Sascha Dinse, Dipl.- Soziologe

Messenger sicher einsetzen

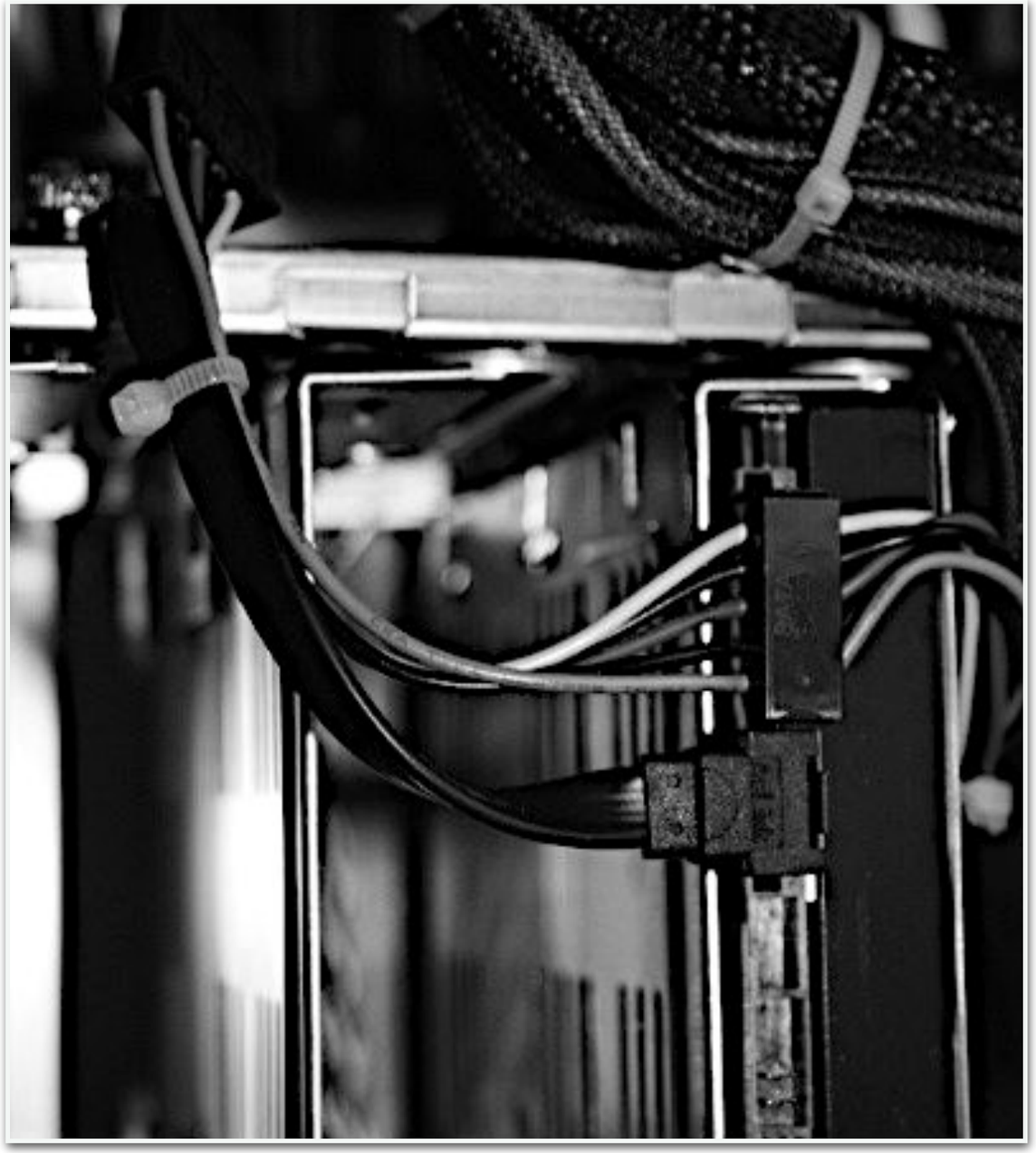
Wer bin ich überhaupt?

- Jahrgang 1978
- Diplom-Soziologe (Medien- und Kultursoziologie, Anthropologie, Geschlechterforschung, Subkulturen)
- freiberuflicher Dozent für Medienkompetenz, hauptsächlich im NGO-Bereich aktiv
- mehr als 25 Jahre Netzerfahrung, beginnend mit analogen Modems und 286er-Rechnern, Amiga 500 & Co.
- enge Zusammenarbeit mit sozialen Einrichtungen, Wohlfahrtsverbänden, Beratungsstellen
- Schriftsteller, Musiker, Blogger, Gamer. Sonst aber ganz nett.

Womit beschäftigen wir uns?

Inhalt

- Kriterien
- Vergleich aktueller Messenger
- Theorie vs. Praxis



Kriterien

Kriterien

Einfachheit der Nutzung

Die aktuellen Messenger sind im Grunde alle sehr ähnlich in der Benutzung. Lediglich spezielle Funktionen wie die »geheimen Chats« in Telegram (die müssen nämlich speziell aktiviert werden) fallen hier aus dem Rahmen.

Kriterien

Akzeptanz bei Klient*innen

Einer der wichtigsten Faktoren: Nehmen die Klient*innen den Messenger an? Wie hoch ist die Hürde, die Software zu verwenden? Kann man die eigene Klientel von WhatsApp abbringen?

Kriterien

Verschlüsselung der Daten

Eine immer aktive **Ende-zu-Ende-Verschlüsselung*** ermöglicht eine »geheime« Kommunikation zwischen Gesprächsteilnehmern.

Nicht alle Messengerdienste erfüllen diese Voraussetzung, bei z.B. Telegram muss E2E-Verschlüsselung manuell aktiviert werden.

*bedeutet, dass nur Sender und Empfänger eine Nachricht entschlüsseln können, nicht einmal der Anbieter selbst kann die Inhalte lesen

Kriterien

Anonyme Nutzung

Eine Nutzung von Messengerdiensten ohne vorherige Anmeldung erlaubt es, nur ein Mindestmaß an personenbezogenen Daten zu verwenden.

Gleichzeitig wird die Zuordnung eines Nutzers zu einem Account erschwert (Nachweispflichten?).

Speicherung von Nachrichten auf externen Servern

Die meisten gängigen Messenger speichern Nutzernachrichten nur temporär auf eigenen Servern (zum Zwecke der Zustellung) und bestenfalls verschlüsselt. Dadurch hat der Anbieter selbst keinen Zugriff auf die Nachrichteninhalte.

Kriterien

Speicherung von Telefonnummern auf externen Servern

Idealerweise werden Telefonnummern, sofern diese nötig sind, nicht im Klartext auf externen Servern gespeichert. Diese ist besonders relevant, wenn Kommunikation mit Klienten stattfindet.

Kriterien

Speicherung von Metadaten auf externen Servern

Metainformationen (z.B. wer mit wem kommuniziert, Absturzberichte etc.) sollten wenn überhaupt nur in komplett anonymisierter Form gespeichert werden. Am besten natürlich überhaupt nicht.

Kriterien

Selbstlöschende Nachrichten

Einige Dienste (u.a. Telegram) bieten an, Nachrichten nach dem Versand auf allen (!) Geräten (also auch bei Empfängern) zu löschen. Dies klingt aus Datenschutzsicht sinnvoll, ist aber für Nachweise etc. eher ungünstig.

Kriterien

DSGVO-Kompatibilität

Liegen Datenschutzerklärung und AGB auf Deutsch vor? Falls nicht, ergibt sich ein Zustimmungs-Problem, da deutsche Nutzer*innen normalerweise nur deutschen AGB wirklich »informiert« zustimmen können.

Kriterien

Serverstandort

Der Serverstandort ist seit DSGVO im Grund irrelevant*, aber aufgrund des »Datenschutzniveaus« doch wieder nicht. Besonders, wenn es zu einem Gerichtsverfahren kommt, ist eine Klage gegen einen Anbieter aus der EU deutlich einfacher.

*Nach dem »Marktortprinzip« der DSGVO müssen alle Dienste, die in Deutschland/EU verwendet werden können, auch deutsches bzw. europäisches Recht erfüllen.

Kriterien

Serverstandort

Die Annahme, dass der Serverstandort Deutschland die Sicherheit der Daten erhöht oder eine bessere Servicequalität ermöglicht, ist indes Unsinn. Reines Marketing.

Kriterien

Weitergabe von Daten an Behörden

In einigen Berichten wird der Messenger »Signal« dafür kritisiert, dass dort laut AGB unter Umständen Informationen an Behörden weitergegeben werden. Rechtlich dürften jedoch alle Anbieter zu so etwas verpflichtet sein, wenn Straftaten begangen werden, egal ob es in den AGB steht oder nicht.

Kriterien

Open Source vs. proprietärer Code

Zwar bedeutet Open Source nicht automatisch eine besser funktionierende oder sicherere App, aber die Möglichkeit, Einblick in die Funktionsweise nehmen zu können, ist ein großer Transparenzvorteil.

Nutzer sollten bestmöglich über die Funktionsweise einer App informiert sein, bevor sie diese nutzen.

Kriterien

Updatefrequenz

Updates bedeuten Sicherheit. Von daher ist es nötig, einen Messenger einzusetzen, bei dem etwaige Lücken möglichst schnell geschlossen werden (vgl. WhatsApps Historie von Lücken und Softwarefehlern als eher schlechtes Beispiel).

Kriterien

Gerätekompatibilität / Weiterentwicklung

Messengerapps setzen häufig aktuelle und anspruchsvolle Technologien z.B. zur Verschlüsselung ein. Hierbei sollte darauf geachtet werden, einen Dienst zu nutzen, der nicht nur alle gängigen Versionen eines OS (z.B. Android) unterstützt, sondern auch auf den neusten Versionen läuft. Beispiel: MacOS/Windows10 unterstützen nur noch 64-bit-Versionen von Software.

Kriterien

Riskante Funktionen

Nicht alle Apps bieten identische Funktionen.
Sprachnachrichten sind zwar in den meisten Diensten möglich, stellen aber u.U. ein Datenschutzrisiko dar (Mithören bei der Aufnahme).

Kriterien

Vorhandensein einer Desktop-App

Einige Dienste bieten eine Desktop-App zur Nutzung am Rechner. Dies kann ein Datensicherheits- und Datenschutzproblem darstellen, wenn Arbeitsplätze unzureichend gesichert sind.

Vergleich aktueller Messenger

Vergleich

Überblick

Aufgrund der Vielzahl verfügbarer Messenger kann hier nur auf einen Teil eingegangen werden.

In diesem Artikel der Verbraucherzentrale finden Sie weitere Informationen, auch zu Messenger, die hier nicht direkt angesprochen werden.

https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/whatsappalternativen-messenger-im-ueberblick-13055

Vergleich

WhatsApp

Pro: extrem hohe Verbreitung, einfach zu nutzen, viele Funktionen, Inhalte der Nachrichten wirksam verschlüsselt

Contra: Meta-Daten (Telefonnummer, Info wer mit wem kommuniziert) werden unverschlüsselt übertragen, Software nicht komplett offen, gibt Nutzerdaten an Facebook weiter

Vergleich

Signal

Pro: OpenSource, kostenlos, Desktop-App vorhanden, Kontaktabgleich nur gehasht, häufige Updates, Backups möglich (verschlüsselt) für Übernahme auf neue Installation

Contra: Telefonnummer (und damit SIM-Karte) nötig für Anmeldung, keine deutschen AGB, u.U. wird die IP-Adresse temporär gespeichert, Daten können laut AGB an Behörden weitergegeben werden (was aber kein Negativpunkt ist, sondern gesetzlich so vorgeben)

Vergleich

Telegram

Pro: recht weit verbreitet, bietet selbst-löschende Nachrichten (was bezüglich Dokumentation ungünstig ist)

Contra: Verschlüsselung nicht standardmäßig aktiv (muss manuell angeschaltet werden), keine deutsche Datenschutzerklärung, Standort der Server unklar (Firmensitz laut Website in Dubai)

Vergleich

~~Hoccer~~

~~**Pro:** anonyme Nutzung möglich, AGB auf Deutsch, angeblich unbegrenzte Dateigröße für Uploads, Sprachnachrichten möglich, verschlüsselte Backups möglich~~

~~**Contra:** nicht OpenSource (aus eher fadenscheinigen Gründen), kein Desktop/Web-Client, nur auf einem Gerät gleichzeitig nutzbar laut FAQ, »in der Nähe«-Funktion spricht nur von »transportverschlüsselt«, u.U. werden Metadaten temporär erhoben, letztes Update GooglePlay 4.9.2018~~

Mittlerweile eingestellt
https://www.heise.de/newsticker/meldung/Sichere-Messenger-Hoccer-gibt-auf-4724448.html

Vergleich

Wire

Pro: OpenSource, bis zu 8 Geräte pro Nutzer möglich, Kontakte werden nicht extern gespeichert

Contra: Schweizer Gerichtsbarkeit (Server in D und Irland), Backups von Unterhaltungen möglich (aber unter Android NICHT verschlüsselt)

Vergleich

Threema

Pro: E2E standardmäßig aktiv, deutsche AGB, anonyme Nutzung möglich, Nachrichten werden verschlüsselt für max. 2 Wochen auf dem Server gehalten, keine Speicherung von Kontaktdaten (nur gehashter Abgleich, danach Löschung), Desktop-App vorhanden

Contra: einmalig kostenpflichtig, nicht OpenSource, u.U. werden Standortdaten verwendet, einige technische Metadaten werden erhoben, Backups zwar verschlüsselt möglich aber unter iOS nur als Beta

Vergleich

Threema Work (für Unternehmen und Einrichtungen)

Pro: vorkonfigurierbar, ID-Trennung bei Mitarbeiterwechsel möglich, Chatzugriff kann unterbunden werden, Termine- und Umfragenfunktion, nach eigenen Angaben voll DSGVO-konform, 60-Tage-Testversion kostenlos

Contra: analog Threema, kostenpflichtig ab 1,40CHF pro Gerät und Monat

Theorie vs. Praxis

Theorie vs. Praxis

Prozesse

Definieren interner Prozesse für Archivierung, Nachweise, Account-Übergabe etc. müssen vorher (!) geklärt sein.

Wird eine einheitliche technische Grundlage (Geräte, OS-Versionen) eingesetzt?

Soll langfristig mit Klient*innen kommuniziert werden? Akzeptanzschwelle? Verbreitung der Dienste?

Theorie vs. Praxis

Prozesse

Wie häufig werden Übergabeprozesse oder das Einspielen von Backups erwartet?

Wie hoch ist die technische Kompetenz der Mitarbeiter*innen?

Sind finanzielle Mittel vorhanden? (siehe Threema Work)

Vielen Dank für Ihre Aufmerksamkeit!

Sascha Dinse
Dipl.-Soziologe
Stralauer Allee 17b
10245 Berlin

01758602557
sascha@sozialvernetzer.de
