CRYPTO PARTY

Themenschwerpunkt: Messenger

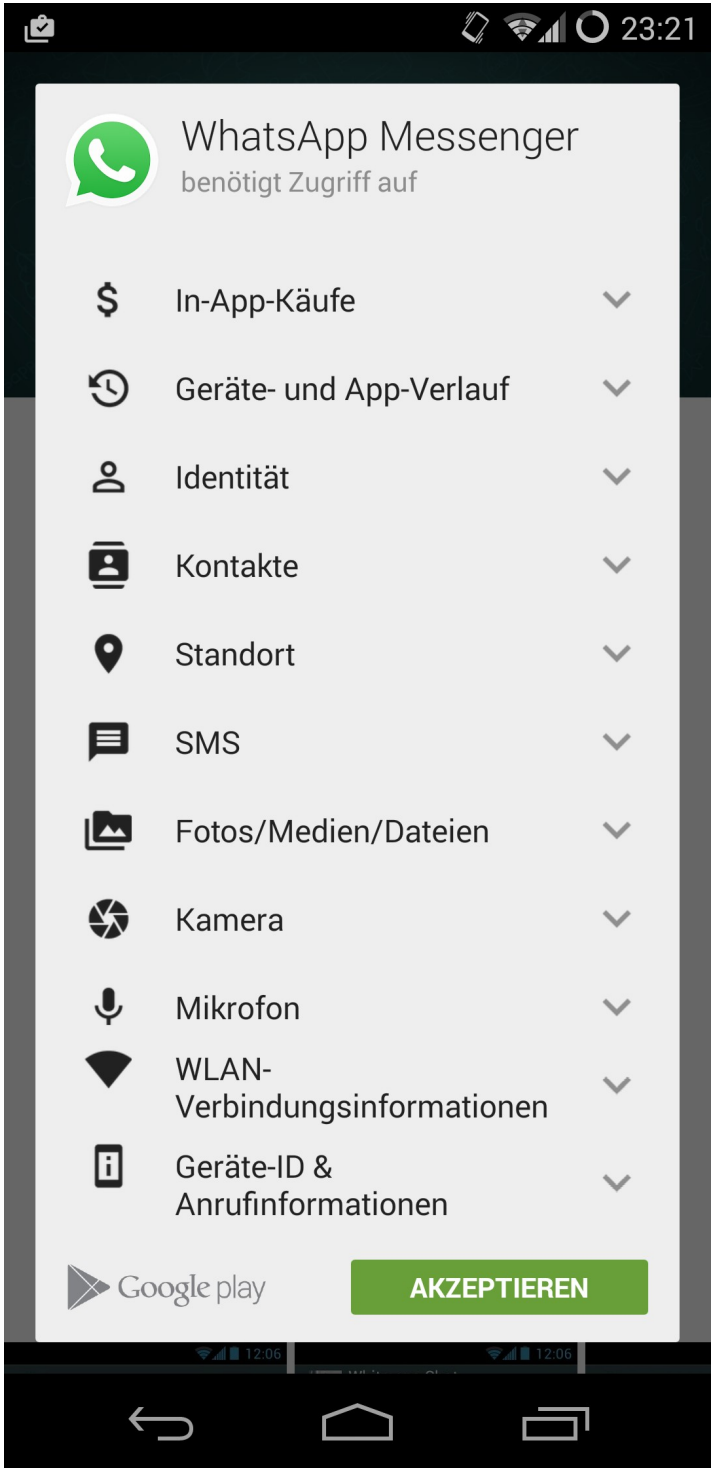
Wer sind wir?

Motivation

- Bei jeder Kommunikation fallen Daten an
  - Wer mit wem?
  - Wann?
  - Wo?
- Wer hat Zugriff auf diese Daten?
  - Der Diensteanbieter
  - Der Staat?
  - Kriminelle?

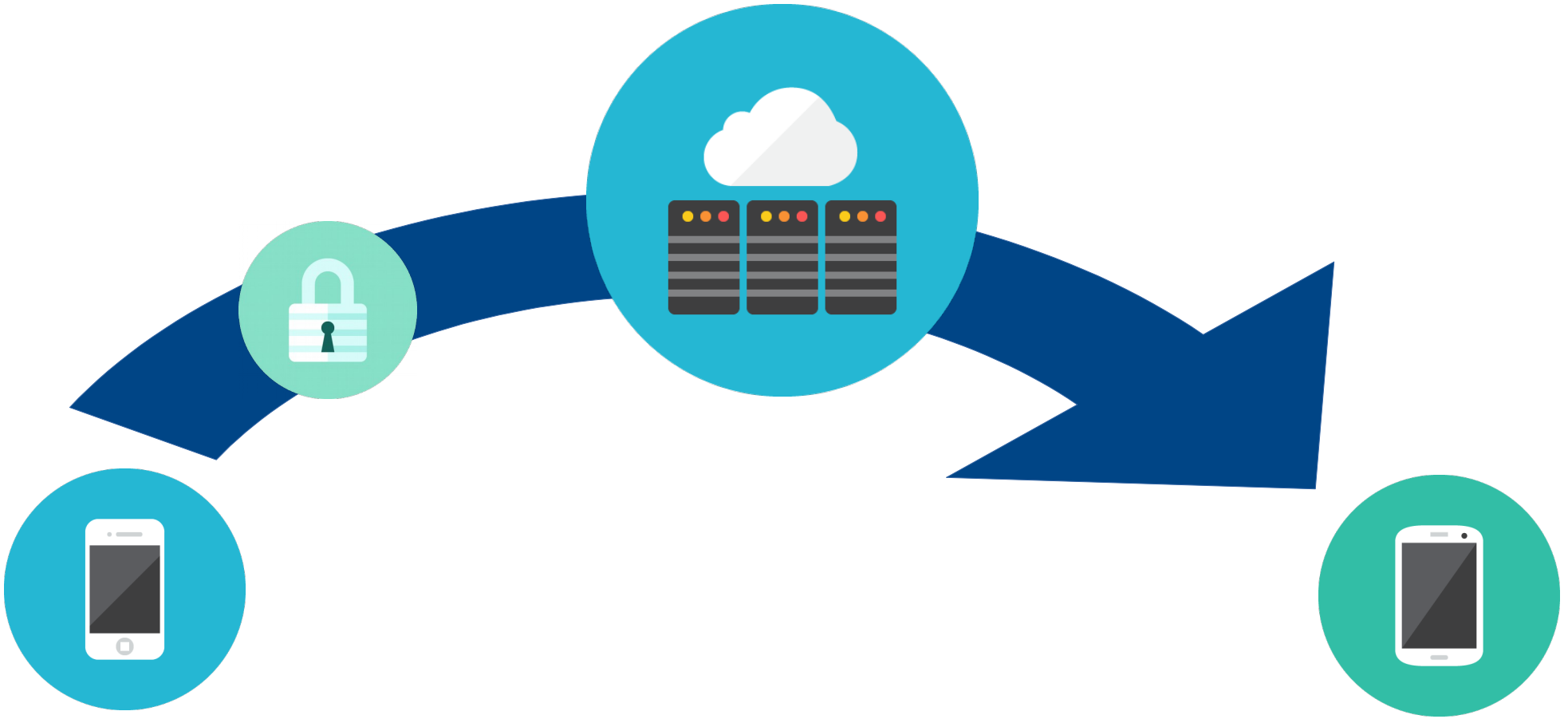
Was interessiert uns?

- Geschäftsmodelle
- Verschlüsselung
- Offenheit

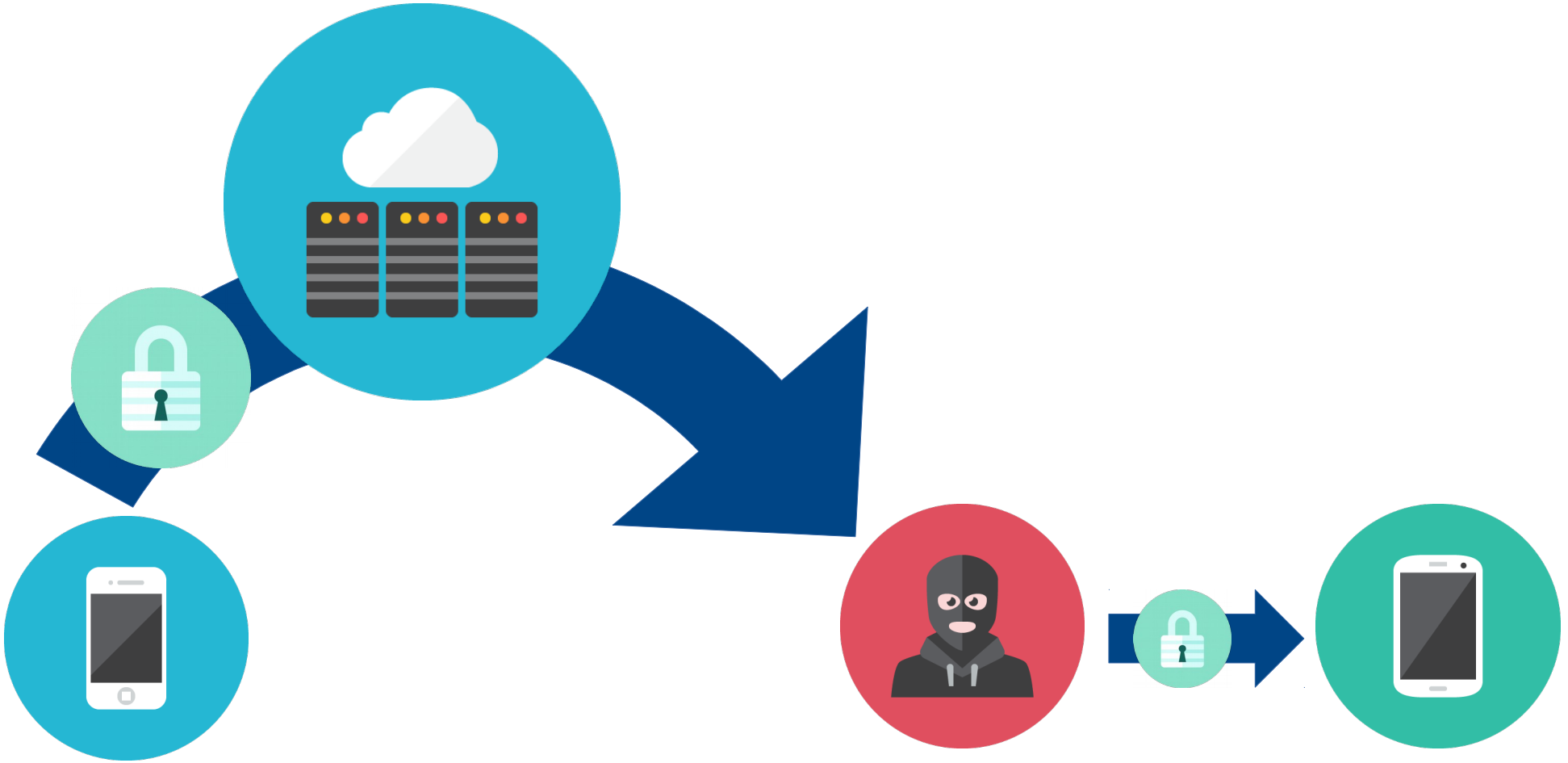

23:21
WhatsApp Messenger
benötigt Zugriff auf
In-App-Käufe
Geräte- und App-Verlauf
Identität
Kontakte
Standort
SMS
Fotos/Medien/Dateien
Kamera
Mikrofon
WLAN-Verbindungsinformationen
Geräte-ID & Anrufinformationen
Google play
AKZEPTIEREN

Transport-Verschlüsselung

Ende-zu-Ende-Verschlüsselung



Man in the Middle



WhatsApp

Transportverschlüsselung:
Ja.

Ende-zu-Ende-Verschlüsselung:
Nicht wirklich.

Plattformen:
Android, iOS, Windows Phone, BlackBerry, Symbian

Betreiber:
WhatsApp Inc. (USA), im Besitz von Facebook

Geschäftsmodell:
Verkauf der Software

Open Source:
Nein

Facebook Messenger

Transportverschlüsselung:
Ja.

Ende-zu-Ende-Verschlüsselung:
Nein.

Plattformen:
Android, iOS, Windows Phone, BlackBerry

Betreiber:
Facebook (USA)

Geschäftsmodell:
Verkauf von Werbung

Open Source:
Nein

iMessage

Transportverschlüsselung:
Ja.

Ende-zu-Ende-Verschlüsselung:
Ja, evtl. Man-in-the-Middle-anfällig

Plattformen:
iOS

Betreiber:
Apple

Geschäftsmodell:
Verkauf der Software und Geräte

Open Source:
Nein

Threema

Transportverschlüsselung:
Ja.

Ende-zu-Ende-Verschlüsselung:
Ja.

Plattformen:
Android, iOS, Windows Phone

Betreiber:
Threema GmbH (CH)

Geschäftsmodell:
Verkauf der Software

Open Source:
Nein

Telegram

Transportverschlüsselung:
Ja.

Ende-zu-Ende-Verschlüsselung:
Ja, aber Sicherheit ist unklar.

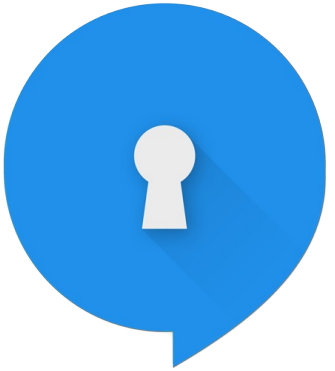
Plattformen:
Android, iOS, Windows Phone

Betreiber:
Telegram Messenger LLP

Geschäftsmodell:
Spenden, Stiftungen

Open Source:
Großteils

TextSecure / Signal



Transportverschlüsselung:
Ja.

Ende-zu-Ende-Verschlüsselung:
Ja.

Plattformen:
Android, iOS

Betreiber:
Open Whisper Systems

Geschäftsmodell:
Spenden, Stiftungen

Open Source:
Komplett

Also was nun?

TextSecure / Signal

Telegram
Threema

WhatsApp
Facebook Messenger

Vielen Dank!

Material und Links:
www.cryptoparty-hd.de

Weitere Termine:
E-Mails: 17.6. INF 368, 22.6. hier
Anonymität: 29.6. INF 368

Quellennachweise

- Wikipedia
- https://threema.ch/press-files/cryptography_whitepaper.pdf
- http://www.apple.com/business/docs/iOS_Security_Guide.pdf