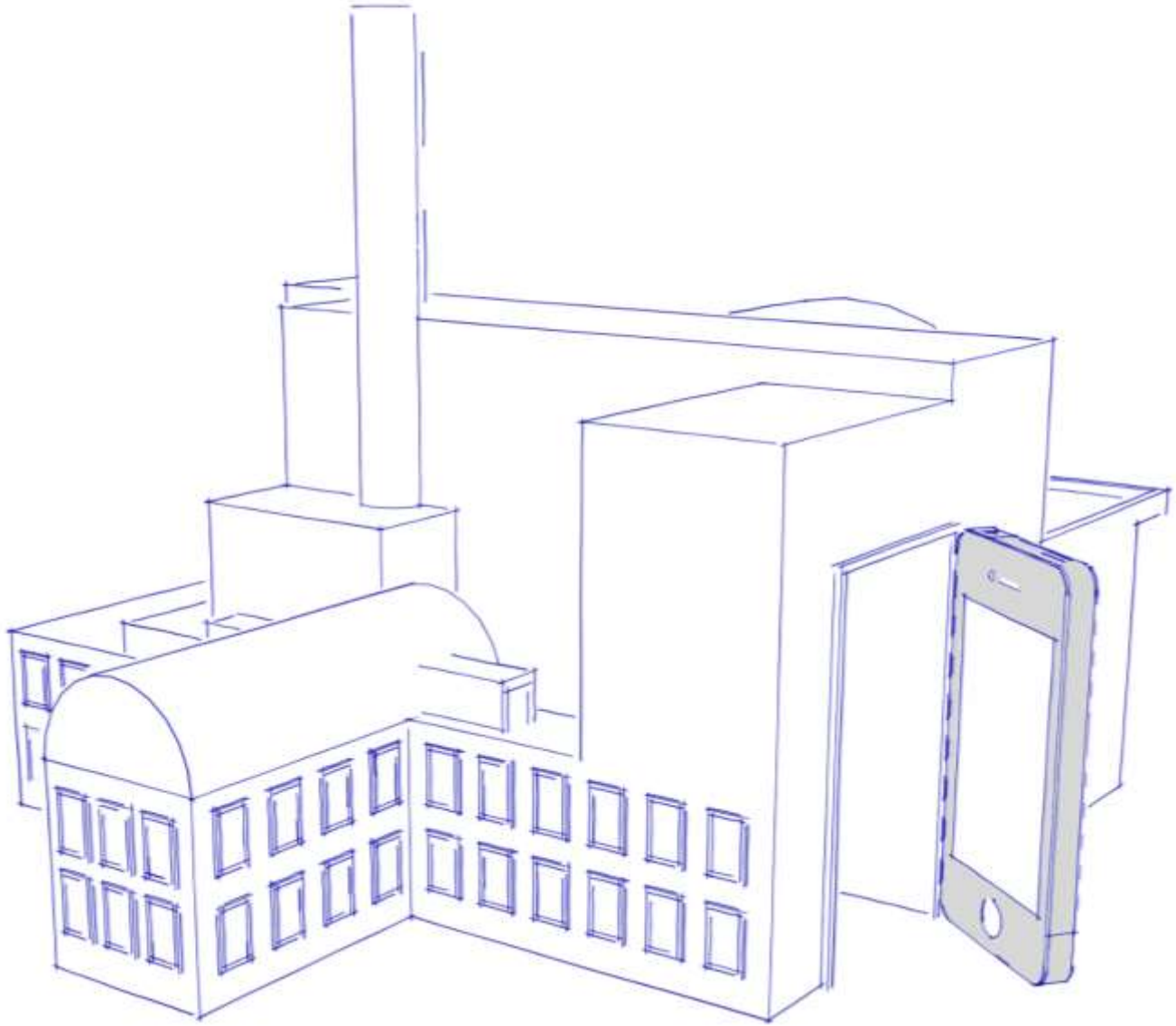
App-Sicherheit - Automatisierte Analyse für den Unternehmensschutz



Apps als **Einfallstor für Angriffe** auf Ihr Unternehmen

Apps im Unternehmenseinsatz

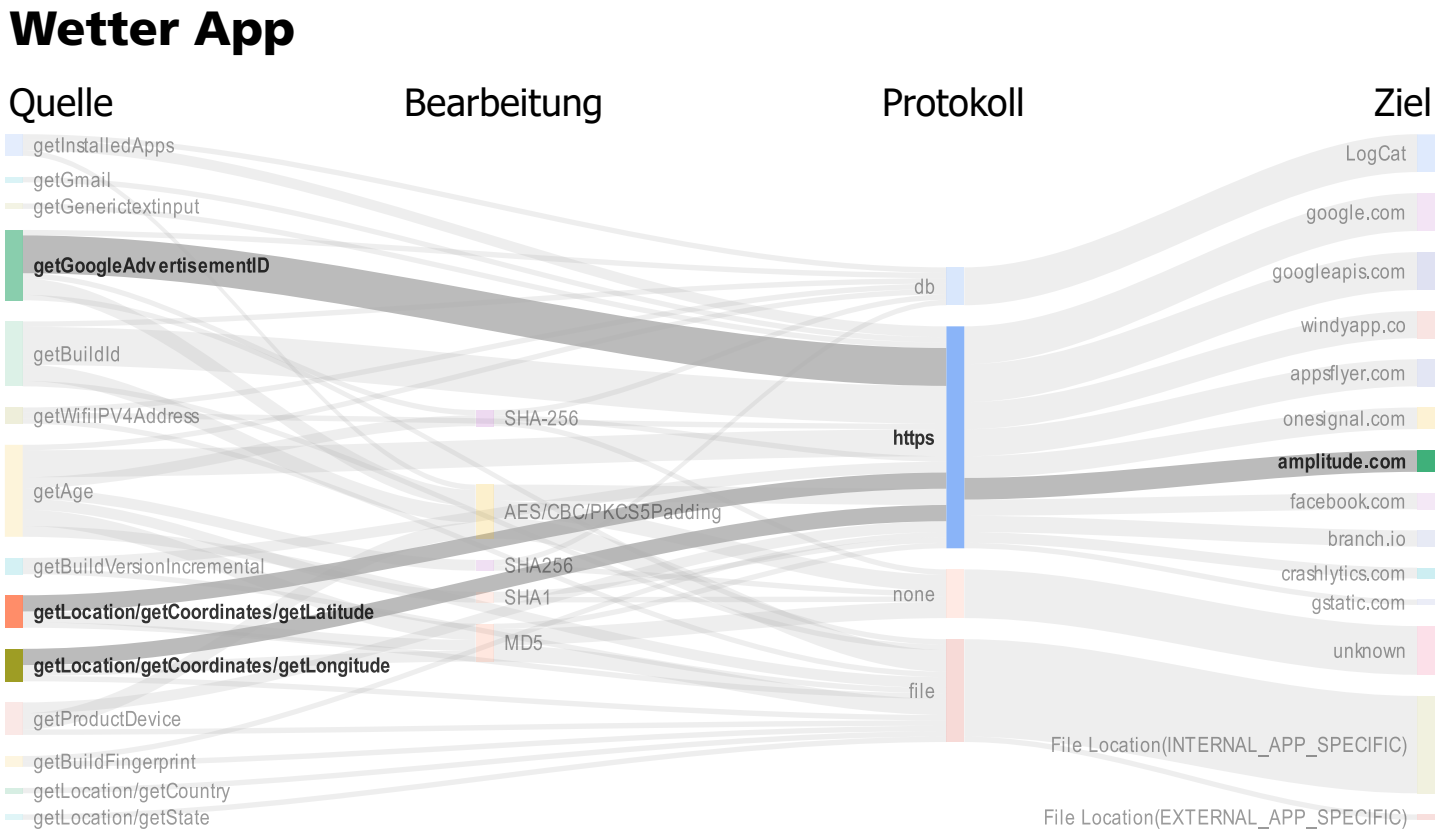
- Apps verarbeiten Unternehmensdaten
  - Daten durch Sandbox gegen andere Apps geschützt
  - Prüfung der Apps im App Store
  - Berechtigungen schützen Datenzugriffe
  - Weiterer Schutz abhängig von App-Programmierung
    - Speicherort
    - Verschlüsselung / Kryptographie
    - Datenschnittstellen
    - Nutzerschnittstellen
    - Kommunikation

Auszug Appicaptor Top 2000 iOS Analyse, Oktober 2022

Datenflüsse zu Fremdanbietern

Beispiel: GPS-Daten

- Berechtigungsnutzung
  - Freigabe für Positionsbestimmung zum Wetterabruf nachvollziehbar
  - Drittanbieter-Bibliotheken nutzen erteilte Berechtigung ebenfalls
  - Drittanbieter erhält kontinuierliche Position der Mitarbeiter bei App-Nutzung

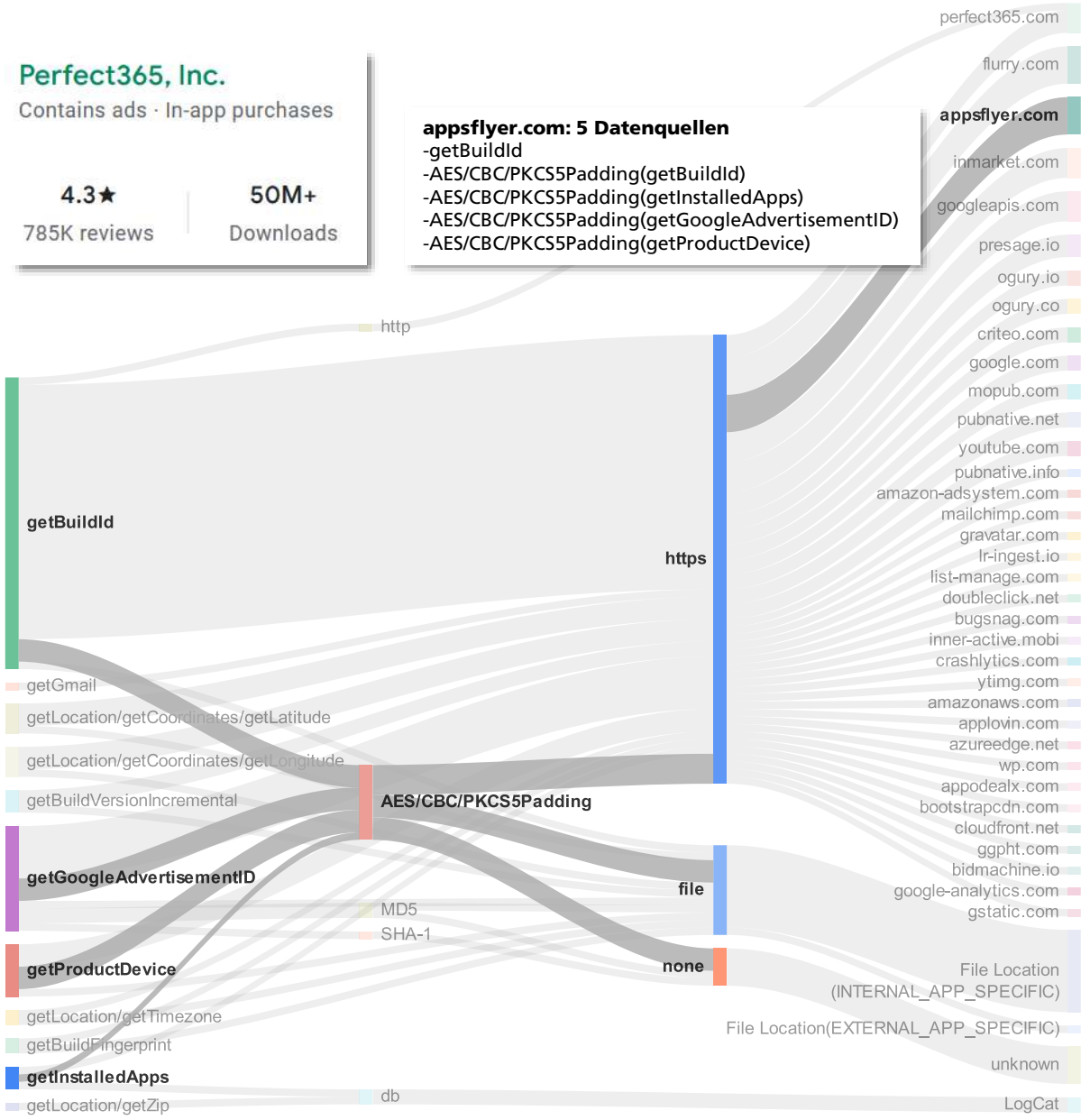


Auszug dynamische Datenflussanalyse: PANDERAM BMBF Projekt

Datenflüsse zu Drittanbietern

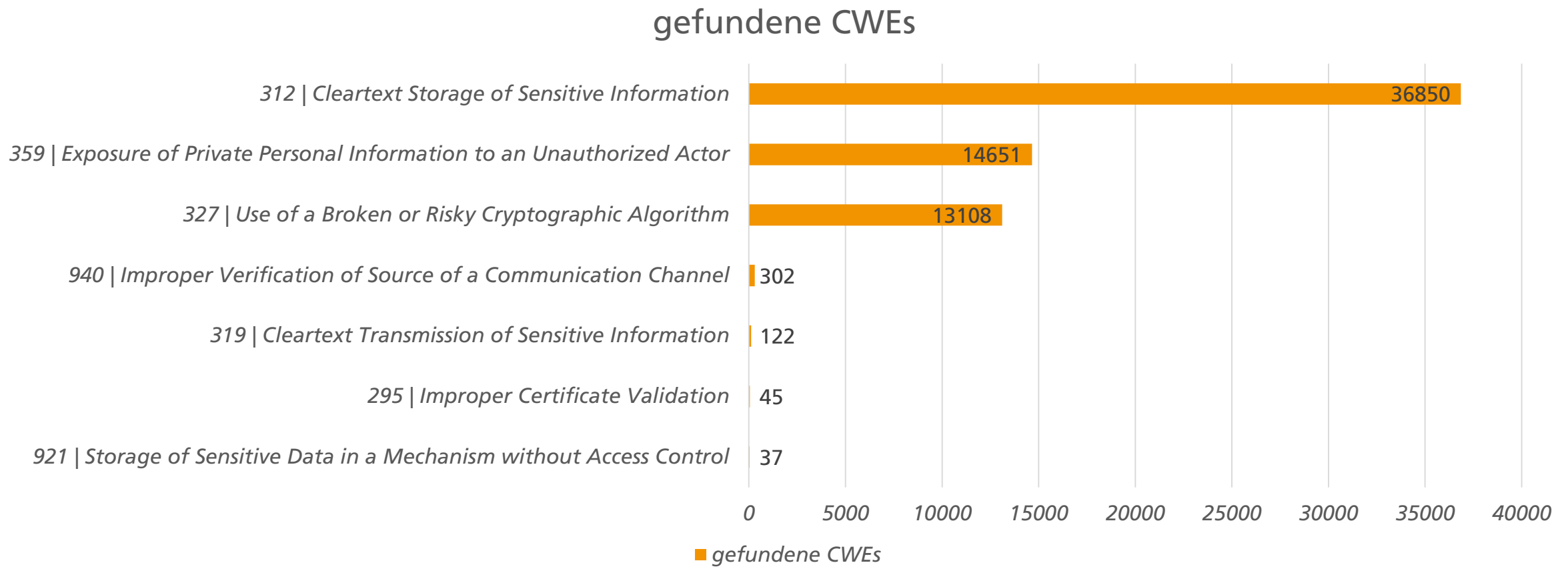
Beispiel: Endpunkte und Verschlüsselung

- Interaktionen mit Drittanbietern
  - Drittanbieter nutzen Verschlüsselung auf Anwendungsebene
  - Neben Domain des Appanbieters erhalten 34 weitere Drittanbieter Informationen über App-Nutzung
  - App Stores geben zwar inzwischen die Datenarten an, die von der App gesammelt werden, aber nicht mit wie vielen diese Information geteilt wird



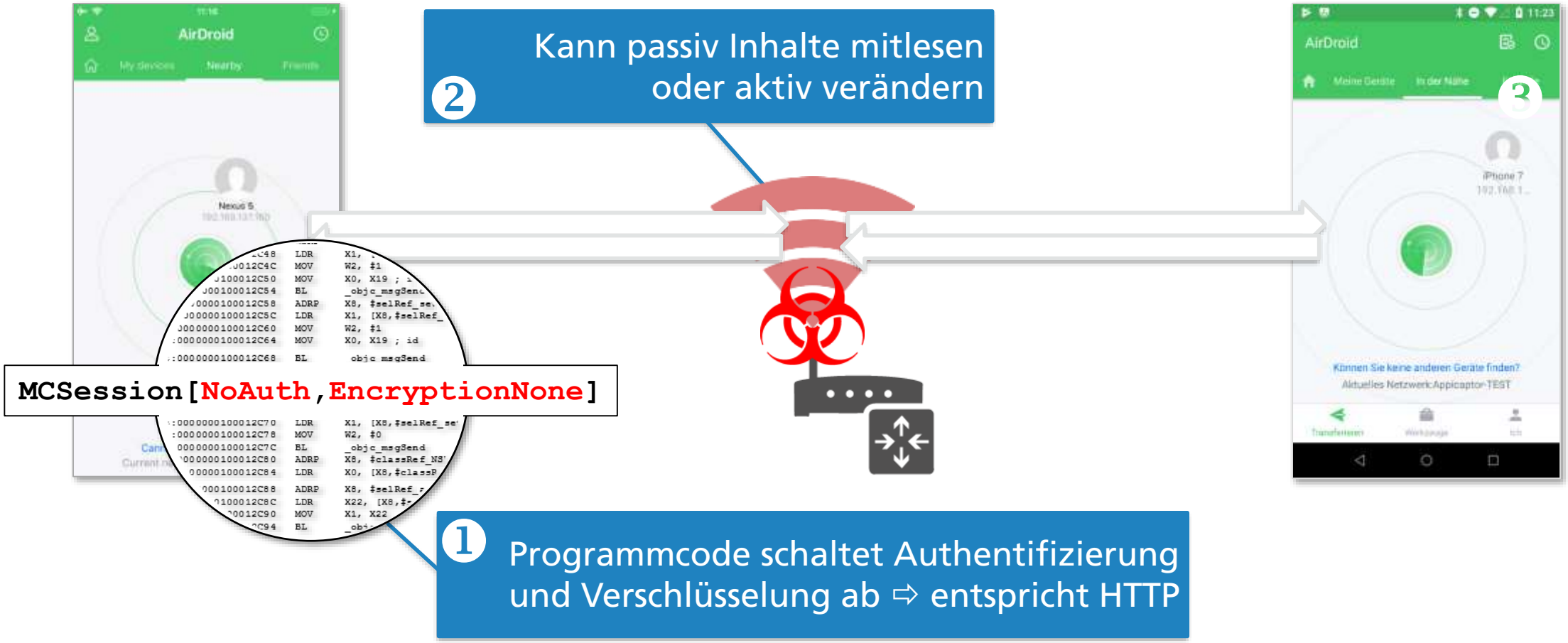
Auszug dynamische Datenflussanalyse: PANDERAM BMBF Projekt

Analyse der Top 1000 Android Apps
Common Weakness Enumeration



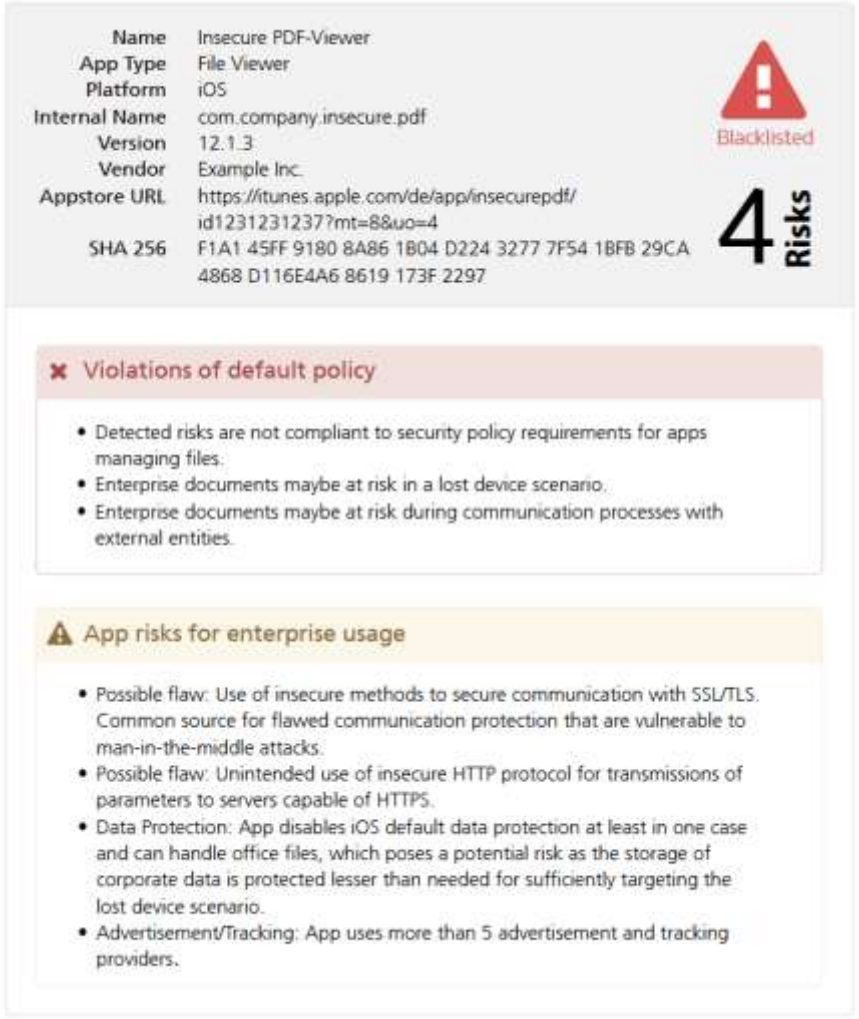
Auszug dynamische Datenflussanalyse: PANDERAM BMBF Projekt

Fehlende **App-Sicherheitsqualität** gefährdet Unternehmen: *Schlechte / Fehlende Kryptographie*



AirDroid: Version 1.0.3

Freigabe- und Prüfkonzept für Apps notwendig



Name	Insecure PDF-Viewer
App Type	File Viewer
Platform	iOS
Internal Name	com.company.insecure.pdf
Version	12.1.3
Vendor	Example Inc.
Appstore URL	https://itunes.apple.com/de/app/insecurepdf/id1231231237?mt=8&uo=4
SHA 256	F1A1 45FF 9180 8A86 1B04 D224 3277 7F54 1BFB 29CA 4868 D116E4A6 8619 173F 2297

Blacklisted

4 Risks

Violations of default policy

- Detected risks are not compliant to security policy requirements for apps managing files.
- Enterprise documents maybe at risk in a lost device scenario.
- Enterprise documents maybe at risk during communication processes with external entities.

App risks for enterprise usage

- Possible flaw: Use of insecure methods to secure communication with SSL/TLS. Common source for flawed communication protection that are vulnerable to man-in-the-middle attacks.
- Possible flaw: Unintended use of insecure HTTP protocol for transmissions of parameters to servers capable of HTTPS.
- Data Protection: App disables iOS default data protection at least in one case and can handle office files, which poses a potential risk as the storage of corporate data is protected lesser than needed for sufficiently targeting the lost device scenario.
- Advertisement/Tracking: App uses more than 5 advertisement and tracking providers.

- App-Sicherheit: Thema für alle Unternehmen, unabhängig von Gerätestrategie
- Einschätzung der Sicherheitsqualität nur durch Audit oder Code-Analyse möglich
- Ohne Automatisierung nur für kleine App-Auswahl wirtschaftlich
- Zyklische Wiederholung der Tests ermöglichen

- Sicherheitskonzept: Reaktiv oder Proaktiv
  - Analyse Inventar + Blacklisting
  - Analyse Interner App-Store + Freigabekonzept

Automatisierte App-Sicherheitsanalyse mit Appicaptor

- Ihr Weg zu Appicaptor
  - Appicaptor auf der it-sa 2022: Fraunhofer-Gesellschaft (Stand 210 in Halle 6)
  - Individuelle Live Demo für Sie und Ihre Kollegen (auf der Messe oder im Nachgang)
  - Testen Sie den Appicaptor-Dienst einen Monat kostenlos

  - Kontaktieren Sie uns
    - E-Mail: appicaptor@sit.fraunhofer.de
    - Webseite: www.appicaptor.de