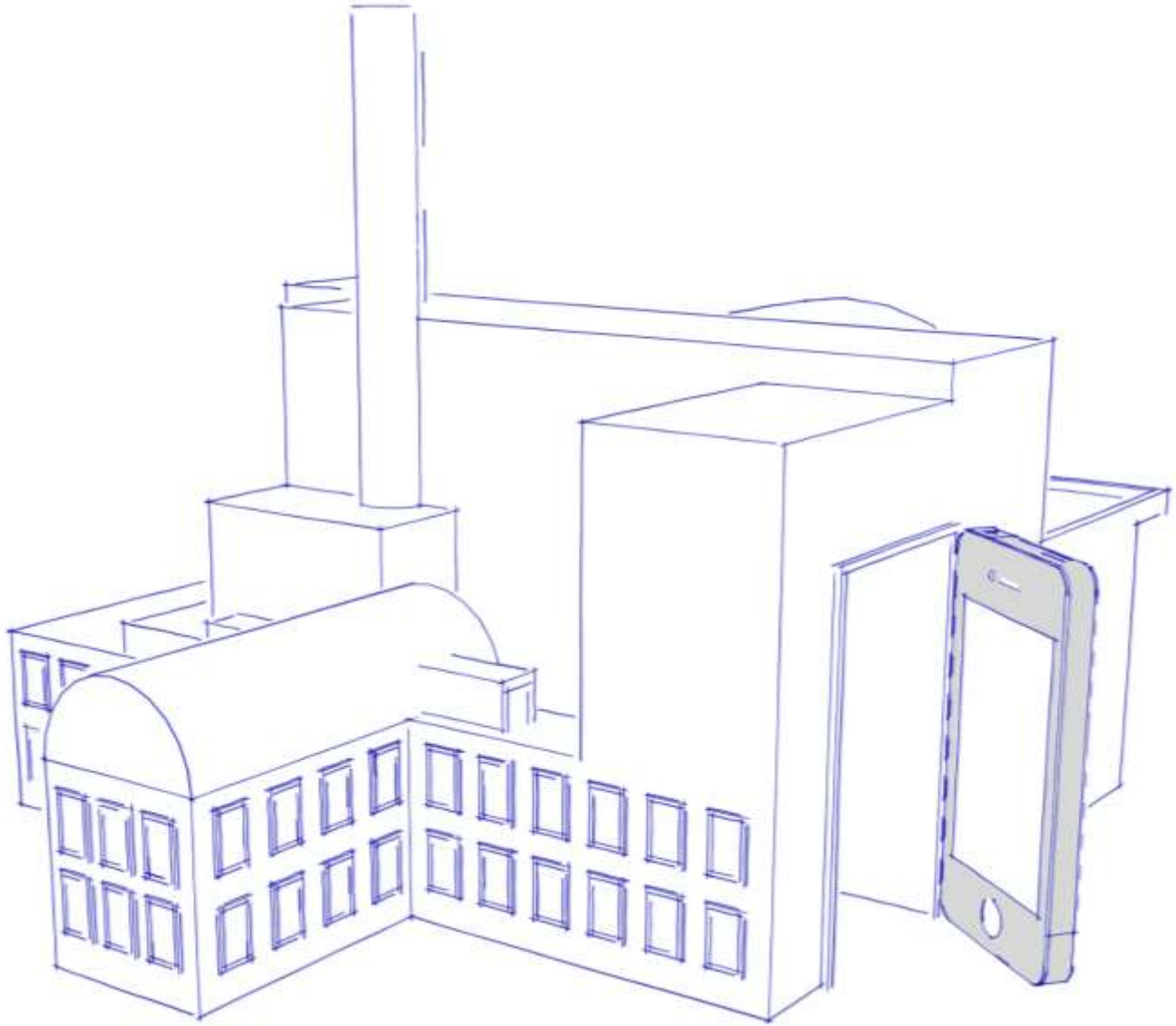
App-Sicherheit - Automatisierte Analyse für den Unternehmensschutz



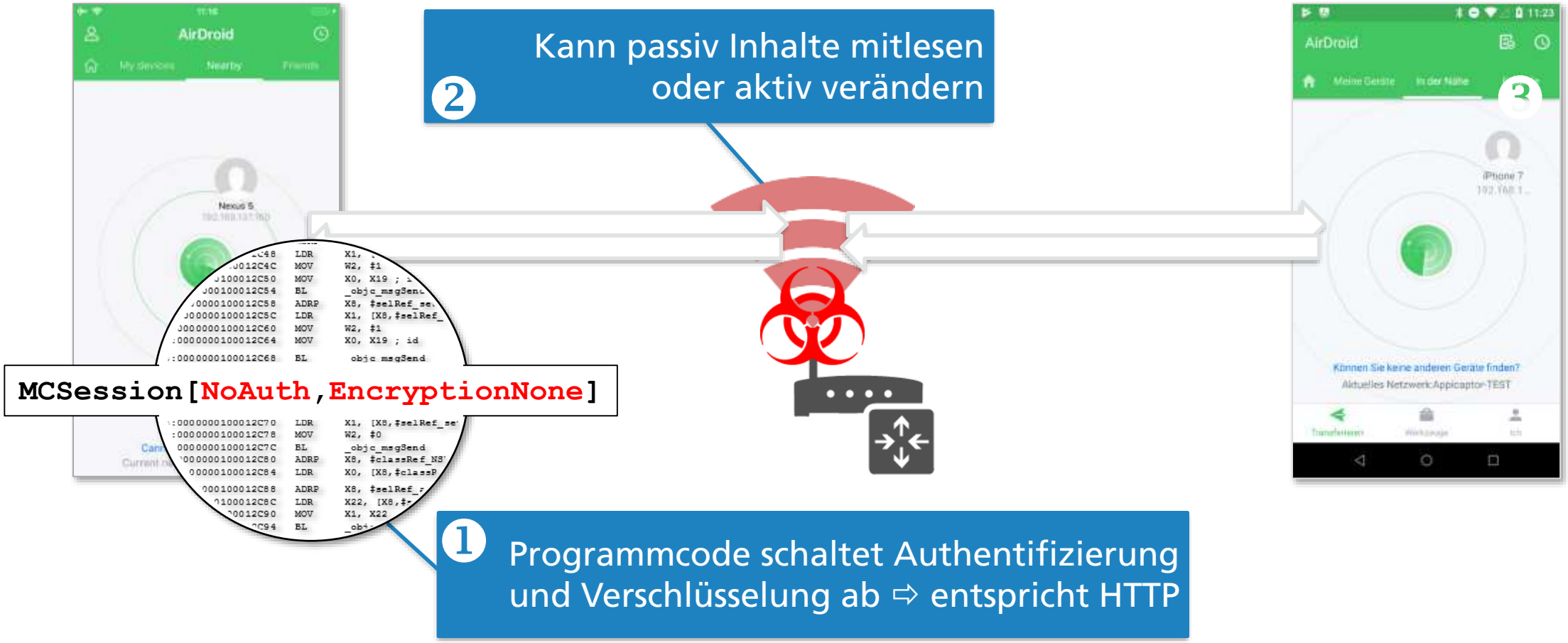
Apps als **Einfallstor für Angriffe** auf Ihr Unternehmen

Fehlende **App-Sicherheitsqualität** gefährdet Unternehmen: ***Verwundbare Bibliotheken***

- **TwitterKit for iOS** enthält Fehler bei TLS-Zertifikatsprüfung
  - Ermöglicht Mitlesen von Nachrichten und OAuth-Token
  - Detektiert durch statische Binär-Code-Analyse
  - Bibliothek weit verbreitet, trotz End-of-Life im Okt. 2018
  - Twitter hat Verwundbarkeit bestätigt, wird wegen End-of-Life aber nicht patchen
- Verwundbarkeiten in Bibliotheken verbleiben lange in Apps
  - AFNetworking-Verwundbarkeit nach 4 Jahren noch in Top 2000 iOS Apps vertreten (CVE-2015-3996)

TwitterKit for iOS <= 3.4.2, CVE-2019-16263

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

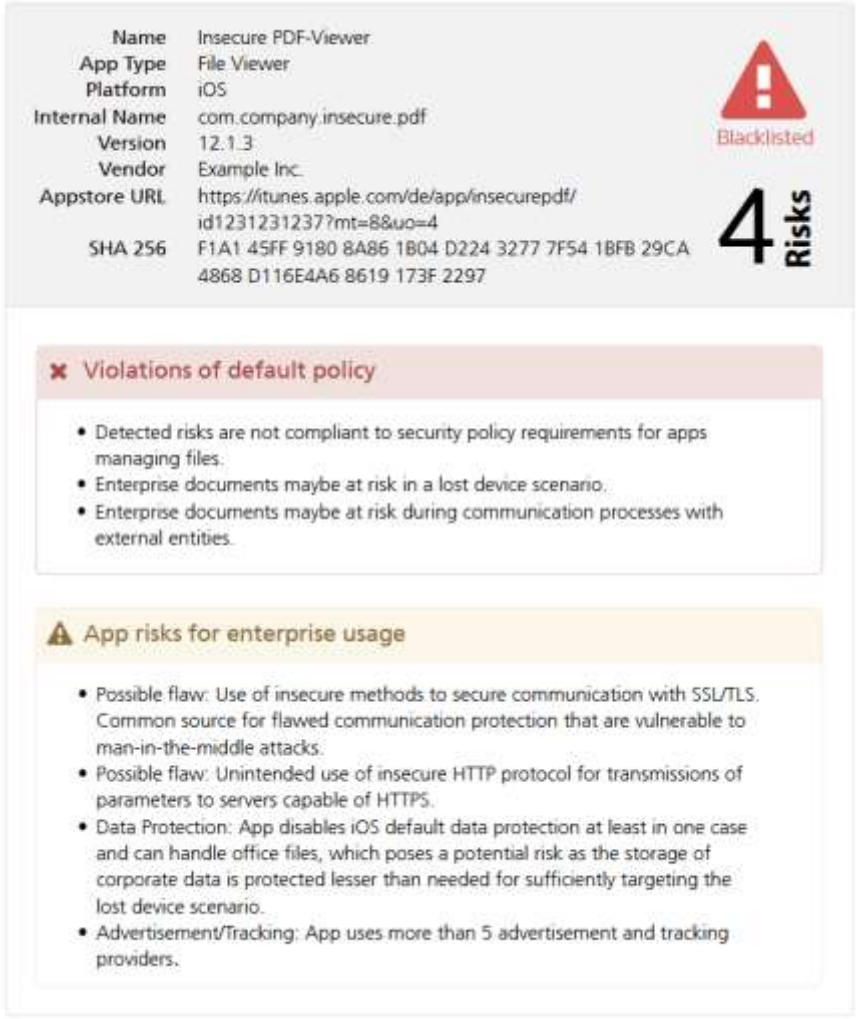


AirDroid: Version 1.0.3

Fehlende **App-Sicherheitsqualität** gefährdet Unternehmen: ***Missbrauch von Funktionalität***

rbb|24: Version 1.9.3

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.

- Apps: 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 2019: Fraunhofer-Gesellschaft (Stand 234 in Halle 9)
  - 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