machbarkeit eines Entwurfs belegt, ohne Produktreife zu beanspruchen.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Öffentlich.

2. Die veränderte Bedrohungslage

2.1 KI-gestützte Schwachstellensuche: das Beispiel Linux

Linux betreibt den grössten Teil der Server weltweit, und seine Entwicklung ist ungewöhnlich transparent. Das macht es zu einem guten Indikator dafür, was KI-gestützte Codeanalyse für jede grosse Codebasis bedeutet.

An der Linux Plumbers Conference 2026 legten Ingenieure, die den Kernel für eine grosse Cloud-Infrastruktur betreuen, Daten aus zwei Jahren vor. Vor 2024 sahen sie rund zwei Kernel-CVEs pro Woche. Danach stieg die Rate auf rund sechzehn pro Tag, eine Zunahme um mehr als das Fünfzigfache, und Spitzen von Hunderten pro Tag wurden üblich. Am 15. August 2026 wurden an einem einzigen Tag 848 Kernel-CVEs veröffentlicht. Ihr Schluss: Eine manuelle Triage ist nicht mehr möglich. [Q01] Ein Teil dieses Wachstums ist verfahrensbedingt, denn das Kernel-Projekt vergibt seit 2024 eigene CVE-Kennungen und erklärt, nicht beurteilen zu können, welche Einträge für ein bestimmtes System von Bedeutung sind. [Q09] Fachberichte über Daten des Stable-Maintainers des Kernels nennen die zweite Ursache: Die Zahl der pro Kernel-Release behobenen CVEs stieg innerhalb weniger Releases von rund 500 auf mehr als 1’500, und die meisten Fehler der jüngsten Releases wurden von KI-Plattformen für Code-Reviews und grossen Sprachmodellen gefunden. [Q10]

Auch der Schritt vom Finden zum Ausnutzen ist automatisiert. Laut einem am 4. November 2026 veröffentlichten Bericht identifizierte eine Prototyp-Pipeline eines KI-Anbieters 2’308 mögliche Schwachstellen im Linux-Kernel, reproduzierte 1’724 davon dynamisch und erzeugte 948 verschiedene lokale Exploits zur Rechteausweitung, die einem unprivilegierten Benutzer Root-Zugriff verschaffen. Die angegebenen Kosten betrugen rund 1,2 Millionen US-Dollar an Rechenguthaben. Der Anbieter erwartet, dass führende Modelle innerhalb weniger Jahre voraussichtlich alle Schwachstellen finden werden, die in einem bestimmten Softwareprojekt vorhanden sind. [Q02] Ein zweiter Anbieter meldete im April 2026, sein unveröffentlichtes Modell habe Tausende bisher unbekannte Schwachstellen hohen Schweregrads gefunden, darunter solche in jedem grossen Betriebssystem und jedem grossen Webbrowser, und habe mehrere Fehler im Linux-Kernel selbständig zu einer vollständigen Übernahme eines Rechners verkettet. [Q11]

Zwei Einschränkungen gelten. Viele Kernel-CVEs sind von geringem Schweregrad oder betreffen Code, den ein bestimmtes System nicht nutzt. [Q09], [Q10] Und die zitierten Anbieter melden ihre Funde den Maintainern, damit diese sie beheben können. Keine der beiden Einschränkungen ändert den strukturellen Befund: Die Kosten, einen ausnutzbaren Fehler in komplexer Software zu finden, sinken um Grössenordnungen, und die Fähigkeit wird nicht allein bei den Verteidigern bleiben. [Q11]

2.2 Jüngste Vorfälle in der Schweiz und in den Vereinigten Staaten

Die Gefahr ist nicht hypothetisch. Allein die Vorfälle des Jahres 2026 zeigen in beiden Ländern dasselbe Muster.

Schweiz. Im ersten Halbjahr 2026 gingen beim Bundesamt für Cybersicherheit 27’128 freiwillige Meldungen und 200 Meldungen meldepflichtiger Cybervorfälle ein; es zählte 79 Ransomware-Fälle. Das Amt hält zudem fest, dass Cybersabotage für einzelne Staaten zu einem praktikablen Instrument geworden ist. [Q12]

Der schwerwiegendste Fall betrifft die Bundesverwaltung selbst. Ende September 2026 drangen Angreifer bei PK Softech ein, einem Softwarelieferanten von Pensionskassen, darunter der Pensionskasse des Bundes Publica. Gemäss Fachberichten, die sich auf Recherchen des Tages-

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Öffentlich.

Anzeigers stützen, wurden Datensätze von mehr als 100’000 aktiven und ehemaligen Bundesangestellten entwendet, mit Namen, Geburtsdaten, AHV-Nummern, Adressen und Lohndaten, teilweise auch mit Bankverbindungen. Der Arbeitgeber ist selbst bei Angehörigen der Bundespolizei und des Nachrichtendienstes ersichtlich, die unter Legendenidentitäten arbeiten, und der Bund setzte eine Taskforce ein. Der Angriff wird der Ransomware-Gruppe Akira zugeschrieben. Eine städtische Pensionskasse, die Daten lediglich zum Test eines geplanten Systemwechsels übermittelt hatte, stellte fest, dass auch die Daten ihrer Versicherten abgeflossen waren. [Q05]

Zwei weitere Fälle zeigen die Breite. Am 30. April 2026 wurde das Radiologienetzwerk Groupe 3R mit 20 Zentren in der Westschweiz zum zweiten Mal innerhalb eines Jahres angegriffen. Unternehmensdaten wurden gestohlen und von den Tätern veröffentlicht, medizinische Daten wurden verschlüsselt und vorübergehend unbrauchbar, und die IT-Infrastruktur aller Zentren musste neu aufgebaut werden. [Q13] Im Herbst 2026 wurden Daten zum Kauf angeboten, die bei einem Waadtländer Unternehmen für Sicherheitsinstallationen entwendet worden waren. Gemäss der Berichterstattung umfassen sie Grundrisse, Kamerastandorte und teilweise Zugangsdaten für Gefängnisse, Polizeieinrichtungen, Banken und Unternehmen. [Q14]

Vereinigte Staaten. Das Internet Crime Complaint Center des FBI registrierte für 2025 1’008’597 Anzeigen mit gemeldeten Schäden von 20,877 Milliarden US-Dollar, 26 Prozent mehr als im Vorjahr. [Q07] Im März 2026 drangen Angreifer, die die US-Regierung einem iranischen Nachrichtendienst zuordnete, beim Medizintechnikhersteller Stryker ein und löschten aus der Ferne Zehntausende Mitarbeitergeräte auf einen Schlag. Der Betrieb war tagelang gestört, und der Vorfall wirkte sich wesentlich auf das Quartalsergebnis des Unternehmens aus. Im August 2026 legte ein Cyberangriff das weltweite Netzwerk des Medizinprodukteherstellers Boston Scientific lahm. Bestellungen und Versand standen still, und die unmittelbare Wiederherstellung dauerte zwei Wochen. Im Bildungsbereich stahlen Angreifer personenbezogene Daten von mehr als 30 Millionen Lernenden und Mitarbeitenden der Lernplattform Canvas, verunstalteten später während der Abschlussprüfungen deren Anmeldeseiten, und der Betreiber zahlte schliesslich ein Lösegeld. [Q06]

Daraus folgen drei Beobachtungen. In nahezu jedem Fall entstand der Schaden an einem Konzentrationspunkt: bei einem Lieferanten, der die Daten vieler Organisationen hielt, bei einer zentralen Funktion, von der aus Zehntausende Geräte auf einmal gelöscht werden konnten, oder bei einer Plattform, die die Daten Tausender Institutionen speicherte. Daten, die nur zu Testzwecken übergeben worden waren, gingen zusammen mit Produktivdaten verloren. Und die Opfer waren keine nachlässigen Aussenseiter. Zu ihnen gehören die Pensionskassenverwaltung eines Staates und börsenkotierte Technologieunternehmen.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Öffentlich.

2.3 Warum zentrale Serverstrukturen das Risiko bündeln

Ein Softwarefehler ist in dem Mass gefährlich, in dem das betroffene System Daten hält. Zentrale Plattformen halten alles: die Konten aller Nutzenden, ihre Inhalte oder zumindest deren Chiffretext, Schlüssel oder Material zur Schlüsselwiederherstellung sowie die Metadaten jeder Interaktion. Ein einziger erfolgreicher Angriff erfasst deshalb die gesamte Nutzerbasis.

Zwei amtliche Untersuchungen veranschaulichen dies. Das US-amerikanische Cyber Safety Review Board untersuchte das Eindringen in einen grossen Cloud-Maildienst im Jahr 2023. Ein einziger kompromittierter Signaturschlüssel erlaubte den Angreifern den Zugriff auf die Postfächer von 22 Organisationen und mehr als 500 Einzelpersonen, und das Board kam zum Schluss, dass das Eindringen vermeidbar gewesen wäre. [Q15] Im November 2024 bestätigten FBI und CISA, dass staatsnahe Akteure die Netze mehrerer Telekommunikationsunternehmen kompromittiert hatten. Die Angreifer stahlen Verbindungsdaten von Kunden, fingen private Kommunikation ausgewählter Personen ab und kopierten Informationen, die gerichtlich angeordneten Auskunftsersuchen von Strafverfolgungsbehörden unterlagen. [Q16] Der zweite Fall verdient Beachtung, weil die Zugriffseinrichtungen, die Betreiber für Behörden vorhalten müssen, selbst zum Angriffsziel wurden.

KI-gestützte Schwachstellensuche vervielfacht diese Exponierung. Ein zentraler Dienst muss jeden relevanten Fehler beheben, bevor ein Angreifer ihn nutzt, und zwar über einen Stapel aus Betriebssystem, Virtualisierung und Anwendungssoftware, der sich täglich ändert. Abschnitt 2.1 zeigt, dass dieser Wettlauf immer schwerer zu gewinnen ist.

2.4 Quantencomputer und Harvest Now, Decrypt Later

Heutiger Schlüsselaustausch und heutige digitale Signaturen beruhen auf mathematischen Problemen, die ein ausreichend grosser Quantencomputer lösen könnte. NIST hat seinen Bericht zur Umstellung im Oktober 2026 fertiggestellt. Es wird quantenanfällige Public-Key-Kryptografie, darunter RSA, Diffie-Hellman und Verfahren auf elliptischen Kurven, nach 2030 als veraltet einstufen und nach 2035 unter seinen Standards nicht mehr zulassen. Der Bericht nennt den Grund für die Dringlichkeit: Bei der als Harvest Now, Decrypt Later bezeichneten Bedrohung sammeln Angreifer heute verschlüsselte Daten, um sie zu entschlüsseln, sobald die Technik ausgereift ist. Symmetrische Kryptografie ist deutlich weniger betroffen. [Q03] Die Ersatzstandards liegen vor. NIST veröffentlichte seinen ersten Post-Quanten-Standard für die Schlüsselkapselung im August 2024. [Q17]

Wie weit ist die Bedrohung entfernt? Die Schätzungen bewegen sich stetig in eine Richtung. 2019 schätzte man, dass die Faktorisierung eines 2048-Bit-RSA-Schlüssels 20 Millionen verrauschte Qubits erfordere. Eine Analyse von 2025 eines Forschers an einem führenden Quantenlabor senkt dies auf weniger als eine Million verrauschte Qubits und weniger als eine Woche Laufzeit, bei unveränderten Annahmen über die Hardware. [Q18] Eine solche Maschine existiert heute nicht. Doch Daten, die zehn oder zwanzig Jahre vertraulich bleiben müssen, sind bereits jetzt gefährdet, wenn ihr Chiffretext heute aufgezeichnet werden kann.

Damit rückt eine Frage in den Blick, die leicht übersehen wird: Wo lässt sich Chiffretext in grossen Mengen sammeln? Die Antwort lautet wiederum: an zentralen Punkten, etwa bei Plattformen, die verschlüsselte Archive für Millionen von Nutzenden speichern, und an Netzwerkstellen, an denen deren Verkehr zusammenläuft.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Öffentlich.

2.5 Behördlicher Zugriff und Rechtshoheit

Die zweite Herausforderung ist kein Angriff, sondern eine rechtliche Konstruktion. Section 2713 von Title 18 des United States Code, 2018 durch den CLOUD Act eingefügt, verpflichtet Anbieter von Kommunikations- und Clouddiensten, Daten in ihrem Besitz, ihrer Verwahrung oder unter ihrer Kontrolle zu sichern und herauszugeben, unabhängig davon, ob sich die Daten innerhalb oder ausserhalb der Vereinigten Staaten befinden. [Q04] Entscheidend ist damit die Kontrolle durch einen Anbieter unter US-Rechtshoheit, nicht der Standort des Rechenzentrums. Ein europäisches oder schweizerisches Rechenzentrum, das ein solcher Anbieter betreibt, ändert an der rechtlichen Reichweite nichts.

Die Vereinigten Staaten sind nicht das einzige Beispiel. Das Schweizer Recht verpflichtet Fernmeldedienstanbieterinnen, Verbindungsdaten aufzubewahren und Überwachungsmassnahmen zu unterstützen. [Q19] Im Vereinigten Königreich gab ein führender Gerätehersteller 2025 bekannt, seine Ende-zu-Ende-verschlüsselte Option für Cloud-Speicher dort neuen Nutzenden nicht mehr anbieten zu können, und erklärte zugleich, nie eine Hintertür in seine Produkte eingebaut zu haben. [Q20] Diese Studie beurteilt die Legitimität solcher Befugnisse nicht. Sie bestehen in demokratischen Staaten im Rahmen gerichtlicher Verfahren. Der architektonische Befund ist enger gefasst: Jedes dieser Instrumente richtet sich an einen Vermittler, der Daten oder Schlüssel hält. Wo kein Vermittler lesbare Daten hält, kann sich eine Anordnung nur an die Personen richten, die tatsächlich kommunizieren. Genau dort verortet sie der Rechtsstaat traditionell.

Für Industrie, Behörden und Privatpersonen gleichermassen folgt daraus eine Abhängigkeit, die Verträge nicht beseitigen können. Solange ein Dritter die Daten technisch lesen oder herausgeben kann, hängt deren Vertraulichkeit von der Rechtsordnung und der inneren Sicherheit dieses Dritten ab.

2.6 Synthese

Druckfaktor	Was sich ändert	Warum zentrale Plattformen exponiert sind
KI-gestützte Schwachstellensuche	Ausnutzbare Fehler werden schneller und kostengünstiger gefunden und zu Angriffswerkzeugen gemacht	Ein Fehler in einer Plattform legt alle Nutzenden und alle Daten auf einmal offen
Quantencomputer	Aufgezeichneter Chiffretext kann später lesbar werden	Plattformen und ihre Netzwerkränder sind die natürlichen Sammelpunkte für Chiffretext in grossen Mengen
Grenzüberschreitender behördlicher Zugriff	Anbieter müssen herausgeben, was sie kontrollieren, unabhängig vom Standort	Der Plattformbetreiber ist der Adressat, der Daten, Schlüssel oder Metadaten hält
Innentäter- und Betreiberrisiko	Administratoren und Lieferanten haben technischen Zugriff	Gebündelte Berechtigungen ermöglichen gebündelten Missbrauch

Alle vier Druckfaktoren wirken auf dieselbe strukturelle Eigenschaft. Die folgenden Prinzipien beginnen deshalb nicht bei stärkeren Mauern um das Zentrum. Sie beginnen mit der Frage, welche Funktionen überhaupt ein Zentrum brauchen.

3. Gestaltungsprinzipien der Antwort

3.1 Kein zentraler Punkt, der Identitäten, Inhalte und Schlüssel hält

Das erste Prinzip ist Trennung. Zentrale Dienste vereinen Identität, Inhaltsschutz, Transport, Zwischenspeicherung und Abrechnung in einer Hand. Werden diese Funktionen getrennt und verschiedenen Parteien zugewiesen, die ihr Wissen nicht zusammenführen können, legt die Kompromittierung einer Partei nicht mehr das Ganze offen. Identitäten entstehen auf dem Gerät und

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Öffentlich.

werden nirgends registriert. Abrechnung und Betriebserlaubnisse übernimmt eine Verwaltung, die nie Kommunikationsdaten sieht.

3.2 Ende-zu-Ende-Verschlüsselung mit Schlüsseln nur auf den Endgeräten

Inhalte werden auf dem sendenden Gerät verschlüsselt und auf dem empfangenden Gerät entschlüsselt. Die Verfahren dafür sind veröffentlicht und formal analysiert. Der Double-Ratchet-Algorithmus erneuert die Schlüssel fortlaufend, sodass ein kompromittierter Schlüssel weder frühere noch, nach der Wiederherstellung, spätere Nachrichten preisgibt. [Q21], [Q22] Die Forschung betrachtet den Inhaltsschutz bei führenden Messengern als weitgehend gelöst, den Schutz der Metadaten dagegen als offen. [Q23] Das Prinzip überträgt dieselbe Regel auf alles Gespeicherte: Ruhende Daten auf dem Gerät sind mit einem Geheimnis verschlüsselt, das nur die Nutzerin oder der Nutzer kennt und das kein Anbieter zurücksetzen kann.

3.3 Transport über ein anonymisiertes Netzwerk

Verschlüsselung verbirgt, was gesagt wird, nicht, wer mit wem spricht. Die zweite Schicht leitet deshalb den gesamten Verkehr über ein anonymisiertes Netzwerk, in dem mehrere unabhängige Stationen die Daten in mehrschichtiger Verschlüsselung weitergeben, ein Konzept, das auf Chaums Arbeit über nicht rückverfolgbare Kommunikation zurückgeht. [Q08] Keine Station kennt beide Enden einer Verbindung, und weder die Dienstknoten noch ein Beobachter des Netzanschlusses der Nutzenden erfahren, wer das Gegenüber ist. Wo dieses Prinzip strikt angewendet wird, gibt es keinen Ausweichweg: Ist das anonymisierte Netzwerk nicht verfügbar, stoppt der geschützte Verkehr und nimmt nie einen direkten Weg.

Die Forschungsliteratur benennt die Grenzen klar. Starke Anonymität, geringe Latenz und geringer Bandbreitenmehraufwand lassen sich nicht alle zugleich erreichen. [Q24] Ein anonymisiertes Netzwerk mit geringer Latenz schützt nicht vor einem Angreifer, der beide Enden einer Verbindung gleichzeitig beobachten kann.

3.4 Segmentierte Datenhaltung

Die Datenspeicher der Zukunft sind segmentiert. Nicht alle Daten liegen an einem Ort in einem System. Dieses Prinzip beantwortet alle vier Druckfaktoren aus Abschnitt 2.6 zugleich, und es hat drei Dimensionen.

Segmentierung nach Funktion bedeutet, dass die Partei, die eine Nachricht speichert, deren Beteiligte nicht identifizieren kann, und dass die Partei, die einen Knoten zulässt oder eine Lizenz abrechnet, nie eine Nachricht sieht. Segmentierung nach Eigentümer bedeutet, dass Daten der kleinsten sinnvollen Einheit gehören, dem Gerät einer Person oder der Infrastruktur einer Organisation, und nicht kundenübergreifend auf einer gemeinsamen Plattform gebündelt werden. Segmentierung nach Ort bedeutet, dass Daten, die ausserhalb eines Geräts gespeichert werden müssen, in verschlüsselte Kopien auf mehrere unabhängige Speicherknoten aufgeteilt werden, die zufällig gewählt und im Lauf der Zeit ersetzt werden, sodass kein Knoten ein vollständiges oder dauerhaftes Bild hat.

Die Idee folgt den klassischen Sicherheitsprinzipien der minimalen Berechtigung und der Trennung von Berechtigungen, die Saltzer und Schroeder 1975 formuliert haben. [Q25] Ihre Wirkung: Ein erfolgreicher Angriff, ein aufgezeichneter Chiffretextstrom oder eine Herausgabeanordnung liefert ein Bruchstück und nicht das Ganze.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Öffentlich.

3.5 Standardmässig private Erreichbarkeit

Ein Server, der nicht erreichbar ist, kann aus dem offenen Internet nicht angegriffen werden. Wo Server nötig sind, werden sie nicht öffentlich exponiert und sind nur über ein verschlüsseltes privates Mesh erreichbar, dessen Mitglieder einzeln zugelassen werden. Das entspricht dem von NIST standardisierten Zero-Trust-Modell, in dem Zugriff pro Gerät und pro Anfrage gewährt wird und nie aufgrund des Netzwerkstandorts. [Q26] Gegen automatisierte Massenausnutzung, wie sie Abschnitt 2.1 beschreibt, gehört das Entfernen der öffentlichen Angriffsfläche zu den wirksamsten verfügbaren Massnahmen.

3.6 Speichersichere Umsetzung und kleine Angriffsfläche

Ein grosser Teil der ausnutzbaren Fehler in Systemsoftware sind Speichersicherheitsfehler. Cybersicherheitsbehörden mehrerer Staaten fordern Hersteller deshalb auf, auf speichersichere Programmiersprachen umzusteigen. [Q27] Beide Demonstratoren setzen ihren sicherheitsrelevanten Kern in einer solchen Sprache um, verwenden einen gemeinsamen Kern auf allen Plattformen und stützen sich auf etablierte, veröffentlichte kryptografische Bausteine ohne selbst erfundene Kryptografie. Funktionen, die nicht gebraucht werden, werden nicht eingebaut. Es gibt keine Telemetrie und keine Werbe- oder Analysekomponenten.

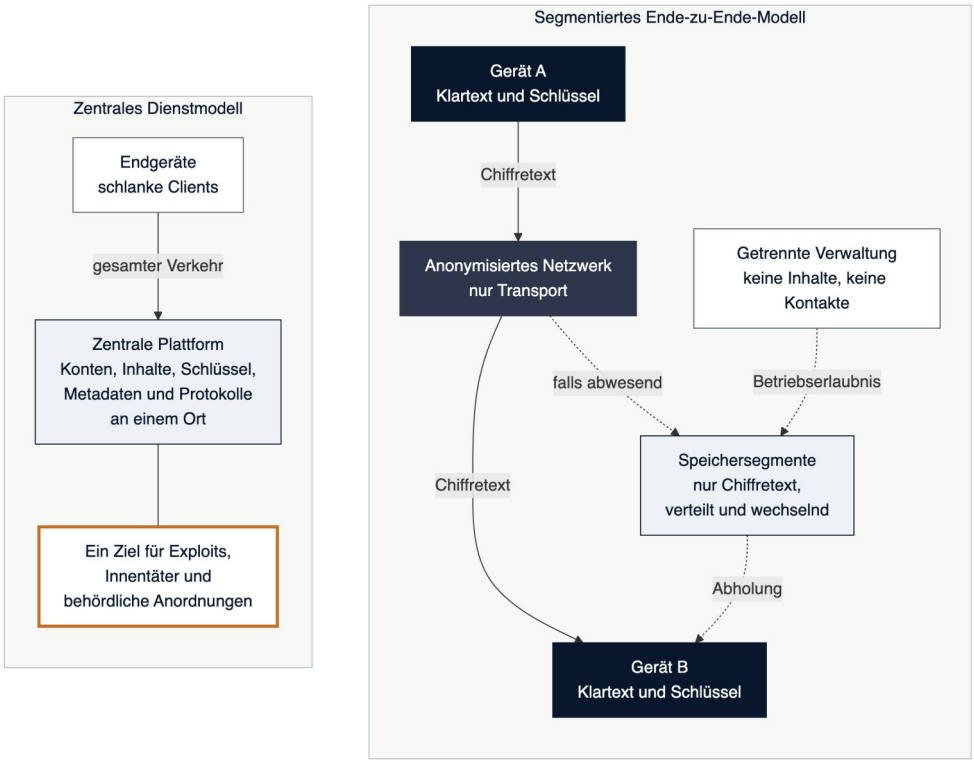


Abbildung 1: Zentrales Dienstmodell und segmentiertes Ende-zu-Ende-Modell.

Im zentralen Modell hält eine Plattform Konten, Inhalte, Schlüssel und Metadaten und ist deshalb ein einziges Angriffsziel. Im segmentierten Modell bestehen Klartext und Schlüssel nur auf den Endgeräten, das anonymisierte Netzwerk transportiert nur, Speicherknoten halten verteilten Chiffretext, und eine getrennte Verwaltung erhält keine Kommunikationsdaten. Eigene Darstellung, ohne Protokolldetails.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Öffentlich.

4. Technologiedemonstrator 1: HeyAppPro

4.1 Zweck

HeyAppPro ist ein Messenger für Personen und Organisationen, die vertraulich kommunizieren wollen, ohne von den Servern und dem Datenzugriff eines einzelnen Anbieters abhängig zu sein. Er umfasst Textnachrichten, Medien- und Dateianhänge sowie Sprachkommunikation. Seine Entwurfsannahme ist streng: Ein Cloud- oder Plattformanbieter oder eine Behörde erhält sämtliche Daten, die bei irgendeinem Anbieter gespeichert sind. Ohne ein Geheimnis, das ausschliesslich die Nutzerin oder der Nutzer besitzt, dürfen diese Daten weder die Entschlüsselung von Gesprächen noch die Übernahme einer Identität ermöglichen.

4.2 Funktionsprinzip

Identität ohne Register. Die Identität einer Person ist ein kryptografisches Pseudonym, das auf dem Gerät erzeugt wird. Weder eine Telefonnummer noch eine E-Mail-Adresse ist erforderlich, und kein zentrales Verzeichnis erfasst, wer das System nutzt. Kontakte entstehen über einmalig verwendbare Einladungen mit begrenzter Gültigkeit, die als Link oder QR-Code weitergegeben werden und von den beiden Beteiligten überprüft werden können.

Inhaltsschutz. Nachrichten und Anhänge werden mit einem etablierten Ratchet-Verfahren Ende-zu-Ende verschlüsselt. [Q21] Schlüssel verlassen die Geräte nie. Alle lokalen Daten sind verschlüsselt und lassen sich nur mit einem separaten App-Passwort öffnen, das weder dauerhaft gespeichert noch übertragen wird und das kein Anbieter zurücksetzen kann. Schlüssel und Gespräche sind von automatischen Cloud-Sicherungen ausgenommen.

Transport. Die gesamte Kommunikation läuft ausschliesslich über das anonymisierte Netzwerk. Ein Notschalter auf App-Ebene sperrt den geschützten Verkehr, sobald dieser Transport nicht verfügbar ist: beim Start, nach einem Ausfall und während eines Netzwechsels. Eine direkte Verbindung wird nie als Ausweichweg genutzt.

Zustellung an abwesende Empfänger. Telefone und Laptops sind nicht immer online. Zentrale Messenger lösen dies mit einer Warteschlange beim Betreiber. HeyAppPro legt die vollständig verschlüsselte Nachricht stattdessen bei einer kleinen Gruppe zufällig ausgewählter, ständig verfügbarer Knoten ab, die der Kontaktbeziehung zugeordnet sind. Die Zusammensetzung dieser Gruppe wird im Lauf der Zeit erneuert, selbständig und ohne Mitwirkung der Endgeräte, die beide offline sein können. Ein privater Index, der selbst redundant gespeichert und für Aussenstehende unlesbar ist, erlaubt es dem Empfänger, die Kopien auch dann zu finden, wenn der Absender inzwischen abgeschaltet hat. Erst die authentifizierte Empfangsbestätigung des Empfängers löst die Löschung aller Kopien aus.

Getrennte Verwaltung. Ein Knoten darf dem Netzwerk nur mit einer kurzlebigen Betriebserlaubnis dienen, die eine separate Stelle ausstellt. Diese Stelle kann fehlerhafte oder feindliche Knoten ausschliessen und erhält nie Nachrichteninhalte, Kontaktlisten oder Identitäten von Personen. Lizenzierung und Zahlung sind auf dieselbe Weise von der Kommunikation getrennt.

Geschlossene Netze für Organisationen. Eine Organisation kann innerhalb derselben Architektur ein eigenes geschlossenes Netz betreiben, mit selbst zugelassenen Knoten, signierten Verwaltungshandlungen, Vier-Augen-Freigabe für kritische Schritte und einem manipulationssicheren Prüfprotokoll.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Öffentlich.

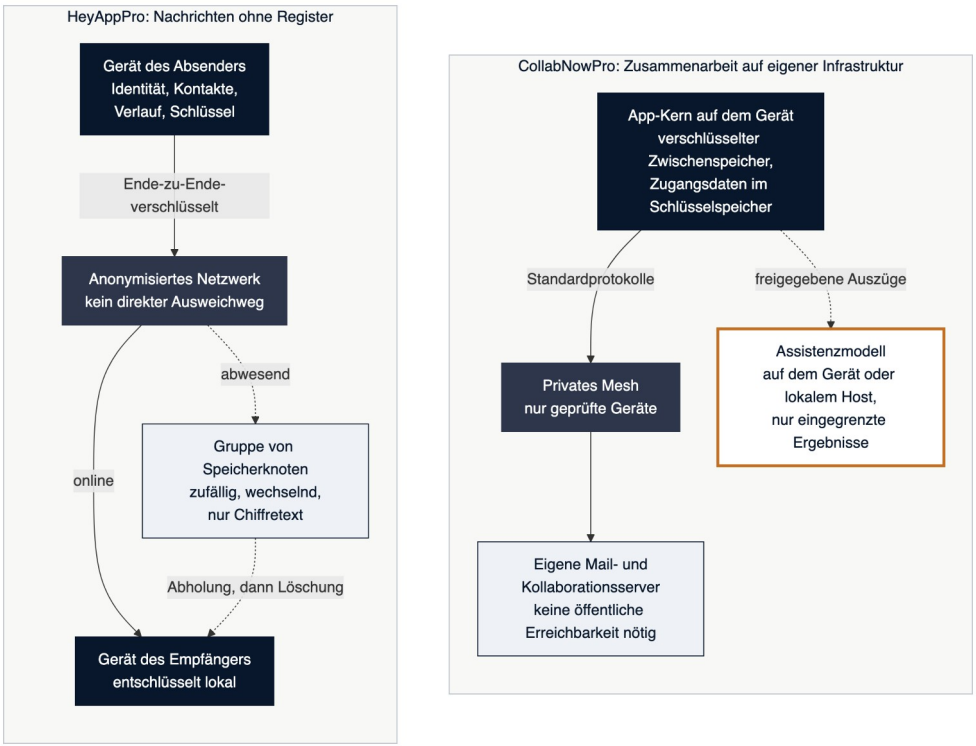


Abbildung 2: Funktionsprinzip der beiden Technologiedemonstratoren.

HeyAppPro transportiert Ende-zu-Ende-verschlüsselte Nachrichten über das anonymisierte Netzwerk und legt sie für abwesende Empfänger als Chiffretext auf einer wechselnden Gruppe von Knoten ab. CollabNowPro verbindet einen Anwendungskern auf dem Gerät über ein privates Mesh mit Mail- und Kollaborationsservern, die die Organisation selbst kontrolliert, und beschränkt den KI-Assistenten auf freigegebene Auszüge. Eigene Darstellung, ohne Protokolldetails.

4.3 Vorteile

- **Kein zentrales Angriffsziel.** Es gibt kein Teilnehmerregister, keinen zentralen Nachrichtenspeicher und kein zentrales Protokoll darüber, wer mit wem kommuniziert. Ein Angreifer, der einen Knoten kompromittiert, erhält Bruchstücke von Chiffretext ohne Kenntnis der Personen dahinter.
- **Geringerer Wert von Herausgabeanordnungen gegen Vermittler.** Kein Betreiber und kein Knoten hält lesbare Inhalte, Kontaktlisten oder Inhaltsschlüssel. Was bei einem Vermittler nicht vorhanden ist, kann er nicht herausgeben.
- **Schutz der Metadaten.** Weder die Knoten noch ein Beobachter des Netzanschlusses der Nutzenden erfahren die Netzwerkadresse des Gegenübers. Identitäten sind nicht an Telefonnummern gebunden.
- **Segmentierte Speicherung.** Gespeicherte Nachrichten existieren nur als verschlüsselte Kopien auf mehreren unabhängigen Knoten, die im Lauf der Zeit wechseln, und werden nach bestätigter Zustellung gelöscht.
- **Zuverlässige Zustellung ohne zentrale Warteschlange.** Nachrichten erreichen Empfänger, die offline waren, auch wenn der Absender inzwischen offline gegangen ist.
- **Kontrolle über das Gerät.** Lokale Daten bleiben verschlüsselt, und die App sperrt sich, sobald sie in den Hintergrund wechselt. Die automatische Löschung von Gesprächen nach kurzer Aufbewahrungsdauer ist als weitere Anforderung spezifiziert.
- **Steuerbarer Betrieb.** Die Betriebsstelle kann einzelne Knoten oder ein ganzes Netz stoppen, ohne dadurch Nutzerdaten lesen oder löschen zu können.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Öffentlich.

- **Ein speichersicherer Kern auf allen Plattformen.** Derselbe Kern bedient Desktop- und Mobilsysteme, was den zu prüfenden Code verkürzt.

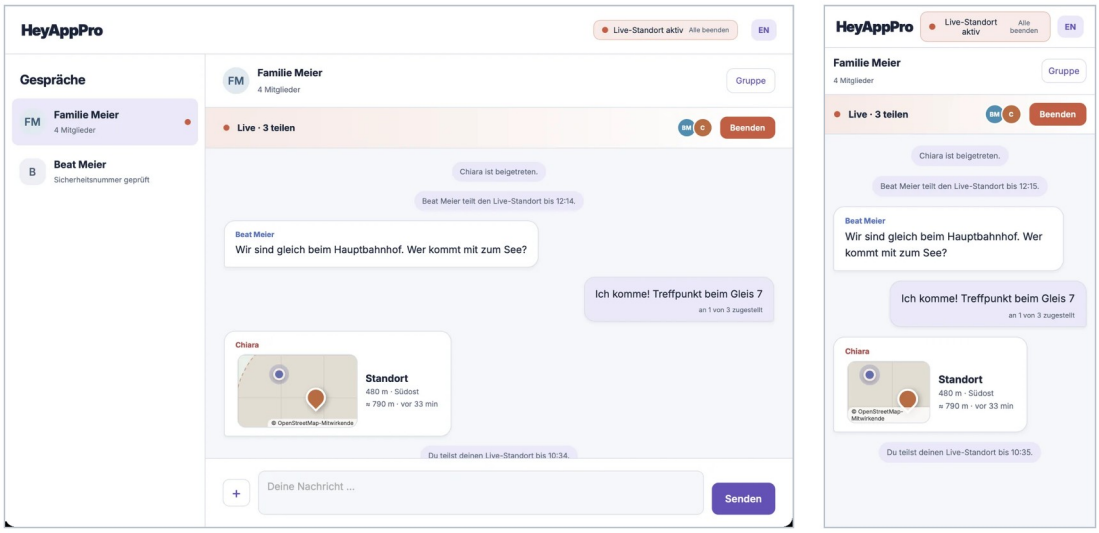


Abbildung 3: HeyAppPro auf dem Desktop und auf einem Telefon.

Das Gruppengespräch zeigt den Zustellstatus einer Nachricht und einen geteilten Live-Standort. Aufnahmen der deutschsprachigen Anwendungsoberfläche mit Beispieldaten.

4.4 Umsetzungsstand und Nachweise

Gemäss den Fortschrittsaufzeichnungen des Projekts ist Folgendes nachgewiesen. Nachrichten werden über das anonymisierte Netzwerk zwischen Desktop- und Mobilgeräten ausgetauscht. Eine laufende Testflotte von Knoten auf mehreren unabhängigen Hosts ist in Betrieb, und am 8. November 2026 wurde ein physisches Tablet mit allen Knoten dieser Flotte verbunden. Automatische Ausstellung, Verwendung, Widerruf und Ablauf von Zulassungsrichtlinien wurden in einem separaten Test über das reale anonymisierte Netzwerk überprüft. Eine Flottensimulation mit 99 Clients, die Texte, Bilder und Standorte austauschen, sich planmässig aus- und einschalten und jede Zustellung überprüfen, ist als Entwicklungswerkzeug umgesetzt. Die automatisierten Testsuiten des Projekts waren beim letzten erfassten Lauf am 10. November 2026 erfolgreich. Builds bestehen für macOS, iOS, Android, Windows und Linux.

Umgesetzt und lokal getestet, aber im Live-Betrieb noch nicht abgenommen sind geschlossene Kundennetze mit signierter Verwaltung und die zugehörige Lizenzierung. Noch ausstehend sind die vollständige Abnahme auf physischen Android-Geräten, signierte und reproduzierbare Releases für alle Plattformen, der Langzeitbetrieb der selbständigen Knotenerneuerung in grossem Massstab sowie ein unabhängiges Sicherheitsaudit. Die projekteigenen Dokumente halten fest, dass noch kein Meilenstein formell als Produkt abgenommen ist.

5. Technologiedemonstrator 2: CollabNowPro

5.1 Zweck

Nachrichtenaustausch ist ein Teil der digitalen Arbeit. Der grössere Teil besteht aus Mail, Kalendern, Kontakten, Aufgaben, Notizen und Dateien, die heute typischerweise als Paket eines Hyperscale-Cloud-Anbieters bezogen werden. CollabNowPro vereint diese Funktionen und einen KI-Assistenten in einer einzigen Anwendung für Mobilgeräte und den Desktop und arbeitet mit Infrastruktur, die die

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Öffentlich.

Organisation selbst kontrolliert. Ein Konto bei einem Anbieter von Cloud-Paketen ist nicht erforderlich. Ein bestehendes Groupware-System eines Unternehmens kann als zusätzliches Konto angebunden werden, wo eine Organisation noch darauf angewiesen ist.

5.2 Funktionsprinzip

Ein Kern, offene Protokolle. Ein einziger Anwendungskern, geschrieben in einer speichersicheren Sprache, enthält die Logik für Mail, Kalender, Kontakte, Aufgaben, Notizen, Dateien, Suche und Erinnerungen. Er spricht die offenen Standardprotokolle für diese Funktionen, sodass die Daten in Formaten und auf Servern bleiben, die die Organisation jederzeit verlagern kann. Die Benutzeroberflächen für Telefon, Tablet und Desktop sind dünne Schichten über diesem Kern.

Privates Mesh. In der Referenzeinrichtung erreicht die Anwendung die Mail- und Kollaborationsserver der Organisation nur über ein verschlüsseltes privates Mesh, zu dem jedes Gerät einzeln zugelassen wird. Die Server müssen deshalb nicht im öffentlichen Internet erreichbar sein. Ist dieser Modus aktiv, verlangt die Anwendung eine überprüfte Mesh-Verbindung und weicht nie auf einen direkten Weg aus.

Schutz auf dem Gerät. Das Gerät hält nur einen verschlüsselten Zwischenspeicher kürzlich verwendeter Daten für die Offline-Arbeit. Zugangsdaten der Konten liegen im geschützten Schlüsselspeicher des Betriebssystems. Offline vorgenommene Änderungen werden als ausstehend markiert und später mit Versionsprüfung übertragen, und eine Aktion gilt erst als erledigt, wenn der Server sie bestätigt hat.

Ein Assistent unter der Kontrolle der Anwendung. Der Assistent kann in einem Chat über alle Funktionen hinweg lesen, zusammenfassen und Aktionen vorbereiten; der Entwurf sieht auch Sprachbedienung vor. Die entscheidende Gestaltungsentscheidung betrifft den Ort der Kontrolle. Die Anwendung, nicht das Modell, führt Datenzugriffe und Aktionen aus. Das Modell erhält nur die für die Aufgabe freigegebenen Auszüge und nie die Zugangsdaten der Konten. Nutzende legen Bereiche fest, die bestimmen, welche Kalender, Adressbücher, Mailordner und Listen der Assistent lesen oder ändern darf. Jede Änderung erscheint als Karte zur Bestätigung. Das Modell läuft auf dem Gerät oder auf Hardware im eigenen Besitz der Organisation. Ein externer Modelldienst wird nur verwendet, wenn die Nutzerin oder der Nutzer ihn ausdrücklich auswählt; ein automatisches Ausweichen auf ein Cloud-Modell gibt es nicht.

5.3 Vorteile

- **Daten bleiben unter der eigenen Rechtsordnung der Organisation.** Keine Drittplattform speichert oder verarbeitet die Inhalte. Die Frage, welches ausländische Gesetz für den Anbieter gilt, stellt sich nicht, weil sich kein solcher Anbieter im Datenweg befindet.
- **Keine öffentliche Angriffsfläche.** Server, die nur über das private Mesh erreichbar sind, sind automatisiertem Massenscannen und Massenausnutzen entzogen.
- **Segmentierung nach Eigentümer.** Die Daten jeder Organisation bleiben in deren eigenen Systemen und werden nicht mit denen anderer Kunden auf einer gemeinsamen Plattform gebündelt. Ein Fehler in einer Installation legt keine andere offen.
- **KI-Unterstützung ohne Datenabfluss.** Mit dem Modell auf dem Gerät oder auf lokaler Hardware werden sensible Inhalte nicht an einen externen KI-Dienst gesendet, und der Assistent handelt nur in Bereichen, die die Nutzenden freigegeben haben.
- **Eine Anwendung statt vieler.** Mail, Termine, Aufgaben, Kontakte, Notizen und Dateien teilen eine Suche und eine Übersicht. Der Assistent macht aus wiederkehrender mehrstufiger Arbeit eine einzige bestätigte Anweisung.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Öffentlich.

- **Keine Herstellerbindung.** Offene Protokolle und selbst betriebene Server lassen der Organisation die Freiheit, Komponenten zu wechseln.
- **Volle manuelle Kontrolle.** Alles bleibt auch ohne den Assistenten direkt nutzbar.

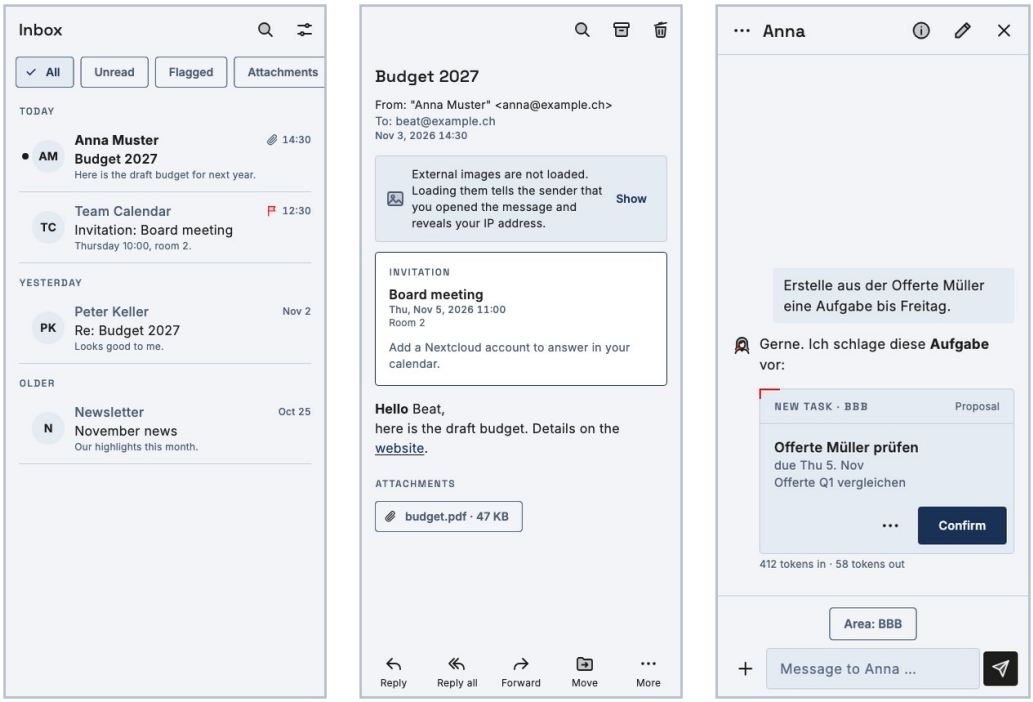


Abbildung 4: CollabNowPro auf einem Telefon.

Von links nach rechts: der Posteingang, eine Nachricht mit blockierten externen Bildern und einer Besprechungseinladung sowie der Assistent, der eine Aufgabe als Karte vorschlägt, die die Nutzerin oder der Nutzer bestätigt. Aufnahmen der Anwendungsoberfläche aus der Testsuite des Projekts mit erfundenen Beispieldaten.

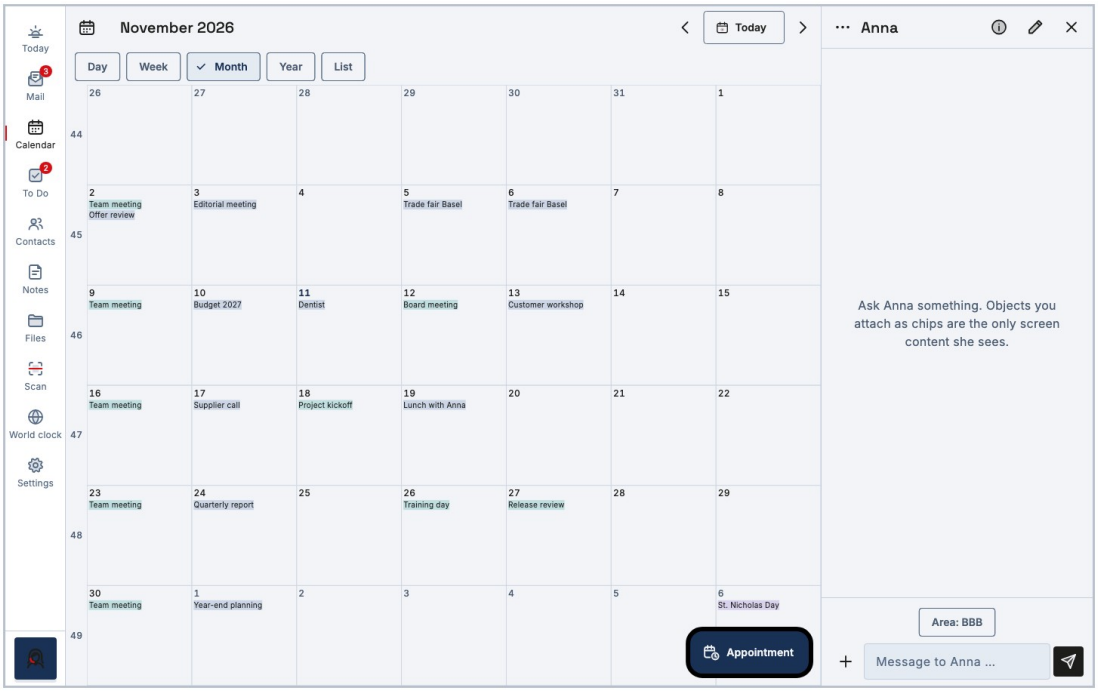


Abbildung 5: CollabNowPro auf dem Desktop.

Der Kalender in der Monatsansicht, links die Navigationsleiste und rechts der Assistent als Seitenleiste, der als einzigen Bildschirminhalt die Objekte sieht, die die Nutzerin oder der Nutzer anhängt. Aufnahme der Anwendungsoberfläche im breiten Layout, erzeugt mit den Testwerkzeugen des Projekts und erfundenen Beispieldaten.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Öffentlich.

5.4 Umsetzungsstand und Nachweise

Die Desktop-Anwendung besteht mit einem breiten, getesteten Umfang an Mail-, Kalender-, Kontakt-, Aufgaben-, Notiz- und Dateifunktionen. Die mobile Anwendung läuft seit dem 10. November 2026 auf einem physischen Tablet, das über das private Mesh mit den Servern der Organisation verbunden ist. Gerätetests am 11. November 2026 bestätigten, jeweils mit Überprüfung auf dem Server, das Lesen und Bearbeiten von Mail, Kalenderansichten und Kalendereinträge sowie das Anlegen, Ändern und Löschen von Aufgaben, Kontakten, Notizen und Ordnern. Der letzte erfasste Lauf der automatisierten Tests des Kerns verlief ohne Fehler. Tests, die die Live-Serverumgebung erfordern, werden separat geführt.

Zu den vom Projekt erfassten offenen Punkten gehören die langsame globale Suche und das langsame Laden der Kontakte auf dem Tablet, der Umgang mit einer ausgehenden Nachricht, deren Zustellstatus unbekannt ist, die vollständige Abnahme auf Android-Geräten, die Härtung der Releases und eine unabhängige Sicherheitsprüfung.

5.5 Versiegelte Mail

Eine Funktion verbindet die beiden Demonstratoren. Beide Anwendungen bieten die Möglichkeit, E-Mails in versiegelter Form zu senden. Eine versiegelte Nachricht wird auf Grundlage des OpenPGP-Standards Ende-zu-Ende verschlüsselt. [Q28] Schlüssel werden im Hintergrund automatisch erzeugt und verwaltet und nur zwischen den Korrespondenzpartnern ausgetauscht, ohne Veröffentlichung in einem Verzeichnis. Versiegelte Nachrichten laufen ausschliesslich über das anonymisierte Netzwerk durch Knoten der bestehenden Flotte. Diese Knoten halten jede Nachricht eine zufällige Zeit lang zurück und verändern ihre scheinbare Grösse, sodass selbst grossflächige statistische Beobachtung Mühe hat, Eingehendes und Ausgehendes einander zuzuordnen. Eine Empfangsbestätigung kehrt auf demselben Weg zurück und erscheint beim Absender als Häkchen. Die Nutzenden sehen von dieser Mechanik nichts, nur die Möglichkeit, sicher zu senden, und die Empfangsbestätigung. Eine für die versiegelte Zustellung markierte Nachricht wird nie ohne ausdrückliche Entscheidung des Absenders unverschlüsselt versendet.

Das Prinzip hinter dem Entwurf ist das von Chaum beschriebene Mix-Konzept. [Q08] Seine Grenzen sind die in Abschnitt 3.3 genannten, und der Entwurf selbst schliesst Versprechen absoluter Anonymität aus.

6. Diskussion

6.1 Wie die Demonstratoren den vier Druckfaktoren begegnen

Druckfaktor	HeyAppPro	CollabNowPro
KI-gestützte Schwachstellensuche	Kein zentrales System, dessen Kompromittierung alle Nutzenden offenlegt; Knoten halten nur Bruchstücke von Chiffretext; speichersicherer Kern	Server brauchen keine öffentliche Erreichbarkeit; eine Installation pro Organisation; speichersicherer Kern; Zugangsdaten nur im Schlüsselspeicher des Geräts
Quantencomputer	Weniger Punkte, an denen sich Chiffretext ansammelt; gespeicherte Kopien sind verteilt und werden nach der Zustellung gelöscht; Post-Quanten-Algorithmen noch nicht im Einsatz	Kein Chiffretextarchiv bei einem Dritten; Mesh-Verkehr bleibt zwischen eigenen Geräten und eigenen Servern; Post-Quanten-Algorithmen noch nicht im Einsatz
Grenzüberschreitender behördlicher Zugriff	Kein Vermittler hält lesbare Inhalte, Kontaktlisten oder ein Teilnehmerregister	Kein Drittanbieter im Datenweg; Daten bleiben bei der Organisation, unter ihrer eigenen Rechtsordnung
Innentäter- und Betreiberrisiko	Verwaltung von der Kommunikation getrennt; signierte Handlungen, Vier-Augen-Freigabe, Prüfprotokoll	Assistent auf freigegebene Bereiche und Auszüge beschränkt; jede Änderung erfordert Bestätigung

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Öffentlich.

6.2 Restrisiken und Grenzen

Quantenresistenz ist nicht erreicht. Keiner der beiden Demonstratoren verwendet derzeit Post-Quanten-Algorithmen für Schlüsselvereinbarung oder Signaturen, und das anonymisierte Netzwerk selbst stützt sich auf klassische Public-Key-Verfahren. Die Architektur verringert, wie viel Chiffretext ein Angreifer an einem einzelnen Punkt sammeln kann, und senkt damit den Ertrag von Harvest Now, Decrypt Later. Sie beseitigt die Bedrohung nicht. Versiegelte Mail beruht auf einem Standard, dessen gängige Schlüsseltypen ebenfalls quantenanfällig sind. Die Umstellung auf die standardisierten Post-Quanten-Verfahren innerhalb des von NIST gesetzten Zeitplans ist deshalb notwendig. [Q03], [Q17]

Anonymität ist nicht absolut. Ein Angreifer, der beide Enden einer Verbindung oder grosse Teile des Netzwerks über lange Zeit beobachtet, kann Verkehr korrelieren. [Q24] Bei wenigen Nutzenden ist die Menge der Personen, unter denen sich eine Person verbirgt, klein. Grössen und Zeitpunkte bleiben für die beteiligten Knoten in grober Form sichtbar.

Segmentierte Speicherung hat ein Fehlermodell. Die Replikation über eine kleine Gruppe von Knoten übersteht den Ausfall einzelner Knoten. Sie übersteht keine böswillige Mehrheit, wofür byzantinisch fehlertolerante Protokolle mit mehr Replikaten nötig wären. [Q29] Eine offene Teilnahme würde zudem Angreifer einladen, viele Knoten unter falschen Identitäten zu betreiben. [Q30] HeyAppPro begegnet dem mit der Zulassung von Knoten durch eine zentrale Stelle.

Die zentrale Betriebsstelle ist eine bewusste Abhängigkeit. Sie löst das Zulassungsproblem und schafft zugleich eine Abhängigkeit für Verfügbarkeit und Vertrauen. Sie kann keine Nachrichten lesen, aber sie kann das Netz stoppen.

CollabNowPro ist auf Server angewiesen. Die Architektur verlagert die Server aus der öffentlichen Erreichbarkeit in die eigenen Hände der Organisation. Sie beseitigt sie nicht. Innerhalb einer Organisation bleiben die Kollaborationsdaten auf deren eigenen Systemen gebündelt, und die Organisation trägt die Betriebspflicht, die sonst ein Cloud-Anbieter übernähme. Gewöhnliche E-Mails an externe Empfänger laufen weiterhin auf dem üblichen Weg über deren Anbieter.

Die Endgeräte bleiben entscheidend. Ist ein Gerät kompromittiert oder sein Betriebssystem manipuliert, können entschlüsselte Inhalte dort abgegriffen werden. Bildschirmfotos, schwache Passwörter und das Gerät des Empfängers liegen ausserhalb der Kontrolle beider Anwendungen. Mobile Betriebssysteme beschränken zudem Hintergrundaktivität, was die Zustellung verzögern kann.

Die Bestätigung durch Dritte steht noch aus. Beide Demonstratoren sind funktionierende Software, doch keiner hat ein unabhängiges Sicherheitsaudit durchlaufen, und die Geräteabnahme ist unvollständig. Ihre Schutzversprechen sind Entwurfseigenschaften, gestützt durch die projekteigenen Tests, keine zertifizierten Garantien.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Öffentlich.

6.3 Gegenpositionen

Die Argumente für zentrale Plattformen sind nicht schwach, und sie sollen genannt werden. Grosse Anbieter beschäftigen Sicherheitsteams und beheben Fehler in einem Tempo, mit dem kleine Organisationen nicht mithalten können. Gerade die KI-Systeme, die Schwachstellen finden, werden zuerst Verteidigern zur Verfügung gestellt, mit dem erklärten Ziel, kritische Software zu reparieren, bevor Angreifer dieselbe Fähigkeit nutzen können. [Q11] Selbst betriebene Infrastruktur, die vernachlässigt wird, kann weniger sicher sein als eine professionell betriebene Cloud. Dezentralisierung kostet zudem Bedienkomfort und Leistung: Ein anonymisiertes Netzwerk ist langsamer als eine direkte Verbindung, und wer das einzige Geheimnis verliert, verliert den Zugang zu den Daten, weil kein Anbieter es zurücksetzen kann.

Diese Einwände widerlegen die Argumentation nicht. Sie bestimmen ihren Geltungsbereich. Die hier beschriebene Architektur beruht nicht auf der Annahme, ihre eigene Software sei fehlerfrei. Sie beruht darauf, zu begrenzen, was ein Fehler, ein aufgezeichneter Datenstrom oder eine Anordnung offenlegen kann. Für Kommunikation, deren Vertraulichkeit über viele Jahre und gegenüber fähigen Angreifern bestehen muss, ist die Schadensbegrenzung die robustere Strategie. Bei Daten geringer Schutzwürdigkeit mag der Komfort zentraler Dienste durchaus überwiegen.

7. Schlussfolgerung und Empfehlungen

KI-gestützte Schwachstellensuche, das absehbare Ende der heutigen Public-Key-Kryptografie und grenzüberschreitende Zugriffsrechte sind voneinander unabhängige Entwicklungen, die auf dieselbe strukturelle Schwäche treffen: die zentrale Plattform, die Identitäten, Inhalte, Schlüssel und Metadaten an einem Ort hält. Diese Plattform weiter zu härten, behandelt das Symptom. Die Alternative ist eine Architektur, die sie nicht benötigt: Ende-zu-Ende-Verschlüsselung mit Schlüsseln nur auf den Endgeräten, Transport über ein anonymisiertes Netzwerk, segmentierte Datenhaltung, nicht öffentlich erreichbare Server und eine kleine, speichersichere Codebasis.

HeyAppPro und CollabNowPro zeigen, dass sich diese Alternative mit heutigen Mitteln bauen und auf gewöhnlichen Geräten nutzen lässt. HeyAppPro zeigt es für die Kommunikation von Person zu Person ohne jedes Teilnehmerregister. CollabNowPro zeigt es für die tägliche Arbeit einer Organisation, einschliesslich einer KI-Unterstützung, die keine Daten an Dritte sendet. Beide belegen die Machbarkeit. Die Produktreife ist noch nachzuweisen.

Aus der Analyse folgen fünf Empfehlungen.

1. **Unabhängige Sicherheitsaudits in Auftrag geben** für beide Demonstratoren, einschliesslich des anonymisierten Transports, der Speicher- und Erneuerungsmechanismen und der Verwaltungsfunktionen, und die Ergebnisse in geeigneter Form veröffentlichen.
2. **Die Post-Quanten-Umstellung jetzt planen.** Standardisierte Post-Quanten-Schlüsselvereinbarung in hybrider Form zuerst für den Inhaltsschutz und langlebige gespeicherte Daten einführen und alle Protokolle so gestalten, dass sich Algorithmen austauschen lassen.
3. **Die Geräte- und Live-Abnahme abschliessen**, insbesondere auf physischen Android-Geräten, für geschlossene Kundennetze im Live-Betrieb und für die langfristige selbständige Erneuerung der Speichergruppen unter Last.
4. **Die Segmentierung in CollabNowPro ausbauen.** Prüfen, wie sich Kollaborationsdaten innerhalb einer Organisation weiter aufteilen lassen, sodass die Kompromittierung eines einzelnen Servers weniger offenlegt.

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Öffentlich.

5. **Die Grenzen so klar kommunizieren wie die Vorteile.** Schutzziele, Angreifermodell und Restrisiken gehören in jede Produktbeschreibung. Absolute Versprechen von Anonymität oder Sicherheit sind zu vermeiden.

Quellenverzeichnis

Online-Quellen wurden, sofern nicht anders vermerkt, am 11. November 2026 abgerufen. Die Quellen [Q04], [Q19], [Q21], [Q22], [Q23], [Q29] und [Q30] wurden zuletzt am 19. oder 20. Oktober 2026 abgerufen. Herstellerpublikationen sind Selbstauskünfte.

[Q01] Johnson, D.; Bouron, J.; Zielman, A.; Kudrjavets, G. Kernel CVEs at AWS Scale: Two Years of Empirical Findings. Linux Plumbers Conference 2026, Prague, presentation slides. https://lpc.events/event/20/contributions/2373/

[Q02] Larabel, M. OpenAI Finds 948 Local Privilege Escalation Bugs In The Linux Kernel. Phoronix, November 5, 2026. Trade report on OpenAI, A thousand fewer paths to root, November 4, 2026; the original publication could not be retrieved by automated access on November 11, 2026. https://www.phoronix.com/news/OpenAI-948-Linux-LPE-Bugs

[Q03] Moody, D.; Perlner, R.; Regenscheid, A.; Robinson, A.; Cooper, D. Transition to Post-Quantum Cryptography Standards. NIST Internal Report 8547, final, October 2026. https://doi.org/10.6028/NIST.IR.8547

[Q04] United States Code. 18 U.S.C. § 2713, Required preservation and disclosure of communications and records, added by Pub. L. 115-141 (CLOUD Act), March 23, 2018. https://uscode.house.gov/us/usc/119-118/t18/s2713/

[Q05] Netzwoche. Update: Zürcher Pensionskasse verschiebt Softwareumstellung nach Cyberangriff. Running coverage of the data leak at PK Softech and Publica, with reference to the Tages-Anzeiger, first published October 8, 2026, updated November 4, 2026. https://www.netzwoche.ch/news/2026-10-08/bundespensionskasse-publica-meldet-datenabfluss

[Q06] TechCrunch. Leaks, data breaches, and ransom notes: The worst hacks of 2026 so far. First published June 8, 2026, updated September 15, 2026. https://techcrunch.com/2026/09/15/the-worst-hacks-and-breaches-of-2026-so-far/

[Q07] Federal Bureau of Investigation, Internet Crime Complaint Center. Internet Crime Report 2025. 2026. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[Q08] Chaum, D. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM 24(2), 1981. https://doi.org/10.1145/358549.358563

[Q09] The Linux Kernel Organization. CVEs. The Linux Kernel documentation, process guide. https://www.kernel.org/doc/html/latest/process/cve.html

[Q10] TechSpot. AI is finding thousands of bugs in Linux, and maintainers can barely keep up. September 2026. Trade report on data published by the Linux stable kernel maintainer. https://www.techspot.com/news/113716-ai-finds-1500-vulnerabilities-linux-kernel-linus-torvalds.html

[Q11] Anthropic. Project Glasswing. April 7, 2026. https://www.anthropic.com/glasswing

[Q12] Federal Office for Cybersecurity (BACS). Halbjahresbericht 2026/1. Swiss Confederation, published August 24, 2026. https://www.bacs.admin.ch/de/hjb-26-de1

[Q13] Netzwoche. Update: Westschweizer Radiologienetzwerk bestätigt Datendiebstahl nach Cyberangriff. May 7, 2026, updated July 7, 2026. https://www.netzwoche.ch/news/2026-05-07/cyberangriff-legt-westschweizer-radiologie-netzwerk-erneut-lahm

[Q14] Netzwoche. Cyberangriff auf Waadtländer Firma legt sensible Sicherheitsdaten offen. October 8, 2026, with reference to Le Temps. https://www.netzwoche.ch/news/2026-10-08/cyberangriff-auf-waadtlaender-firma-legt-sensible-sicherheitsdaten-offen

[Q15] Cyber Safety Review Board. Review of the Summer 2023 Microsoft Exchange Online Intrusion. U.S. Department of Homeland Security, released April 2, 2024. https://www.cisa.gov/resources-tools/resources/CSRB-Review-Summer-2023-MEO-Intrusion

[Q16] Federal Bureau of Investigation; Cybersecurity and Infrastructure Security Agency. Joint Statement from FBI and CISA on the People's Republic of China (PRC) Targeting of Commercial Telecommunications Infrastructure. November 13, 2024. https://www.cisa.gov/news-events/news/joint-statement-fbi-and-cisa-peoples-republic-china-prc-targeting-commercial-telecommunications

[Q17] National Institute of Standards and Technology. Module-Lattice-Based Key-Encapsulation Mechanism Standard. FIPS 203, August 13, 2024. https://doi.org/10.6028/NIST.FIPS.203

[Q18] Gidney, C. How to factor 2048 bit RSA integers with less than a million noisy qubits. arXiv:2505.15917, May 21, 2025. https://arxiv.org/abs/2505.15917

[Q19] Swiss Confederation. Federal Act on the Surveillance of Post and Telecommunications (BÜPF/SPTA) of March 18, 2016, SR 780.1, status as of September 1, 2023; official German text. https://www.fedlex.admin.ch/eli/cc/2018/31/de

[Q20] Apple. Apple can no longer offer Advanced Data Protection in the United Kingdom to new users. Apple Support. https://support.apple.com/en-us/122234

[Q21] Perrin, T.; Marlinspike, M.; Schmidt, R. The Double Ratchet Algorithm. Signal Specifications, Revision 4, November 4, 2025. https://signal.org/docs/specifications/doubleratchet/

[Q22] Cohn-Gordon, K.; Cremers, C.; Dowling, B.; Garratt, L.; Stebila, D. A Formal Security Analysis of the Signal Messaging Protocol. Journal of Cryptology 33, 2020. https://doi.org/10.1007/s00145-020-09360-1

[Q23] Unger, N.; Dechand, S.; Bonneau, J.; Fahl, S.; Perl, H.; Goldberg, I.; Smith, M. SoK: Secure Messaging. IEEE Symposium on Security and Privacy, 2015. https://doi.org/10.1109/SP.2015.22

[Q24] Das, D.; Meiser, S.; Mohammadi, E.; Kate, A. Anonymity Trilemma: Strong Anonymity, Low Bandwidth Overhead, Low Latency, Choose Two. IEEE Symposium on Security and Privacy, 2018. https://doi.org/10.1109/SP.2018.00011

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Öffentlich.

[Q25] Saltzer, J. H.; Schroeder, M. D. The Protection of Information in Computer Systems. Proceedings of the IEEE 63(9), 1975. https://doi.org/10.1109/PROC.1975.9939

[Q26] Rose, S.; Borchert, O.; Mitchell, S.; Connelly, S. Zero Trust Architecture. NIST Special Publication 800-207, August 2020. https://doi.org/10.6028/NIST.SP.800-207

[Q27] Cybersecurity and Infrastructure Security Agency; National Security Agency; Federal Bureau of Investigation; international partner agencies. The Case for Memory Safe Roadmaps. December 2023. https://www.cisa.gov/resources-tools/resources/case-memory-safe-roadmaps

[Q28] Wouters, P. (ed.); Huigens, D.; Winter, J.; Niibe, Y. RFC 9580: OpenPGP. IETF, July 2024. https://www.rfc-editor.org/rfc/rfc9580.html

[Q29] Castro, M.; Liskov, B. Practical Byzantine Fault Tolerance. 3rd Symposium on Operating Systems Design and Implementation (OSDI), 1999. https://www.usenix.org/conference/osdi-99/practical-byzantine-fault-tolerance

[Q30] Douceur, J. R. The Sybil Attack. Peer-to-Peer Systems, IPTPS 2002, Lecture Notes in Computer Science 2429. https://doi.org/10.1007/3-540-45748-8_24

© 2026 Beat W. Meier · Alle Rechte vorbehalten.

Status: Öffentlich.