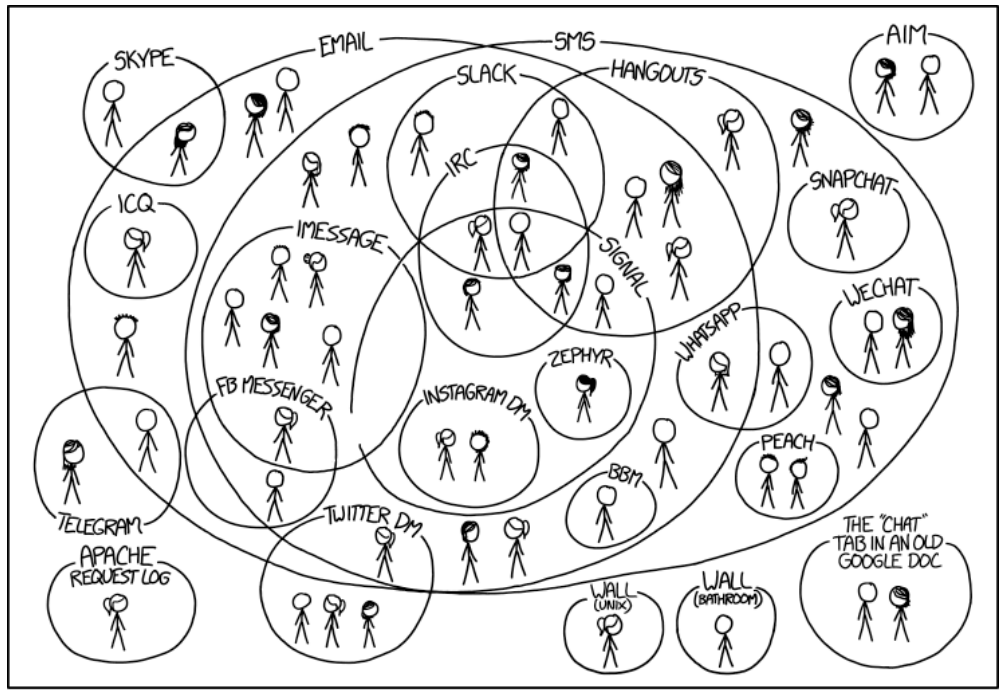
IT Security Awareness Days Herbst 2021

Messenger – Datenschutz und Informationssicherheit

Dr. Holger Beck
Informationssicherheitsbeauftragter der Georg-August-Universität Göttingen
IT-Sicherheitsbeauftragter der GWDG

Kommunikationschaos?



https://xkcd.com/1810/

- Tausend Möglichkeiten – Was nutzen Sie?
- Was sollte man nutzen? – Was darf man nutzen? – Was sollte man beachten?

- Heute nur ein Blick auf Messenger (WhatsApp & Co)

- Mit Blick auf Anforderungen aus zwei Bereichen
  - Informationssicherheit und
  - Datenschutz

- Mit Blick auf zwei Kommunikationsaspekte
  - Inhalte und
  - Umstände

Messenger – eine Auswahl

WhatsApp – meist genutzter Messenger

Signal – viel diskutierte Alternative

Threema – Messenger mit mehr Datenschutz

Telegram – Messenger der Terroristen und Kriminellen?

Rocket Chat – selbst betriebener Messenger-Ersatz

- und etliche andere
  - auch spezielle Varianten für Firmen oder spezielle Berufsgruppen,
  - als Intranet oder mit öffentlichem Zugang
- Bei der Bewertung zu berücksichtigen:
  - Datenschutz und Informationssicherheit
  - jeweils bezüglich Inhalten und Umständen der Kommunikation

Informationssicherheit und Datenschutz

Unterschiedliche Ziele

Informationssicherheit

- Sicherstellen von
  - **Vertraulichkeit**,
  - Integrität und
  - Verfügbarkeit
- von beliebigen Informationen
- als Ziele der
  - **Eigentümer** und
  - **Nutzer** der Informationen.

Datenschutz

- Informationelle Selbstbestimmung
- bezüglich personenbezogener Daten (Informationen)
- aus Sicht der Personen, **über** die Daten verarbeitet werden (**Betroffene**)
- durch Grundsätze nach DSGVO
  - Rechtmäßigkeit
  - Transparenz
  - Zweckbindung
  - **Datenminimierung**
  - Richtigkeit
  - Speicherbegrenzung (Löschrechte)
  - Integrität und **Vertraulichkeit**

Kommunikation – Inhalt versus Umstände

Inhalt

- Welche Informationen werden ausgetauscht?
- Ist sicher, dass nur Berechtigte die Inhalte kennen (Vertraulichkeit)?
- Sind die Inhalte unverfälscht (Integrität)?
- Sind die Inhalte zugreifbar, wenn man Sie benötigt (Verfügbarkeit)?

Umstände

- Wer kommuniziert mit wem?
- Wann?
- Wie oft?
- Umfang der Kommunikation (Größe der Nachrichten u.ä.)
- Von wo aus (genutztes Gerät, Standort)?

- Daten zu den Umständen = Metadaten

- Nebenwirkungen der App
  - Adressierung
  - Datensammlungen

Vertraulichkeit der Kommunikationsinhalte

Zwei Varianten der Verschlüsselung der Übertragung

Ende-zu-Ende-Verschlüsselung

- Verschlüsselung der gesamten Kommunikation
  - Verschlüsselung durch Absender
  - Entschlüsselung nur durch Empfänger
- Vorteil
  - Auf dem Server des Anbieters liegen höchstens verschlüsselte Inhalte

Transportverschlüsselung

- Verschlüsselung nur für die Übertragung auf Teilstrecken:
  - vom Absender zum Server des Anbieters und
  - vom Server zum Empfänger.
- Nachteil
  - Auf dem Server liegt der Inhalt unverschlüsselt vor.

Vertraulichkeit der Kommunikationsinhalte

Varianten der Speicherung von Inhalten

Speicherung auf den Endgeräten

- höchstens vorübergehenden auf einem Server des Anbieters, d.h. wenn der Kommunikationspartner gerade offline ist,
- Inhalte (z.B. Bilder) liegen
  - im normalen Speicher des Endgeräts (z.B. in der allgemeinen Bildergalerie) oder
  - in separatem Speicher der App
- Vorteile:
  - Der Anbieter hat keinen Zugriff auf die Inhalte
  - Separater Speicher zur weiteren Abschottung von Inhalten in speziellen Apps für besonders gesicherte Anwendungsszenarien

Speicherung auf einem Server des Anbieters

- Die Kommunikationsinhalte liegen primär auf dem Server des Anbieters, auf dem Endgerät nur teilweise, zeitweise oder nach explizitem Herunterladen (insbesondere von Anlagen)
- Vorteile:
  - Datensicherung durch Anbieter möglich
  - Geräteunabhängigkeit: Gleiche Ansicht von verschiedenen Geräten
- Nachteil
  - Potentielle Einsicht in Inhalte durch Anbieter

Weitere Optionen

Sprach- und Videokommunikation

- Verschlüsselte Telefon- und Videoanrufe

Löschen von Nachrichten

- Noch eine Option: Automatisch verschwindende Nachrichten
  - Nachrichten, die sich beim Empfänger selbst löschen
    - nach einer bestimmten Zeit oder
    - nach dem Lesen

Fazit Sicherheit der Inhalte

Ende-zu-Ende-Verschlüsselung	✓	✓	✓	✓	✗
Speicherung getrennt von Gerätebibliotheken	✗	✓	✓	✓	⊖
Speicherung auf Server	✗	✗	✗	✓	✓
Verschwindende Nachrichten	✓	✓	✗	✓	✗
Sprach- und Videoanrufe	✓	✓	✓	✓	✗

✓ Optionale geheime Chats, nicht Standard, nicht für Gruppen

- Ende-zu-Ende-Verschlüsselung erwünscht, damit der Anbieter nicht mitlesen kann
- Separater Speicher kann erwünscht sein
- Verschwindende Nachrichten können erwünscht sein

- Also Rangfolge



- Sonderrolle: 

Kommunikationsumstände und andere Datensammlung

Metadaten und Identifikation der Teilnehmer

Metadaten

- Auf dem vermittelnden Server immer sichtbar
- Fragen
  - Wie lange werden die Daten gespeichert?
  - Werden die vom Anbieter ausgewertet?
  - Wie sieht das Datenschutzniveau beim Anbieter aus?

Identifikation der Kommunikationspartner

- Telefonnummer?
- E-Mail-Adresse?
- eigene Identifikationsmerkmale

Verifikation des Kommunikationspartners

- Überprüfung bei persönlichem Kontakt mit QR-Code

Kommunikationsumstände und andere Datensammlung

Datensammlung, Gruppen und Informationen von und zu Nutzenden

Datensammlungen

- Auslesen von Adressbüchern
  - Nur Telefonnummern oder mehr?
  - Speicherung der ausgelesene Daten beim Anbieter?
  - Nutzung nur mit Zugriff auf Adressenbuch möglich?

Speicherung von Daten zu Gruppen

- Auf dem Server?
- Nur auf Endgeräten?

Informationen von und zu Nutzenden

- Profilbilder
  - Auf Server für Anbieter sichtbar?
- Statusinformationen
  - Auf Server für Anbieter sichtbar?
- Zuletzt online
  - Abschaltbar?
  - Für wen sichtbar?

Wenn interessiert schon, wer mit wem kommuniziert?

Fazit Kommunikationsumstände

… vor allem eine Datenschutzfrage

Auslesen des Adressbuchs	✓	✓	✓	✓	✗
Speicherung von Telefonnummern aus Adressbuch beim Anbieter	✓	✗	✗	✗	✗
Speicherung von weiteren Adressbuchinhalten beim Anbieter	✓	✗	✗	✗	✗
Kommunikation unabhängig von Telefonnummern	✗	✗	✓	✗	✓

Speicherung von Metadaten beim Anbieter	✓	✓	✓	✓	✓
Auswertung von Metadaten durch Anbieter	✓	✗	✗	✗	?
Teilung von Daten mit Konzern	✓	✗	✗	✗	✗
EU-Datenschutz konform	✗	✗	✓	✗	✓
Speicherung von Gruppen beim Anbieter	✓	✗	✗	✓	✓

Fazit

Allgemein

- Informationssicherheit
  - Messenger mit Ende-zu-Ende-Verschlüsselung bieten eine vertrauliche Kommunikation (anders als z.B. E-Mail)
  - Zu klären: Dürfen die übermittelten Daten auf dem Smartphone sein / gespeichert werden
- Datenschutz
  - Ist es problematisch, wenn ermittelt werden kann, wer mit wem, wann und mit welchem Umfang kommuniziert?
  - Problem der Datenweitergabe bei Übermittlung von Daten aus Adressbüchern
    - Einwilligung als Rechtsgrundlage?
  - Problematik von Profilbildern, Statusmitteilungen, Onlinestatus

Fazit

… zu den einzelnen Messengern

- **Whatsup**: Sichere Kommunikation, aber Probleme mit Datenschutz, insbesondere unklarer Zugriff auf Adressbuch, US-Firma und dadurch Datenschutz nicht EU-konform, Zweifel bei Datenaustausch mit Facebook
- **Signal**: Sichere Kommunikation, bessere Isolierung von Inhalten gegenüber anderen Apps, datenschutz-freundliche Zusagen, aber US-Firma und Server in USA
- **Threema**: Sichere Kommunikation, bessere Isolierung von Inhalten gegenüber anderen Apps, Verzicht auf Weitergabe von Telefonnummern möglich, Server in der Schweiz (EU-Datenschutzniveau)
- **Telegram**: im Standard keine Ende-zu-Ende-Verschlüsselung (nur optional), Server in Dubai, Nutzung auch von problematischen Gruppen, Betreiber vermeidet Eingriffe und Kooperation mit Behörden
- **Rocket Chat**: Freie Software für eigene Chat-Server, Identifikation über eigene Benutzerverwaltung, nicht öffentlich, Datenspeicherung auf Server, keine Ende-zu-Ende-Verschlüsselung
- … und weitere, insbesondere Messenger für Unternehmen und spezielle Gruppen

Danke

Fragen?

