Nina Gerber, Verena Zimmermann, Birgit Henhapl, Sinem Emeröz, Melanie Volkamer, Tobias Hilt

Nutzerwahrnehmung der Ende-zu-Ende-Verschlüsselung in WhatsApp

Die Einführung einer Ende-zu-Ende-Verschlüsselung in WhatsApp im Jahr 2016 hat eine wichtige Kritik an dem verbreiteten Instant-Messaging-Dienst entkräftet. Wie aber bewerten Benutzer die Verschlüsselung? Hat sich dadurch das Vertrauen der Nutzer in den Dienst geändert? Diesen Fragen ging die im Folgenden vorgestellte Untersuchung nach.

Einleitung

Ende-zu-Ende-Verschlüsselung (E2E) ist eine wirksame Maßnahme gegen Datenschutzverletzungen, die im Jahr 2016 von WhatsApp für alle Nutzer (der aktuellen App-Version) eingeführt wurde. Es ist jedoch unbekannt, wie Endnutzer diese Änderung wahrgenommen haben: Ob sie WhatsApp als Anbieter von E2E-Verschlüsselung vertrauen und wie sich ihr Kommunikationsverhalten verändert hat. Um dies zu erfahren, haben wir semi-strukturierte Interviews mit zwanzig WhatsApp-Nutzern geführt. Dabei stellten wir fest, dass etwa die Hälfte der Teilnehmer annahm, dass ihre Nachrichten auch mit E2E-Verschlüsselung noch gelesen werden können, beispielsweise von Hackern und anderen Kriminellen, staatlichen Institutionen oder Mitarbeitern und Kooperationspartnern von WhatsApp. Viele Teilnehmer identifizierten Absender und Empfänger nach der Einführung der E2E-Verschlüsselung als schwächste Punkte, allerdings gab es auch Probleme mit dem Verständnis von E2E-Verschlüsselung. So dachten Nutzer, dass Nachrichten direkt zwischen zwei Geräten übertragen wurden, ohne weitergeleitet oder auf einem Server gespeichert zu werden, oder interpretierten „Ende-zu-Ende“ zeitlich. Die Mehrheit der Nutzer gab an, dass sie

WhatsApp und deren E2E-Verschlüsselung nicht vertrauen würden und vermuteten Image-begründete Ursachen für die kostenlose Implementierung. Obwohl die meisten Teilnehmer ihr Kommunikationsverhalten nicht änderten, berichteten sie, Schutzstrategien (wie das Versenden sensibler Inhalte über alternative Kanäle) auch nach der Einführung der E2E-Verschlüsselung zu verwenden.

1 WhatsApps Ende-zu-Ende-Verschlüsselung

Der Instant-Messaging-Dienst WhatsApp wurde 2014 von Facebook Inc. übernommen (BBC News Services 2014), was zu Kritik von Datenschützern führte. WhatsApp reagierte darauf mit der Einführung der E2E-Verschlüsselung am 5. April 2016 für alle Nutzer (WhatsApp Inc. 2016a). Nach dem Update auf die neueste Version der Smartphone-App wurde standardmäßig E2E-Verschlüsselung eingestellt, wobei das Protokoll auf dem von Signal basiert (Open Whisper Systems 2013-2016 2016). Die Nutzer wurden über die Änderung mit einer kurzen Textnachricht informiert. WhatsApp hat ein Whitepaper über die Implementierung der E2E-Verschlüsselung veröffentlicht, in dem die technischen Details erläutert werden (WhatsApp Inc. 2016b), der Programmcode wurde jedoch nicht veröffentlicht.

Die E2E-Verschlüsselung in WhatsApp hat allerdings ihre Grenzen. Bspw. wird sie nur in der Smartphone-App unterstützt, so dass die mit einer Desktop- oder Browser-Erweiterung von WhatsApp gesendeten Nachrichten im Klartext unverschlüsselt an die Smartphones der Nutzer weitergeleitet werden, wo die Ver- und Entschlüsselung stattfindet. Die Metadaten (Daten über Empfänger, Absender oder Empfangszeitpunkt), Nutzungs- und Protokollinformationen sowie Geräte- und Verbindungsdaten werden weiterhin von WhatsApp gespeichert (WhatsApp Inc. 2016c). Um Nutzern die Möglichkeit zu geben, die Authentizität des Kommunikationspartners zu überprüfen, wurde die Funktion ‚Sicherheitsnummer bestätigen' implementiert. Diese Nummer repräsentiert den zwischen den Kommunikationspartnern geteilten Schlüssel und ist in Form eines QR-Codes oder einer 60-stelligen Zahlenfolge verfügbar. Diese ändert sich, wenn WhatsApp neu installiert oder das Telefon gewechselt wird.

2 Methodik

Im Folgenden beschreiben wir den methodischen Ansatz in Hinblick auf die Gestaltung des semi-strukturierten Interview-Leitfadens und die Durchführung der Interviews mit insgesamt zwanzig WhatsApp-Nutzern. Die Interviews wurden innerhalb eines zweimonatigen Zeitraums von Mitte Oktober 2016 bis Mitte Dezember 2016 in Deutschland durchgeführt.

2.1 Forschungsfragen

Im Rahmen dieser Studie sollen die folgenden fünf Forschungsfragen (FF) beantwortet werden:

- FF1: Was glauben Nutzer, wie die E2E-Verschlüsselung ihre Nachrichten vor Mitlesern schützt?
- FF2: Wie wird dies durch Verständnisprobleme des E2E-Verschlüsselungskonzepts beeinflusst?
- FF3: Inwieweit vertrauen Nutzer WhatsApp und der E2E-Verschlüsselung?
- FF4: Welche Gründe sehen sie für die Einführung der E2E-Verschlüsselung durch WhatsApp?
- FF5: Haben die Nutzer ihr Messaging-Verhalten nach der Einführung der E2E-Verschlüsselung verändert?

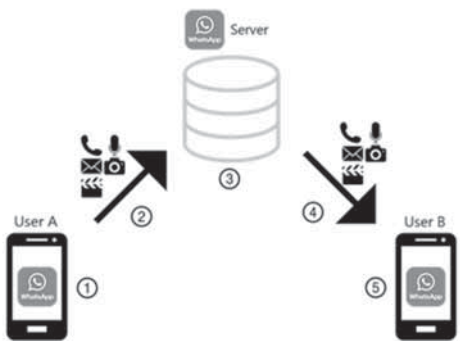
Die Beantwortung dieser Forschungsfragen wird in Abschnitt 3 näher ausgeführt.

2.2 Studien-Design

Jedes Interview bestand aus drei Teilen. Zunächst wurden die Teilnehmer begrüßt und über Studienzweck und -ablauf informiert. Sie wurden anschließend gebeten, das Einverständnisformular sorgfältig zu lesen und zu unterschreiben. Der erste Teil des Interviews erfasste demografische Merkmale und allgemeinen Informationen der Teilnehmer bzgl. ihrer Smartphone- und WhatsApp-Nutzung, um sicherzustellen, dass alle Teilnehmer bereits vor der Einführung der E2E-Verschlüsselung WhatsApp nutzten. Der zweite Teil behandelte das Verständnis der Teilnehmer von E2E-Verschlüsselung. Sie erhielten zwei Zeichnungen, die die unverschlüsselte (Abb. 1) und die E2E-verschlüsselte Übertragung einer Nachricht vom Absender zum Empfänger darstellten. Für jeden Übertragungsschritt sollten die Teilnehmer angeben, ob ihre Nachrichten von Dritten gelesen werden könnten. Wenn sie eine positive Antwort gaben, wurden sie jeweils auch gefragt, wer ihre Nachrichten lesen könnte und wie sehr sie dies störte. Sie wurden zudem gebeten, das Konzept der E2E-Verschlüsselung anhand der Zeichnungen zu erläutern. Der dritte Teil befasste sich mit der Frage, wie Nutzer ihr Messaging-Verhalten in WhatsApp aufgrund der Einführung der E2E-Verschlüsselung geändert haben, z. B. welche Art von Informationen sie über WhatsApp senden.

Gefragt wurde auch nach dem Vertrauen der Nutzer in WhatsApp und ob bzw. wie sich dieses nach der Einführung der E2E-Verschlüsselung geändert hat. Anschließend erhielten alle Teilnehmer, die im zweiten Teil der Studie keine korrekte Erklärung der E2E-Verschlüsselung geliefert hatten, eine Erklärung zur E2E-Verschlüsselung in WhatsApp. Sie wurden anschließend gebeten, ihre Antworten auf die Fragen zu überdenken, wie sich die Einführung der E2E-Verschlüsselung auf ihr Kommunikationsverhalten über WhatsApp ausgewirkt hat.

Abbildung 1 | Nachrichtenübertragung bei WhatsApp



2.3 Ethische Vorgaben

Alle relevanten ethischen Voraussetzungen für die Forschung mit personenbezogenen Daten, die die Ethikkommission unserer Universität[1] zur Verfügung stellt, wurden eingehalten.

2.4 Rekrutierung und Einschreibung

Die Teilnehmer wurden mithilfe des sogenannten „Schneeballsystems" rekrutiert: Zunächst wurden Teilnehmer aus dem Bekanntenkreis ausgewählt. Diese rekrutierten dann weitere Bekannte. Zusätzlich wurden Plakate verwendet, um die Studie weiter zu verbreiten. Die Interviews wurden so lange geführt, bis keine neuen Themen und Probleme in den Interviews mehr genannt wurden. Die Teilnehmer erhielten eine Vergütung von 10 €, jedoch entschied sich etwa die Hälfte der Teilnehmer dafür, auf diese Vergütung zu verzichten. Vor Beginn der Interviews führten wir ein Probeinterview durch, um die Verständlichkeit der Interviewfragen und -materialien zu überprüfen. Infolgedessen wurden kleine Änderungen am Interviewleitfaden vorgenommen.

2.5 Teilnehmer

Insgesamt 20 Nutzer (12 Frauen, 8 Männer) nahmen an unserer Studie teil. Die Teilnehmer waren zwischen 18 und 54 Jahre alt (M=29,95; Med=28; SD=8,94). Ein Teilnehmer war Kryptografie-Experte, alle anderen Teilnehmer hatten weder eine IT-bezogene Ausbildung noch übten sie IT-bezogene Berufe aus. Zehn der Teilnehmer waren Android-Nutzer, neun Teilnehmer nutzten iOS und ein Teilnehmer nutzte Windows 10 als Betriebssystem auf seinem Smartphone. Alle Teilnehmer gaben an, WhatsApp mindestens ein Jahr lang benutzt zu haben.

Im Durchschnitt verwendeten die Teilnehmer drei verschiedene Messenger-Dienste, darunter waren bei allen WhatsApp und der Facebook Messenger. Die höchste Anzahl an verwendeten Messengern wurde vom Kryptografie-Experten angegeben, der acht verschiedene Messenger benutzte. Sieben Teilnehmer gaben an, neben WhatsApp auch andere Messenger mit E2E-Verschlüsselung zu verwenden. Alle Teilnehmer hatten WhatsApp bereits vor der Einführung der E2E-Verschlüsselung genutzt.

2.6 Bewertungsmethodik

Nach der Zustimmung der Teilnehmer wurden alle Interviews aufgezeichnet und transkribiert. Die Transkripte wurden anschließend mithilfe eines Grounded-Theory-Ansatzes (Strauss 1987; Strauss und Corbin 1990) analysiert. Die Interviews dauerten zwischen 33 und 72 Minuten, wobei der Durchschnitt bei 45 Minuten lag.

Wir führten zunächst eine offene Kodierung durch, bei der vier Forscher unabhängig voneinander eine Teilmenge der Transkripte untersuchten, um anhand der Antworten der Teilnehmer relevante Themen zu identifizieren. Diese Themen wurden dann zwischen den vier Forschern diskutiert, was in einer endgültigen Liste von Themen resultierte. Es wurde eine axiale Kodierung verwendet, um Kategorien basierend auf diesen Themen zu bilden und zu gruppieren. Wir identifizierten fünf Gruppen von Kategorien, die jeweils eine Forschungsfrage behandelten:

- (1) Abhörmöglichkeiten
- (2) falsche Vorstellungen bzgl. der E2E-Verschlüsselung
- (3) Vertrauen gegenüber WhatsApp
- (4) vermutete Gründe für die Einführung der E2E-Verschlüsselung und
- (5) Änderungen im Verhalten aufgrund der Einführung der E2E-Verschlüsselung.

Die endgültigen Kategorien wurden in einem gemeinsamen Codebuch niedergeschrieben. Dies wurde von einem weiteren Forscher verwendet, um eine selektive Kodierung durchzuführen, d. h. die Transkripte erneut basierend auf den Kategorien zu kodieren.

3 Ergebnisse

In diesem Abschnitt werden die Ergebnisse der Datenanalyse in Bezug auf die fünf Forschungsfragen vorgestellt.

3.1 FF1 Abhörmöglichkeiten

Um zu beantworten, wie Nutzer die E2E-Verschlüsselung von WhatsApp im Hinblick auf den Schutz vor potenziellen Mitlesern wahrnehmen, fragten wir sie (1) bei welchen Schritten einer Nachrichtenübertragung in WhatsApp Angreifer oder Außenstehende die laufende Konversation mitlesen könnten und (2) wer diese Mitleser sein könnten. Die Teilnehmer beantworteten beide Fragen sowohl für die unverschlüsselte Nachrichtenübertragung als auch für die E2E-verschlüsselte Übertragung. Die Ergebnisse für jeden Übertragungsschritt werden nachstehend beschrieben.

- **Schritt 1 (Absender).** Die Teilnehmer gaben an, dass ihre verschlüsselten und unverschlüsselten Nachrichten bei diesem Schritt hauptsächlich von Umstehenden mit guter Sicht auf das Smartphone gelesen werden könnten.
- **Schritt 2 (Übertragung von Absender zu Server).** Bei der unverschlüsselten Kommunikation gab etwa die Hälfte der Teilnehmer an, dass es leicht wäre, die Nachricht „auf ihrem Weg" abzufangen. Andere wiederum nahmen an, dass das Mitlesen bei diesem Schritt aufgrund des kurzen Zeitrahmens schwieriger sein würde als bei anderen Schritten. Die Teilnehmer glaubten, dass hauptsächlich Hacker und Regierungsinstitutionen in der Lage wären, ihre Nachricht bei diesem Schritt abzufangen. In Bezug auf die verschlüsselte Kommunikation dachten die meisten Teilnehmer, dass es am schwierigsten wäre, Nachrichten in diesem Schritt (zusammen mit Schritt 4) abzufangen.
- **Schritt 3 (Server).** Nur zwei Teilnehmer nahmen an, dass die Nachrichten bei diesem Schritt der unverschlüsselten Kommunikation nicht von anderen gelesen werden konnten. Entweder gingen sie davon aus, dass es einen direkten Pfad zwischen den beiden kommunizierenden Geräten gäbe, so dass Schritt 3 nicht existierte, oder sie nahmen an, dass der Server gut geschützt sei. Die anderen Teilnehmer verdächtigten hauptsächlich mit WhatsApp assoziierte Personen, d. h. Angestellte, Verwaltungspersonal oder Kooperationspartner, ihre Nachrichten lesen zu können. Einige Teilnehmer dachten auch, dass Regierungseinrichtungen Malware verwenden könnten, um ihre Nachrichten in diesem Übertragungsschritt zu lesen. Sie verbanden dieses Vorgehen hauptsächlich mit den Zwecken der

1 https://www.intern.tu-darmstadt.de/gremien/ethikkommisson/index.de.jsp

Strafverfolgung und Terrorabwehr. Hacker wurden ebenfalls als mögliche Mitleser genannt. Etwa die Hälfte der Teilnehmer dachte, dass bei diesem Schritt auch für die verschlüsselte Kommunikation Mitleseangriffe möglich wären.

- **Schritt 4 (Übertragung von Server zu Empfänger).** Diejenigen Teilnehmer, die dachten, dass Nachrichten in Schritt 2 gelesen werden könnten, hatten den gleichen Eindruck in Bezug auf Schritt 4.
- **Schritt 5 (Empfänger).** Ähnlich wie in Schritt 1 erwähnten die Teilnehmer Umstehende als mögliche Mitleser der unverschlüsselten Kommunikation, waren aber zusätzlich besorgt über Personen, denen die Nachricht gezeigt oder weitergeleitet werden könnte. Des Weiteren wurden Menschen mit direktem Zugang zum Smartphone genannt, wie z. B. Personen im selben Haushalt.

3.2 FF2 Verständnisprobleme bzgl. E2E-Verschlüsselung

FF2 beschäftigte sich damit, welches Verständnis Nutzer bzgl. des allgemeinen E2E-Verschlüsselungskonzeptes aufweisen. Tatsächlich gaben nur neun von 20 Teilnehmern korrekterweise an, dass die E2E-Verschlüsselung sie in den Übertragungsschritten 2-4 vor unbefugten Mitlesern schützen soll. Dieses Ergebnis ist nicht weiter überraschend, wenn man bedenkt, dass nur fünf Teilnehmer sich vorab mit dem Thema beschäftigt hatten. Die übrigen Teilnehmer gaben entweder an, die Bedeutung von „E2E-Verschlüsselung" aus der Terminologie abgeleitet oder schlicht geraten zu haben. Insgesamt zeigten sich drei Kategorien von Verständnisproblemen:

- **Nachrichtenübertragung.** Mehrere Teilnehmer hatten ein falsches Verständnis davon, wie sich die E2E-Verschlüsselung auf die Nachrichtenübertragung auswirkt. Einige Teilnehmer gaben an, dass Nachrichten direkt zwischen zwei Geräten übertragen und der Server als Zwischenschritt entfallen würde. Ein anderer Teilnehmer interpretierte die E2E-Verschlüsselung als Nachrichtenübertragung über verschiedene Server hinweg.
- **Interaktion mit der Verschlüsselungsfunktionalität.** Es gab zwei Verständnisprobleme, wie Nutzer mit der E2E-Verschlüsselung in WhatsApp interagieren sollten. Eines davon wurde durch die Benutzeroberfläche verursacht: Einige Teilnehmer verwechselten die Option, einen Kommunikationspartner zu verifizieren, mit einer zur Aktivierung der Verschlüsselung durchzuführenden Handlung. Andere Teilnehmer dachten, die Verschlüsselung würde mittels Verwendung eines Passwortes erfolgen.
- **Wortlaut.** Ein weiteres Problem bezüglich der Formulierung „E2E-Verschlüsselung" stellte der Wortlaut „Ende-zu-Ende" dar. Dieser wurde teilweise als zeitliches Ende der verschlüsselten Kommunikation interpretiert.

3.3 FF3 Vertrauen gegenüber WhatsApp

Das Vertrauen der Nutzer in WhatsApp und seiner E2E-Verschlüsselung ließ sich insgesamt in vier Kategorien abbilden (FF3):

- **Geringes Vertrauen in WhatsApp.** Fünfzehn Teilnehmer bezeichneten ihr Vertrauen in WhatsApp als eher gering, insbesondere im Vergleich zu anderen Messengern wie Telegram, Wire oder Threema. Ein Grund dafür war das fehlende Vertrauen in die Sicherheit der E2E-Verschlüsselung von WhatsApp. Einige Teilnehmer kritisierten die mangelnde Transparenz hinsichtlich der technischen und wirtschaftlichen Struktur von WhatsApp, zum Beispiel im Hinblick auf das Geschäftsmodell und die Verarbeitung der Nutzungsdaten.
- **Hohes Vertrauen in WhatsApp.** Nur fünf Teilnehmer gaben an, WhatsApp aus unterschiedlichen Gründen mehr zu vertrauen als anderen Messenger-Diensten. Einige Teilnehmer verwiesen auf den Erfolg bzw. die große Nutzerbasis von WhatsApp. Andere bezogen sich auf ihre positiven Erfahrungen mit WhatsApp in der Vergangenheit, die sparsame Verwendung personenbezogener Daten und die Datenschutzerklärung von WhatsApp, die im Vergleich zu Facebooks Datenschutzerklärung als „besser" bewertet wurde.
- **Auswirkung der Einführung von E2E-Verschlüsselung auf das Vertrauen**. Die Einführung der E2E-Verschlüsselung hatte sogar einen negativen Einfluss auf das Vertrauen einiger Nutzer

in WhatsApp, da diese annahmen, dass WhatsApp vor der Implementierung der Verschlüsselung nicht sicher war.
- **Misstrauen in die E2E-Verschlüsselung.** Selbst nachdem die Teilnehmer eine Erklärung zum Konzept der E2E-Verschlüsselung erhalten hatten, äußerten viele ein gewisses Misstrauen bzgl. des Schutzes ihrer Nachrichten. Der Experte äußerte Bedenken hinsichtlich möglicher Updates, die die E2E-Verschlüsselung wieder leicht entfernen könnten: „Jeder Entwickler eines Messengers hat die Möglichkeit, ein Update zu veröffentlichen, das vermutlich automatisch installiert wird und einfach die E2E-Verschlüsselung umgehen würde, wodurch die Nachrichten entschlüsselt und im Klartext weitergeleitet werden können."

3.4 FF4 Angenommene Gründe für die Einführung der E2E-Verschlüsselung

Das Misstrauen gegenüber WhatsApp wurde auch in den Aussagen der Teilnehmer zu FF4 deutlich. Insgesamt wurden fünf verschiedene Gründe angegeben, warum WhatsApp eine kostenlose E2E-Verschlüsselung implementiert haben könnte:
- **Wettbewerb mit anderen Messengern**. Nach Ansicht einiger Teilnehmer hatte WhatsApp aufgrund der Übernahme durch Facebook Inc. das Vertrauen der Nutzer verloren und die Einführung der E2E-Verschlüsselung sollte diesem Vertrauensverlust entgegenwirken. Entsprechend dachten die Teilnehmer, dass WhatsApp durch die Einführung der E2E-Verschlüsselung Nutzer behalten oder zurückgewinnen wollte.
- **Finanzielle Leistungen.** Einige Teilnehmer vermuteten, dass WhatsApp die E2E-Verschlüsselung nur kostenlos zur Verfügung stellen konnte, da WhatsApp nun keine Mitarbeiter mehr zum Lesen der nun verschlüsselten Nachrichten bezahlen müsse. Darüber hinaus dachten einige Teilnehmer, dass WhatsApp die E2E-Verschlüsselung eingeführt habe, um andere Unternehmen daran zu hindern, auf WhatsApp-Nachrichten zuzugreifen und Geld mit den erhaltenen Daten zu verdienen.
- **Lockangebot.** Es gab auch Teilnehmer, die ein Lockangebot vermuteten und dachten, dass WhatsApp später eine Gebühr für die E2E-Verschlüsselung verlangen könnte. Andere Teilnehmer waren der Meinung, dass WhatsApp genügend Geldmittel zur Verfügung habe und daher die E2E-Verschlüsselung kostenlos anbieten könne. Diese Teilnehmer vermuteten auch, dass WhatsApp bei jeder Nachricht Gewinne erzielen würde.
- **Gesetzliche Anforderungen erfüllen.** Eine weitere Erklärung war, dass WhatsApp lediglich versucht, gesetzliche Anforderungen oder Standards zu erfüllen. Dementsprechend dachten einige Teilnehmer, WhatsApp versucht die Verantwortung dafür zu umgehen, dass Nutzer illegale Aktivitäten über WhatsApp planen oder durchführen können.
- **Schutz sensibler Daten.** Nur fünf Teilnehmer gingen davon aus, dass WhatsApp eine ausschließlich positive Motivation für die Einführung der E2E-Verschlüsselung hatte. Diese Teilnehmer gaben an, dass WhatsApp aufgrund der Sensitivität der Daten die Verantwortung für deren Schutz übernehmen wolle.

3.5 FF5 Verhaltensänderungen aufgrund der Einführung von E2E-Verschlüsselung

FF5 befasst sich damit, wie die Einführung der E2E-Verschlüsselung das Kommunikationsverhalten der Teilnehmer verändert hat. Wir identifizierten zwei Themenkomplexe, die sich darauf beziehen, ob die Teilnehmer ihr Verhalten bzw. die Anwendung verschiedener Schutzstrategien angepasst haben:
- **Änderungen im Kommunikationsverhalten.** Nur fünf Teilnehmer gaben an, ihr Kommunikationsverhalten nach Einführung der E2E-Verschlüsselung auf WhatsApp geändert zu haben. Sie berichteten, vorzugsweise E2E-verschlüsselte Kanäle für die Kommunikation im Allgemeinen oder zumindest beim Senden sensibler Informationen zu verwenden.
- **Schutzstrategien.** Einige der fünfzehn Teilnehmer, die angaben, ihr Verhalten nicht geändert zu haben, berichteten jedoch weiterhin verschiedene Strategien zum Schutz ihrer privaten Daten einzusetzen. Einer dieser Ansätze bestand darin, die Menge der digital übermittelten sensiblen Informationen zu reduzieren. Andere Ansätze bestanden darin, niemals etwas Sensibles (z. B. Passwörter, Bankdaten) über WhatsApp zu senden bzw. sensible Informationen über andere Kanäle zu übertragen, z. B. per SMS, Brief, Telefon, Mails, persönliche Treffen und alternative Messenger.

4 Diskussion

Die vorgestellte Studie untersuchte die Frage, wie Nutzer die Einführung der E2E-Verschlüsselung in WhatsApp wahrnehmen und wie diese das Vertrauen in WhatsApp bzw. das Kommunikationsverhalten der Nutzer beeinflusst hat.
- **Wahrnehmung von WhatsApps E2E-Verschlüsselung**. Das erste bemerkenswerte Ergebnis in Bezug auf FF1 ist, dass etwa die Hälfte der Teilnehmer der Meinung war, dass das Mitlesen auch nach der Einführung der E2E-Verschlüsselung noch möglich ist, was den Ergebnissen von Abu-Salma et al. (2017a) entspricht. Darüber hinaus dachten mehr Teilnehmer, es sei schwieriger, ihre Nachricht während der Übertragung zwischen Absender/Empfänger und Server abzufangen, als während der Speicherung auf dem Server. Die meisten Teilnehmer nannten Absender und Empfänger als die nach der Einführung der E2E-Verschlüsselung schwächsten Punkte, da Personen in der Umgebung Nachrichten mitlesen könnten und der Empfänger die Nachricht auch nach der Einführung der E2E-Verschlüsselung an Dritte weiterleiten könnte.

Bei der Interpretation der Ergebnisse zur Identität potentieller Mitleser, insbesondere der Rolle staatlicher Institutionen wie Polizei oder Verfassungsschutz, sollte zunächst berücksichtigt werden, dass einige Aussagen hierzu von Medienberichten im Rahmen des Snowden-Effekts beeinflusst worden sein könnten. Da die Interviews in Deutschland stattfanden, könnten auch die öffentlichen Diskussionen über das Recht bestimmter Regierungsinstitutionen auf Zugang zu Daten für die Terrorabwehr eine wichtige Rolle gespielt haben. Des Weiteren sind die in Deutschland lebenden Teilnehmer aufgrund der deutschen Geschichte, dem NS-Regime und der staatlichen Überwachung in der ehemaligen DDR möglicherweise besonders sensibel in Bezug auf das Thema Privatsphäre (Freude und Freude 2016).

In einer von Naiakshina et al. (2016) durchgeführten Studie hatte etwa die Hälfte der Teilnehmer falsche Vorstellungen vom Konzept der E2E-Verschlüsselung. In Bezug auf FF2 könnte dies zu den allgemeinen Zweifeln der Nutzer an der E2E-Verschlüsselung beigetragen haben. Einige der Missverständnisse könnten durch die Benutzeroberfläche von WhatsApp verursacht wer-

den: Mehrere Nutzer verwechselten den Dialog zur Prüfung der Identität eines Kommunikationspartners mit einer Art Schaltfläche zur Aktivierung der E2E-Verschlüsselung. Der Ansatz, die E2E-Verschlüsselung ohne irgendeine Veränderung der Benutzeroberfläche einzuführen, scheint zunächst nutzerfreundlich. Das Missverständnis bzgl. der Schaltfläche könnte jedoch eine Folge der Entscheidung von WhatsApp sein, den zugrundeliegenden Verschlüsselungsprozess vor dem Nutzer zu verbergen. Die Forschungen von Ruoti et al. (2013) und Atwater et al. (2015) legen zwar nahe, dass Nutzer integrierte Lösungen bevorzugen. Dies kann jedoch auch zu Misstrauen in die Anwendung führen (siehe unten), da die Nutzer den Prozess der Verschlüsselung nicht nachvollziehen können. Daher könnte es sinnvoll sein, den Verschlüsselungsprozess für den Nutzer innerhalb der Nutzeroberfläche greifbarer zu machen, z. B. durch Anpassung des Verifizierungsdialogs und die Bereitstellung von mehr Informationen über die E2E-Verschlüsselung.

Der Eindruck, dass sogar E2E-verschlüsselte Kommunikations-Tools anfällig für das Mitlesen seitens sachkundiger Dritter sind, kann jedoch nicht durch einfaches Erhöhen der Sichtbarkeit der Verschlüsselung beseitigt werden. Das fehlende Verständnis des Verschlüsselungskonzepts ist ein grundlegendes Problem, das nicht nur bei Messengern sondern auch bei der E-Mail-Kommunikation auftritt. Regierungen, Bildungseinrichtungen und Dienstleister sollten daher gemeinsam versuchen, die Ausbildung der Bevölkerung in der IT, ihre Schutzmechanismen und nicht zuletzt den Schutz der Privatsphäre zu verbessern.

- **Vertrauen gegenüber WhatsApp.** Die meisten Teilnehmer gaben an, WhatsApp aufgrund mangelnder Transparenz, z. B. hinsichtlich ihres Geschäftsmodells und der Verarbeitung von Nutzerdaten (FF3), mehr zu misstrauen als anderen Messengern. Ein weiterer Grund hierfür waren die bereits beschriebenen falschen Vorstellungen von E2E-Verschlüsselung. Im Einklang mit diesem Misstrauen gingen viele Nutzer davon aus, dass WhatsApps Motivation zur Einführung der E2E-Verschlüsselung ausschließlich darin bestand, mit anderen Messengern zu konkurrieren, finanzielle Vorteile zu erzielen, gesetzliche Anforderungen zu erfüllen oder sogar Nutzer mit einem Lockangebot (FF4) zu verführen. Nur fünf von zwanzig Teilnehmern nahmen an, dass WhatsApp Verantwortung übernehmen und ihre Daten schützen wolle. Einige Teilnehmer interpretierten die Einführung der E2E-Verschlüsselung sogar als schlechtes Zeichen, da dies bedeute, dass „etwas mit Sicherheit von Anfang an falsch gewesen sein muss".

Angesichts dieses mangelnden Vertrauens der WhatsApp-Nutzer könnte es sinnvoll sein, über Maßnahmen nachzudenken, die das Konzept der E2E-Verschlüsselung und ihren beabsichtigten Zweck zu erläutern. Da einige Teilnehmer die mangelnde Transparenz von WhatsApp als Unternehmen kritisierten, bestünde eine weitere Möglichkeit darin, Informationen über das Geschäftsmodell des Unternehmens zur Verfügung zu stellen. Dies kann, je nach bereitgestellten Informationen, das Vertrauen der Nutzer in WhatsApp erhöhen oder aber sogar noch verringern. In jedem Fall könnte die Veröffentlichung des Quellcodes der Verschlüsselung dazu beitragen, Sicherheitsexperten von der Stärke der Verschlüsselung zu überzeugen und schließlich das Vertrauen der Endnutzer in diese Technologie zu erhöhen.

Danksagung

Die in diesem Paper beschriebene Forschung wurde vom Bundesministerium für Bildung und Forschung (BMBF) und dem Hessischen Ministerium für Wissenschaft und Kunst innerhalb des Projekts CRISP (www.crisp-da.de), dem Bundesministerium für Bildung und Forschung (BMBF) innerhalb des Projekts MoPPa und des Kompetenzzentrums für angewandte Sicherheitstechnologie (KASTEL) sowie der DFG als Teil des Projekts D.1 im Rahmen des GRKs 2050 „Privacy and Trust for Mobile Users" gefördert.

Literatur

Abu-Salma, R., Sasse, M. A., Bonneau, J., Danilova, A., Naiakshina, A. and Smith, M. (2017). "Obstacles to the Adoption of Secure Communication Tools". In: Proceedings of the IEEE Symposium on Security and Privacy (S&P 2017). Washington, DC: IEEE Computer Society, pp. 137-153.

Atwater, E., Bocovich, C., Hengartner, U., Lank, E. and Goldberg, I. (2015). "Leading Johnny to Water: Designing for Usability and Trust." In: Proceedings of the Eleventh Symposium on Usable Privacy and Security (SOUPS 2015). Ottawa: USENIX Association, pp. 69–88. Verfügbar unter: https://www.usenix.org/conference/soups2015/proceedings/presentation/atwater.

Facebook Inc. (2014). Facebook to Acquire WhatsApp. URL: https://newsroom.fb.com/news/2014/02/facebook-to-acquire-whatsapp (abgerufen am 30.05.2017).

Freude, A. and Freude, T. (2016). Echos of History: Understanding German Data Protection. Verfügbar unter: http://www.bfna.org/publication/newpolitik/echos-of-history-understanding-german-data-protection (abgerufen am 25.08.2017).

Naiakshina, A., Danilova, A., Dechand, S., Krol, K., Sasse, A. and Smith, M. (2016). "Mental Models – User understanding of messaging and encryption." Poster vorgestellt bei: The First European Symposium on Security and Privacy (Euro S&P 2016).

Open Whisper Systems 2013-2016 (2016). Open Whisper Systems. Verfügbar unter: https://whispersystems.org (abgerufen am 30.05.2017).

Ruoti, S., Kim, N, Burgon, B., Van Der Horst, T. and K. Seamons. (2013). "Confused Johnny: When Automatic Encryption Leads to Confusion and Mistakes." In: Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS 2013). New York: ACM, pp. 51-69.

The H Security (2012). WhatsApp accounts almost completely unprotected. Verfügbar unter: http://www.h-online.com/security/news/item/WhatsApp-accounts-almost-completely-unprotected-1708545.html (abgerufen am 30.08.2017).

Statista (2017). Number of monthly active WhatsApp users worldwide from April 2013 to July 2017 (in millions). Verfügbar unter: https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/ (abgerufen am 30.08.2017).

Strauss, A. and J. Corbin (1990). Basics of Qualitative Research: Grounded Theory Procedures and Techniques. Newbury Park, California: Sage Publications.

Strauss, A. (1987). Qualitative analysis for social scientists. New York, NY: Cambridge University Press.

WhatsApp Inc. (2016a). End-to-End Encryption. Verfügbar unter: https://blog.whatsapp.com/10000618/end-to-end-encryption (abgerufen am 30.08.2017).

WhatsApp Inc. (2016b). WhatsApp Encryption Overview. Verfügbar unter: https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf (abgerufen am 30.05.2017).

WhatsApp Inc. (2016c). WhatsApp Privacy Policy. Verfügbar unter: https://www.whatsapp.com/legal/#privacy-policy abgerufen am 30.08.2017).