Messenger-Bewertung der Digitalen Gesellschaft

Winterkongress
der Digitalen Gesellschaft
24.02.2018

Jakob Bolliger

whoami

- Mitglied der Digitalen Gesellschaft seit 2016
- Berater für Datenschutz und IT-Sicherheit
- Aktuell beteiligt an der Aktualisierung der Messenger-Bewertung 2018

Agenda

- Warum braucht es eine Messenger-Bewertung?
- Was sind die Bewertungskriterien?
- Ergebnisse

Welche Daten wollen wir schützen?

- Kommunikationsinhalt
  - Gespräch, Mail, Nachricht
  - Tiefer Einblick in das Privatleben

- Metadaten
  - Wer / Wann / Wo / Mit wem / Wie lange
  - Beziehungsnetz, Bewegungsprofil

Schutz des Privatlebens

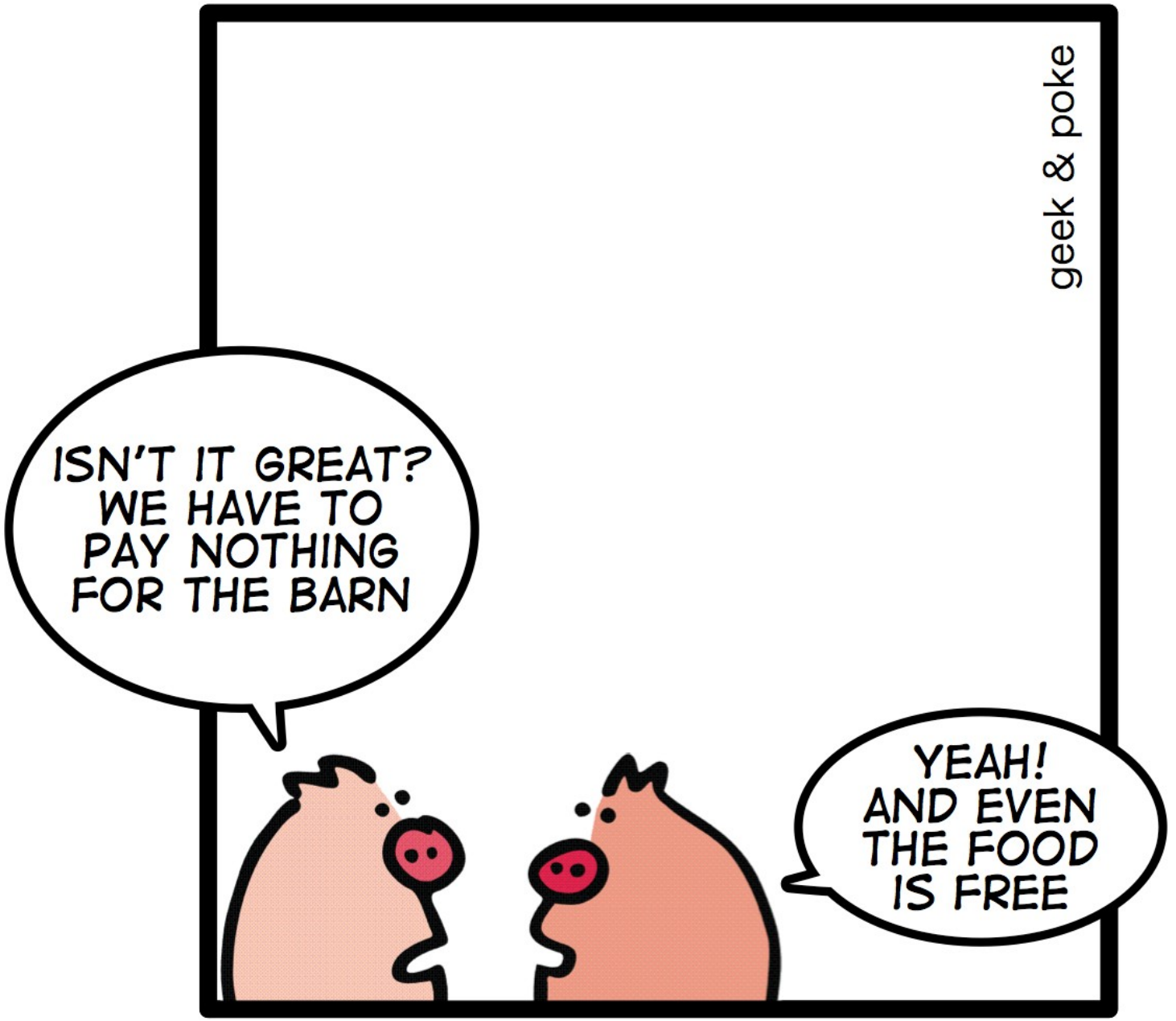
Allgemeine Erklärung der Menschenrechte, Art.12:

Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.

Vor wem möchten wir unsere Daten schützen?

Wer sind die Bedarfsträger? (1/3)

- Kriminelle / böswillige Hacker
  - Riesiger Schwarzmarkt für gestohlene Nutzer-/Zugangsdaten existiert im Dark Web.
  - Entwendete Daten können für Betrug missbraucht werden.
  - Vertrauliche Kommunikationsdaten können geleakt oder verkauft werden.



PIGS TALKING ABOUT THE "FREE" MODEL

http://geekandpoke.typepad.com/geekandpoke/2010/12/the-free-model.html

Wer sind die Bedarfsträger? (2/3)

- Privatwirtschaft
  - Unternehmen bieten die Nutzung der Dienste ‚gratis' an, im Gegenzug gibt der Kunde das Einverständis für die weitere Nutzung seiner Daten.
  - Eigene Nutzung und Weiterverkauf der Daten durch Dienstanbieter
  - Handel mit Nutzerdaten ist Milliardengeschäft

Wer sind die Bedarfsträger? (3/3)

- Strafverfolgungsbehörden
  - Anfrage an Dienstanbieter
  - Zugriff auf die Daten der Vorratsdatenspeicherung

- Geheimdienste
  - Auswertung der Daten durch Geheimdienste

- Siehe auch:

https://www.digitale-gesellschaft.ch/slides/ueberwachungsstaat.html

Wie bewerten wir Messenger?

Bewertungskriterien

- Sicherheit und Privatsphäre
  - Transportverschlüsselung
  - Ende-zu-Ende-Verschlüsselung
  - Keine Metadatenspeicherung
  - Security-/Code-Audits
  - Kein Adressbuch-Zugriff
  - Anonyme Nutzung
- Nachhaltigkeit
  - Offener Standard
  - Open Source Software
  - Dezentrale Architektur
- Benutzerfreundlichkeit

Transportverschlüsselung

- Die Nachrichten sind während dem Transport wirkungsvoll verschlüsselt.
- Dienstanbieter können aber Inhalte der für den Transport verschlüsselten Datenpackete lesen.
- Die Metadaten sind bei der Übertragung geschützt.
- Vertaulichkeit: Daten können von unberechtigten Dritten nicht mitgelesen werden
- Integrität: Daten wurden beim Transport nicht manipuliert
- Autenzität: Datensender und empfänger können sich gegenseitig authentifizieren

Transportverschlüsselung

Transport Layer Security (TLS):

- TLS ist ein Verschlüsselungsprotokoll zur Datenübertragung im Internet.
- Nachfolger von SSL (Secure Sockets Layer)
- TLS verschlüsselt die Daten während dem Transport zwischen Clients und Server (bzw. Nutzer und Dienstanbieter).
- Protokoll auf Ebene Transportschicht im TCP/IP Protokoll Stapel

- Bewertungsaspekte:
  - Überprüfung der Zertifikate
  - Verwendung guter Cypher Suites

Ende-zu-Ende-Verschlüsselung

- Verschlüsselung der Kommunikation zwischen zwei Clients
- Die Nachrichten können nur von den beteiligten Kommunikationspartnern gelesen werden.
- Verschiedene Verschlüsselungsprotokolle werden eingesetz
- Bewertungsaspekte:
    - Wie ist das Schlüsselmanagement gelöst?
    - Authentifikation des Kommunikationspartners möglich?
    - Ist E2E Verschlüsselung standartmässig aktiviert?
    - Verschlüsselung von Gruppenchats

Keine Metadatenspeicherung

- Es findet keine (bekannte) Speicherung von Metadaten durch den Anbieter für eigene Zwecke oder für Strafuntersuchungsbehörden resp. Geheimdienste statt (Vorratsdatenspeicherung).
- Bewertungsaspekte:
  - Aussagen der Anbieter bezüglich Metadatenspeicherung
  - Ist der Anbieter gesetzlich zur Metadatenspeicherung verpflichtet (Vorratsdatenspeicherung)?
  - Ist die Metadatenspeicherung per Design nicht möglich(z.B. Peer-to-Peer)

Security-/Code-Audits

- Es gibt aktuelle und unabhängige Untersuchungen des Source Codes zu den verwendeten Verschlüsselungsmethoden.
- Bewertungsaspekte:
  - Von wem wurde der Audit durchgeführt?
  - Wie aktuell ist der Audit?
  - Falls kein Audit vorhanden ist, ist der Code Open Source?
  - Falls kein Audit vorhanden ist, gibt es Audits für Teile des Codes z.B. Verschlüsselungsprotokoll?

Kein Adressbuch-Zugriff

- Es findet keine Synchronisation (Abgleich) des Adressbuchs zum Anbieter statt.
- Bewertungsaspekte:
  - Gewisse Anwendungen geben dem Nutzer die Wahl zum Abgleich des Adressbuchs (Opt-In).
  - Möglichkeit des Adressbuch-Zugriff auf Betriebsystem-Ebene einzuschränken.
  - Verschiedene Möglichkeiten des Adressbuch-Abgleich:
    - Upload des Adressbuches in Klartext
    - Upload der Hashes
  - Ist Schlüsselaustausch offline und ohne zentraler Server möglich?

Anonyme Nutzung

- Die Benutzeridentifikation ist nicht an eine Telefonnummer, den Personennamen und/oder die physische Adresse gebunden.
- Bewertungsaspekte:
  - Identifikation gebunden an Social Profile
  - Identifikation gebunden an Email-Adresse
  - Ungebundene Identifikation

Offener Standard

- Es wird ein offener Standard verwendet, der frei implementiert werden kann.
- Bewertungsaspekte:
  - Gesellschaftliche Norm, App von verschiedenen Anbietern
  - Öffentlicher/IETF Standard
  - Datenportabilität (Konversationen-Export möglich)

Offener Standard

Definition der Genfer Erklärung 2008 (OpenForum Europe):

„Ein Offener Standard bezieht sich auf ein **Format oder Protokoll**, das

einer **vollständig öffentlichen Bewertung und Nutzung ohne Hemmnisse** auf eine für alle Beteiligten **gleichermassen zugänglichen** Weise unterliegt,

ohne jegliche Komponenten oder Erweiterungen ist, die von **Formaten oder Protokollen abhängen**, die selbst **nicht der Definition eines Offenen Standards** entsprechen,

frei ist von juristischen oder technischen Klauseln, die seine Verwendung von jeglicher Seite oder jeglichem Geschäftsmodell einschränken,

unabhängig von einem einzelnen Anbieter geleitet und weiterentwickelt wird in einem Prozess, der **einer gleichberechtigten Teilnahme von Wettbewerbern und Dritten offen steht**,

verfügbar ist in **verschiedenen vollständigen Implementierungen** von **verschiedenen Anbietern** oder als vollständige Implementierung gleichermaßen für alle Beteiligten."

(https://web.archive.org/web/20130426220816/http://www.openforumeurope.org/library/geneva/declaration/manifesto-with-logos-final.pdf)

Open Source Software

- Die Software steht im Quellcode zur Verfügung und kann von Dritten eingesehen, geändert und weiterverwendet werden.
- Bewertungsaspekte:
    - offener Quellcode Server
    - offener Quellcode App
    - offenes Verschlüsselungsprotokoll

Dezentrale Architektur

- Die Software ist nicht von einem einzigen, zentralen Anbieter abhängig.
- Bewertungsaspekte:
  - Abhängig von einem oder mehreren Anbietern?
  - Föderiert, Möglichkeit eines eignen Servers
  - Dezentrale Architektur, Peer-to-Peer

Benutzerfreundlichkeit

- Bewertungsaspekte:
  - Einfache Benutzung/Installation
  - Grosse Verbreitung/Nutzerbasis (Global / Schweiz)
  - Platform-Unabhängigkeit / Client vorhanden für Android/iOS/Win/macOS/Unix

Ergebnisse

Sicherheit und Nachhaltigkeit von WhatsApp, E-Mail, SMS & Co.

DIGITALE | GESELLSCHAFT

Stand: November 2016

	Sicherheit und Privatsphäre						Nachhaltigkeit			Sonstiges	Resultat
	Keine Metadaten-Speicherung	Transport-Verschlüsselung	Ende-zu-Ende-Verschlüsselung	Security-/Code-Audits	Wählbare Identifikation	Kein Adressbuch-Upload/Zugriff	Offener Standard	Open Source Software	Dezentrale Architektur	Benutzer-freundlichkeit	Schluss-bewertung
Briefpost	☆☆ 2)	☆☆☆	☆☆ 3)	☆	☆	☆☆☆	☆☆ 1)	☆☆ 1)	☆☆ 1)	☆☆☆	★★
Fax	☆	☆☆ 4)	☆	☆	☆	☆☆☆	☆☆ 1)	☆☆ 1)	☆☆ 1)	☆☆☆	★
Festnetztelefon	☆	☆☆ 4)	☆	☆	☆	☆☆☆	☆☆ 1)	☆☆ 1)	☆☆ 1)	☆☆☆	★
Mobiltelefon	☆	☆☆ 4)	☆	☆	☆	☆☆☆	☆☆ 1)	☆☆ 1)	☆☆ 1)	☆☆☆	★
SMS	☆	☆☆ 4)	☆	☆	☆	☆☆☆	☆☆ 1)	☆☆ 1)	☆☆ 1)	☆☆☆	★
E-Mail mit pEp	☆☆ 4)	☆☆ 4)	☆☆☆	☆☆☆ *)	☆☆☆	☆☆☆	☆☆	☆☆☆	☆☆☆	☆☆	★★★
E-Mail mit GnuPG	☆☆ 4)	☆☆ 4)	☆☆☆	☆☆	☆☆☆	☆☆☆	☆☆☆	☆☆☆	☆☆☆	☆	★★★
E-Mail	☆☆ 4)	☆☆ 4)	☆	☆☆ 4)	☆☆☆	☆☆☆	☆☆☆	☆☆ 4)	☆☆☆	☆☆☆	★★
ProtonMail	☆☆ 5)	☆☆☆	☆☆	☆☆	☆☆☆	☆☆☆	☆☆	☆☆	☆☆	☆☆	★★
E-Mail mit S/MIME	☆☆ 4)	☆☆ 4)	☆☆☆	☆☆	☆☆	☆☆☆	☆☆☆	☆☆☆	☆☆	☆	★★
Privasphere	☆☆ 5)	☆☆☆	☆	☆☆☆ *)	☆☆	☆☆☆	☆☆	☆	☆☆	☆☆	★★
Post IncaMail	☆☆ 5)	☆☆☆	☆	☆	☆☆	☆☆☆	☆☆	☆	☆☆	☆☆	★
Jabber/XMPP mit OTR	☆☆☆	☆☆ 4)	☆☆☆	☆☆☆ *)	☆☆☆	☆☆☆	☆☆☆	☆☆☆	☆☆☆	☆	★★★
Wire	☆☆☆	☆☆☆	☆☆☆	☆☆	☆☆☆	☆☆☆	☆	☆☆	☆	☆☆☆	★★
Signal	☆☆☆	☆☆☆	☆☆☆	☆☆☆ *)	☆	☆☆ 6)	☆	☆☆☆	☆	☆☆☆	★★
Threema	☆☆ 5)	☆☆☆	☆☆☆	☆☆☆ *)	☆☆☆	☆☆☆	☆	☆	☆	☆☆	★★
Telegram	☆☆☆	☆☆☆	☆☆ 8)	☆☆	☆	☆	☆	☆☆	☆	☆☆☆	★
Snapchat	☆	☆☆☆	☆	☆	☆☆☆	☆☆☆	☆	☆	☆	☆☆☆	★
WhatsApp	☆	☆☆☆	☆☆☆	☆☆	☆	☆	☆	☆	☆	☆☆☆	★
Viber	☆	☆☆☆	☆☆☆	☆	☆	☆	☆	☆	☆	☆☆☆	★
Facebook Messenger	☆	☆☆☆	☆☆ 8)	☆	☆	☆☆	☆	☆	☆	☆☆☆	★
Direct Message 0)	☆	☆☆☆	☆	☆	☆☆ 1)	☆☆ 1)	☆	☆	☆	☆☆☆	★
iMessage	☆	☆☆☆	☆☆ 7)	☆	☆☆	☆☆	☆	☆	☆	☆☆	★
Swisscom iO	☆☆ 5)	☆☆☆	☆	☆	☆	☆	☆	☆	☆	☆☆☆	★
Tox	☆☆☆	☆☆☆	☆☆☆	☆☆	☆☆☆	☆☆☆	☆	☆☆☆	☆☆☆	☆☆☆	★★★
RetroShare	☆☆☆	☆☆☆	☆☆☆	☆☆	☆☆☆	☆☆☆	☆	☆☆☆	☆☆☆	☆☆	★★★
Mumble	☆☆☆	☆☆☆	☆	☆☆	☆☆☆	☆☆☆	☆	☆☆☆	☆☆☆	☆☆	★★
Skype	☆	☆☆☆	☆	☆	☆☆☆	☆☆☆	☆	☆	☆	☆☆☆	★
Hangouts	☆☆ 1)	☆☆☆	☆	☆	☆☆	☆☆	☆	☆	☆	☆☆☆	★
CryptoPhone	☆☆	☆☆☆	☆☆☆	☆☆	☆	☆☆☆	☆	☆☆	☆	☆	★
Blackphone	☆☆	☆☆☆	☆☆☆	☆	☆☆	☆☆☆	☆	☆	☆	☆	★

https://www.digitale-gesellschaft.ch/messenger/bewertung.html

Fazit - empfehlenswert

- E-Mail mit GnuPG, pEp oder S/MIME
  - Sorgfältige Auswahl des Mailproviders ist wichtig
  - Vorratsdatenspeicherung
  - Transportverschlüsselung
  - Beispiele: posteo.de oder mailbox.org
- Messenger:
  - Wire, Signal und Threema
  - Jabber/XMPP mit OTR
  - Tox, Retroshare und Mumble
  - Briefpost (mit Direkteinwurf)

Fazit – nicht empfehlenswert

- Mobiltelefon und SMS
- WhatsApp
- iMessage
- Skype
- alle anderen aus dem Test

Schlusswort

- Sicherheit und Nachhaltigkeit stehen oft im Widerspruch zur Benutzerfreundlichkeit
- Die Gewichtung sollte den eigenen Präferenzen und dem individuellen Anwendungsfall angepasst werden
- Briefpost aber nicht Telefon/Fax/SMS verwenden
- Sorgfältige Auswahl des E-Mailproviders und Verschlüsselung sind wichtig
- Anstatt WhatsApp die «Alternativen» Wire, Signal, Tox oder Jabber/XMPP mit OTR verwenden

Fragen?