Tobias Scheible, M.Eng.

IT-Forensik

Digitale Spurensuche im Tatort Software

Tobias Scheible, M.Eng.

Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

- 1999 GeoCities Website, 2000 eigene Domain, 2001 erste Projekte
- 2009 bis 2012: Softwareingenieur im Bereich Web Development
- Seit 2012: Wissenschaftlicher Mitarbeiter
  - BMBF gefördertes Forschungsprojekt SEKT (IT Security & Smart Textiles)
  - Aktuelle & ehemalige Lehrmodule (Auswahl):
    - Grundlagen der digitalen Forensik Masterstudiengang IT GRC Management
    - Digitale Forensik Bachelorstudiengang IT Security
    - Internet Grundlagen Masterstudiengang Digitale Forensik
    - Cybersecurity Bachelorstudiengang IT Security
    - Internettechnologien Hochschulzertifikatsprogramm
    - Cloud Technologies and Cloud Security Architectures Masterstudiengang IT GRC
- Blog scheible.it | Zeitschriftenartikel | Vorträge und Workshops

Agenda

- IT-Forensik
  - Digitale Spuren
  - Forensische Untersuchung
  - Analysemethoden
  - Untersuchungsprozess
- Einsatzszenarien für IT-Forensik
  - Aufklärung von Straftaten
  - Analyse von IT-Angriffen
  - Behebung von Fehlfunktionen
  - Untersuchung von Closed-Source-Software
- IT-Forensik in Unternehmen
  - Interne Spannungsfelder
  - Rechtliche Anforderungen
  - Untersuchungen
- Forensic Readiness
  - Effektives Logging
  - Schutz vor Manipulationen
  - Integritätsverifiaktion
  - Digitale Signaturen

Hinweis

Die kompletten Folien der Präsentation mit Zusatzinformationen werden im Blog unter *www.scheible.it* bereitgestellt.

IT-Forensik

IT-Sicherheit vs. IT-Forensik

IT-Sicherheit

Was könnte passieren?

IT-Forensik

Was ist passiert?

IT-Forensik

Bei der digitalen Forensik, auch als IT Forensik bzw. Computer Forensik bezeichnet, geht es um die Untersuchung eines Rechnersystems nach einem Vorfall. In diesem Sinne wird die digitale Forensik als Analyse von digitalen Spuren zur Aufklärung von Vorfällen betrachtet.

Fachdisziplinen

- Datenspeicher-Forensik
- Betriebssystem-Forensik
- Anwendungs-Forensik
- Netzwerk-Forensik

Spezialdisziplinen

- Mobilgeräte-Forensik
- Multimedia-Forensik
- Cloud-Forensik
- Hardware-Forensik
- Malware-Forensik
- Speicher-Forensik

Digitale Spuren

- Digitale Spuren können exakt dupliziert werden

- Flüchtigkeit
  - Können automatisiert überschrieben werden
  - Stehen nur mit einer Stromverbindung zur Verfügung
- Zuordenbarkeit
  - Digitale Spuren sind nicht personenbezogen
  - Ausschließliche Beweisführung aufgrund von digitalen Spuren ist nicht durchführbar
- Manipulation
  - Digitale Spuren können leicht manipuliert werden

Forensische Untersuchung

- Wie bei anderen Untersuchungen im Ermittlungsbereich können auch hier die 7 W-Fragen der Kriminalistik angewendet werden. Damit soll ein behaupteter Vorgang bewiesen oder widerlegt werden.
  - Wer? Was? Wo? Wann? Womit? Wie? Weshalb?

- Zur gerichtsverwertbaren Sicherung digitaler Spuren muss die Untersuchung nach etablierten Standards streng methodisch und jederzeit nachweisbar erfolgen.

- Ermittlungen wegen:
  Tötungsdelikten, Terrorismus, Kinderpornographie, Betrug, Diebstahl, Copyright-Verletzung, Datendiebstahl, Schadsoftware, Garantiefälle, Versicherungsnachweis, Audits, …

Analysemethoden

Post-Mortem Analyse findet die Untersuchung nach einem Vorfall statt. Dies geschieht im Wesentlichen durch die Untersuchung von Datenträgern der betroffenen Rechnersysteme.

- Vorteile
  - Keine Veränderung der Daten und keine Zeitbeschränkung
  - Infizierte Systeme können direkt ausgeschalten werden

- Nachteile
  - Schadsoftware, die sich nur im Arbeitsspeicher befindet, bleibt unerkannt
  - Passwörter, die sich im Arbeitsspeicher befinden, gehen verloren

Analysemethoden

Bei der Live-Analyse wird versucht, sogenannte flüchtige Daten zu gewinnen und zu untersuchen. Diese beinhalten unter anderem den Hauptspeicherinhalt oder Informationen über bestehende Netzwerkverbindungen.

- Vorteile
  - Flüchtige Daten, wie laufende Prozesse, können analysiert werden
  - „Sensible“ Daten, wie Passwörter, können gespeichert werden

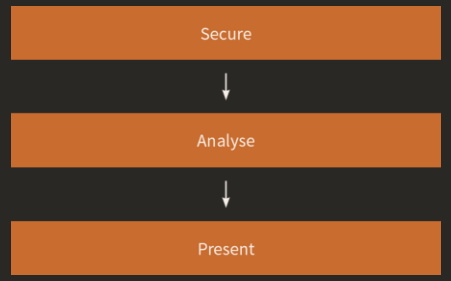
- Nachteile
  - Der Live-Analyse Prozess verändert immer die Daten
  - Relevante Daten können aus dem Arbeitsspeicher „verdrängt“ werden

Untersuchungsprozess

- Anforderungen an die Prozesse
  - Akzeptanz & Glaubwürdigkeit
  - Nachvollziehbarkeit & Wiederholbarkeit
  - Vollständigkeit & Integrität
- Allgemein anerkannte Standards: z.B. ISO/IEC 27035 ISO/IEC 27037

- Vorgehensmodelle

Secure-Analyse-Present Model



Incident Response Model

Investigative Process Model

Einsatzszenarien für IT-Forensik

Aufklärung von Straftaten

- Aufklärung von Cyber-Delikten - sehr breites Einsatzspektrum
  - Betrug durch manipulierte Informationen
  - Angriffe von Außen mit Tools und Schadsoftware
  - Manipulation und Diebstahl von Daten

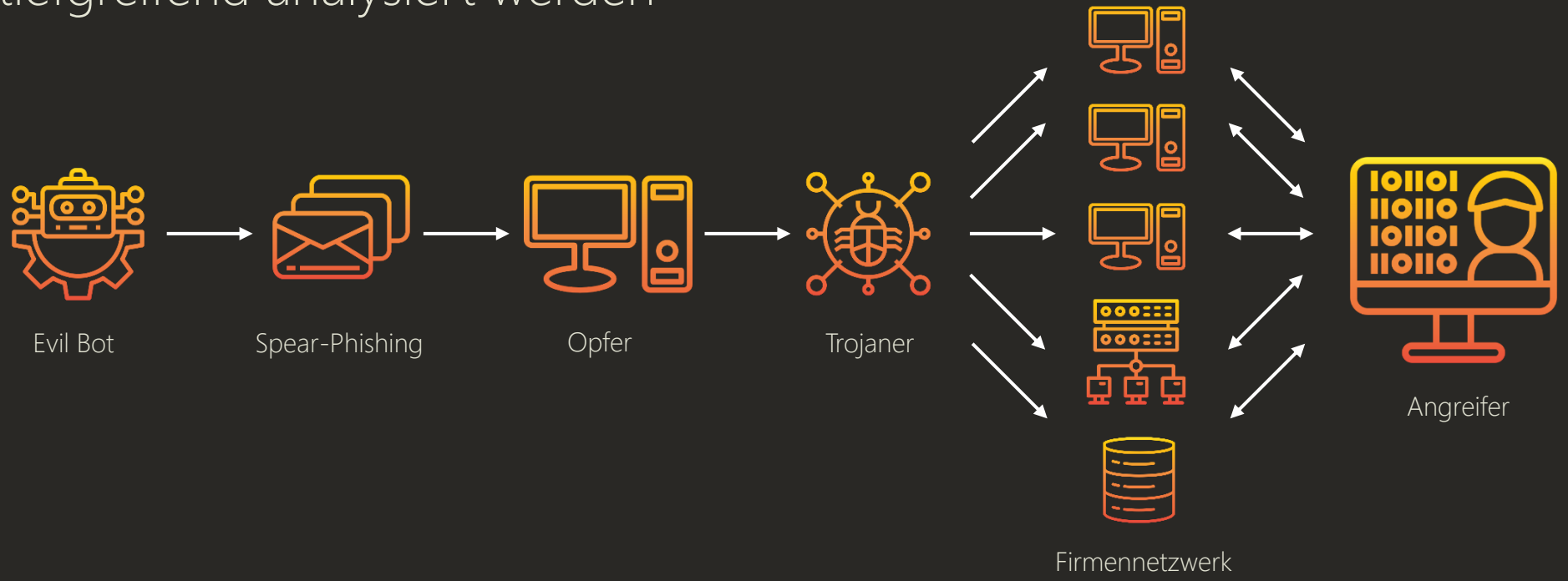
- IT-Forensik wird aber auch eingesetzt, um „klassische“ Straftaten im physischem Raum aufzuklären
  - Viele Spuren durch Wearables (z.B. Smart Wachts), Smartphones und integrierte Rechnersysteme (z.B. Navigationssysteme in Autos)
  - Werden von Tätern während einer Straftat genutzt und erzeugen Spuren

Beispiel
Smart Watch Bewegungsprofil

Beispiel
Smarter Wasserzähler

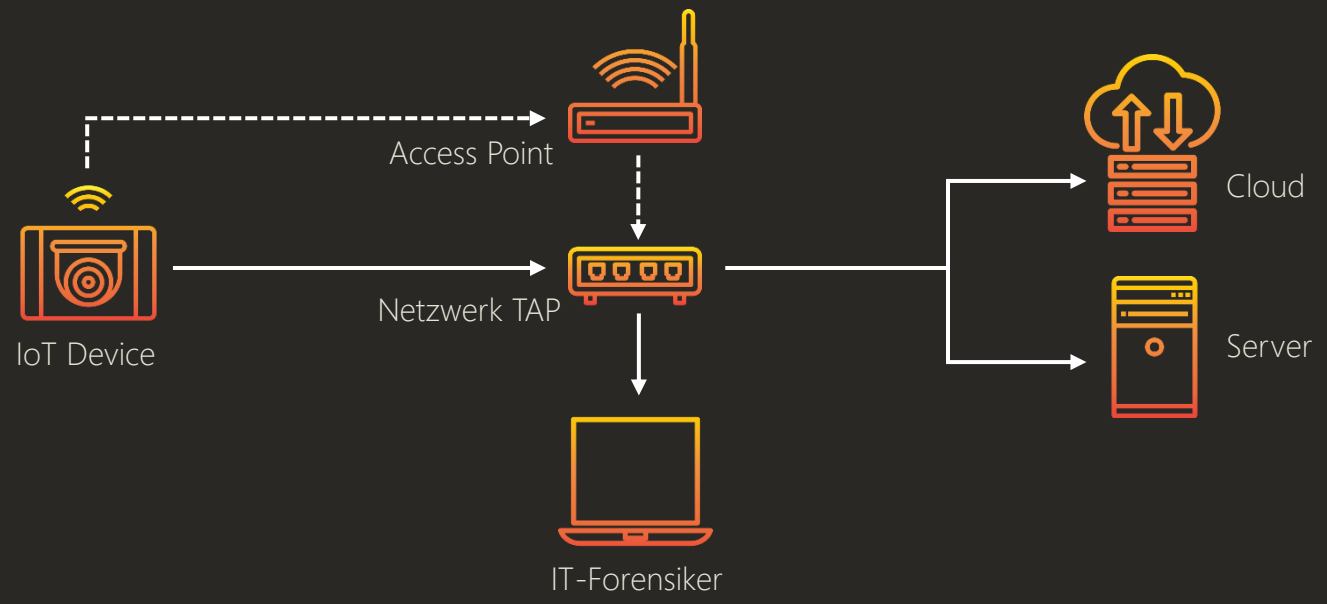
Analyse von IT-Angriffen

- Rekonstruktion, welches System wann und wie angegriffen wurde
- Mit entsprechenden Daten können Tools der Angreifer identifiziert werden
- Auch Angriffsversuche können mittels IT-Forensik tiefgreifend analysiert werden



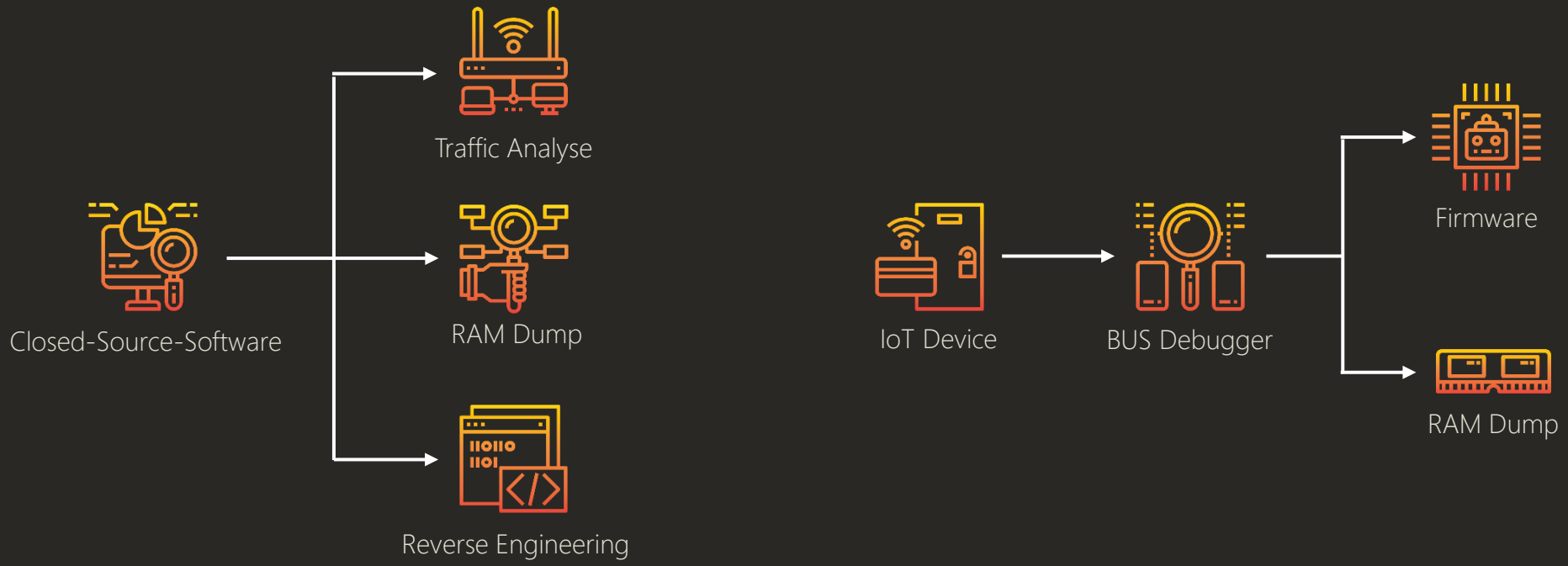
Behebung von Fehlfunktionen

- In Bereichen, die schwierig mit klassischen Entwicklungswerkzeugen zu debuggen sind
- Mittels der Methoden der Netzwerkforensik kann der komplette Datenstrom aufgezeichnet und analysiert werden
- Damit kann auch ein Fehler auf einer niedrigen Netzwerkschicht im Treiber entdeckt werden



Untersuchung von CS-Software

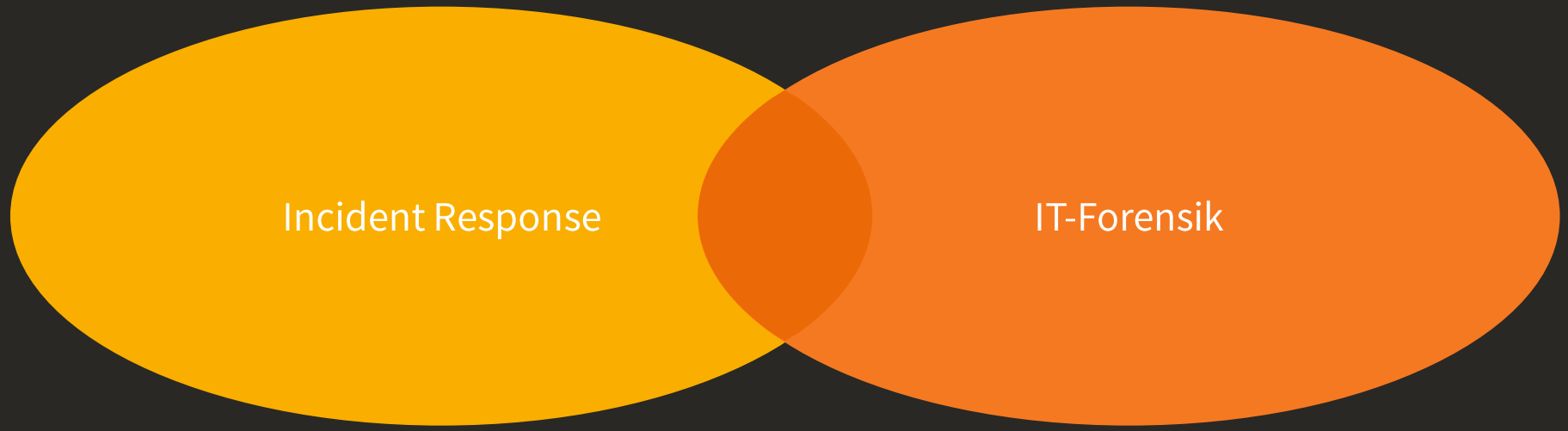
- Funktionsweise von Hardware- oder Software-Komponenten, aber auch Smartphones Apps, untersuchen
  - Datenverkehr über das Netzwerk wird aufgezeichnet
  - Reverse Engineering für Assembly-Code Analyse
  - Extraktion von Firmware aus Hardware zur Analyse



IT-Forensik in Unternehmen

Interne Spannungsfelder

Zielkonflikt zwischen Incident Response und IT-Forensik



- Möglichst schnelle „Beseitigung“ des Vorfalls und seiner Folgen
- Möglichst rasche Absicherung der Systeme, Beseitigung der Ursache des Vorfalls

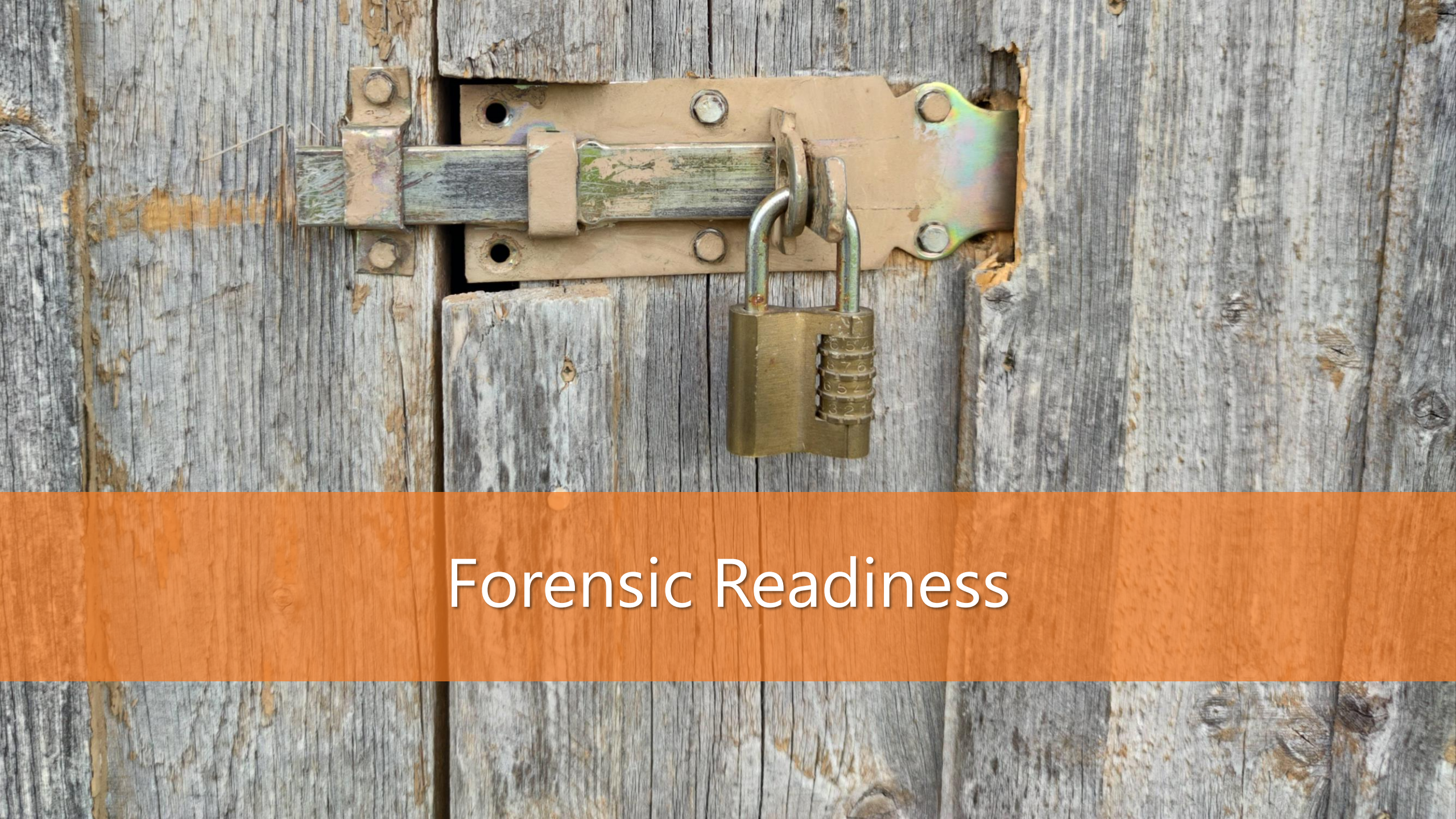
- Keinerlei Veränderung digitaler Spuren
- Systematische Sicherung der Spuren benötigt Zeit / Betriebsunterbrechung
- Aufarbeitung der gefundenen Spuren

Rechtliche Anforderungen

- Mehrere Anforderungen aus verschiedenen Bereichen
- Spannungsfeld zwischen Aufklärungswillen und -pflicht sowie Regelungen nach BDSG/DSGVO
  - IT-Forensik-Untersuchungen umfassen meist auch persönliche Daten
  - Anonymisierung der Datensätze, die untersucht werden
  - Erst bei konkreten Beweisen und weiterer Verfolgung erfolgt eine Zuordnung

Untersuchungen

- Vorgänge rekonstruieren
  - Bei Anomalien kann die IT-Forensik eingesetzt werden, um die Ausgangslage zu sondieren
  - Zum Beispiel wird ein interner Ablauf rekonstruiert, um das weitere Vorgehen auf Basis der erhobenen Daten zu entscheiden
  - Dazu gehört auch, ob die Police einer Versicherung zur Anwendung kommt oder nicht
  - Dabei arbeiten die IT-, Rechts- und Personalabteilungen zusammen
- Analyse des Ist-Zustands
  - Anlassunabhängige Compliance-Prüfungen durchführen
  - Kontrolle von Abläufen und Prozessen mittels forensischer Untersuchungsmethoden



Forensic Readiness

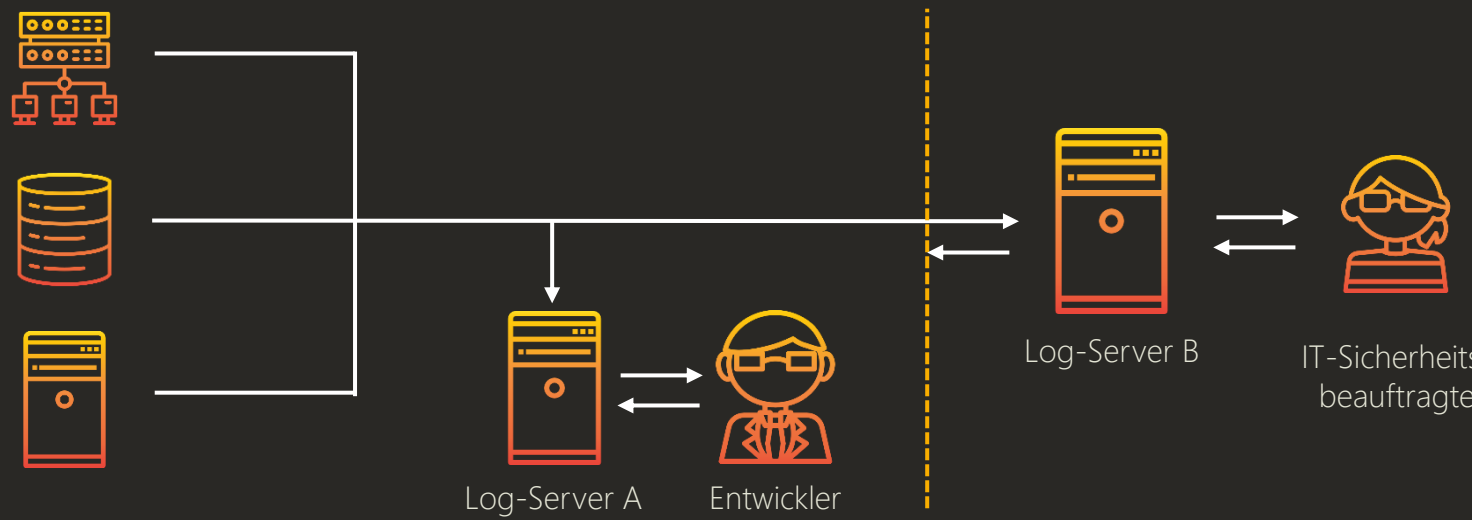
Forensic Readiness

Forensic Readiness umfasst die technischen und organisatorischen Vorbereitungen, um bei einem Sicherheitsvorfall auf eine Untersuchung gerüstet zu sein. Dazu gehören zum Beispiel neben der Organisation, welche Protokolle wo gespeichert werden, die Bereitstellung von Tools und die Schulung des Personals.

- Welche Daten müssen im Notfall verfügbar sein?
- Wie sehen die organisatorischen Maßnahmen dafür aus?
- Wie sehen die technischen Maßnahmen dafür aus?

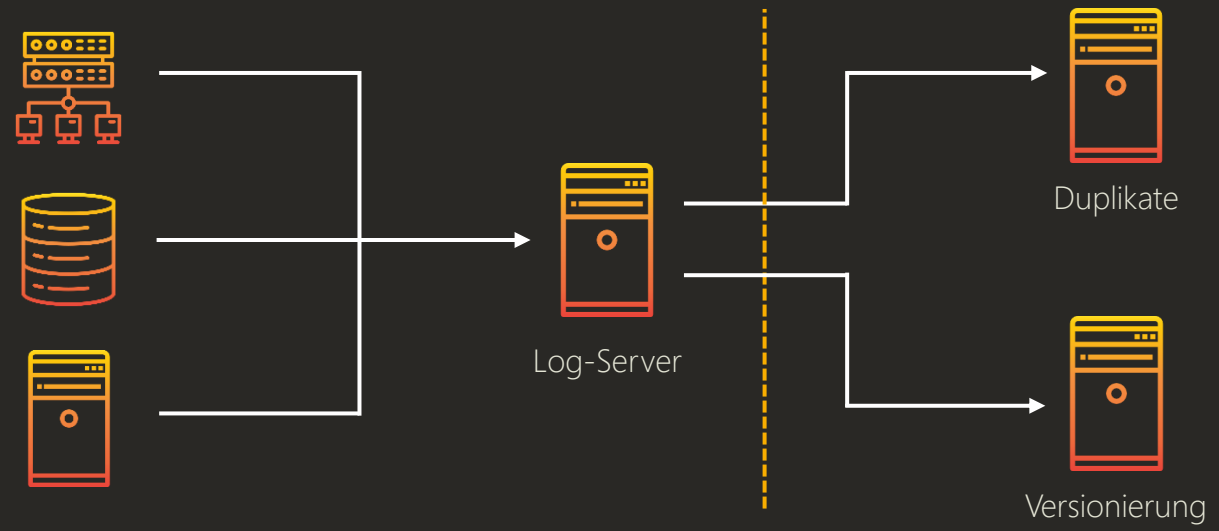
Effektives Logging

- Die Erstellung der Logs sollte aus der Perspektive eines potentiellen Vorfalls erstellt werden und nicht „nur“ zum Debuggen
- Damit sollten alle Schritte nachvollzogen werden können
- Logs sollten zentral auf einem externen System gespeichert werden
- Diese Systeme müssen extra geschützt und abgesichert werden (minimale Zugriffsrechte + Software-WORM)



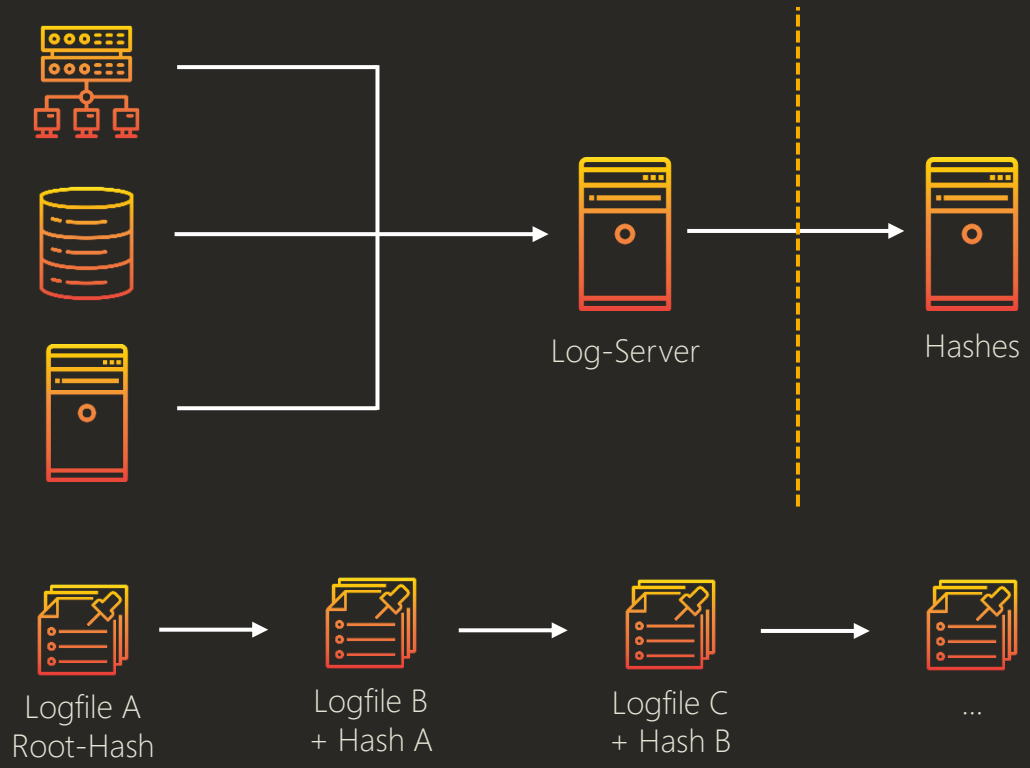
Schutz vor Manipulationen

- Log-Daten müssen vor Manipulationen geschützt werden
- Remote Copy: Mit der Duplizierung von Hashes auf einem externen System lässt sich dies erreichen
- Ist dies nicht möglich, müssen Änderungen protokolliert werden



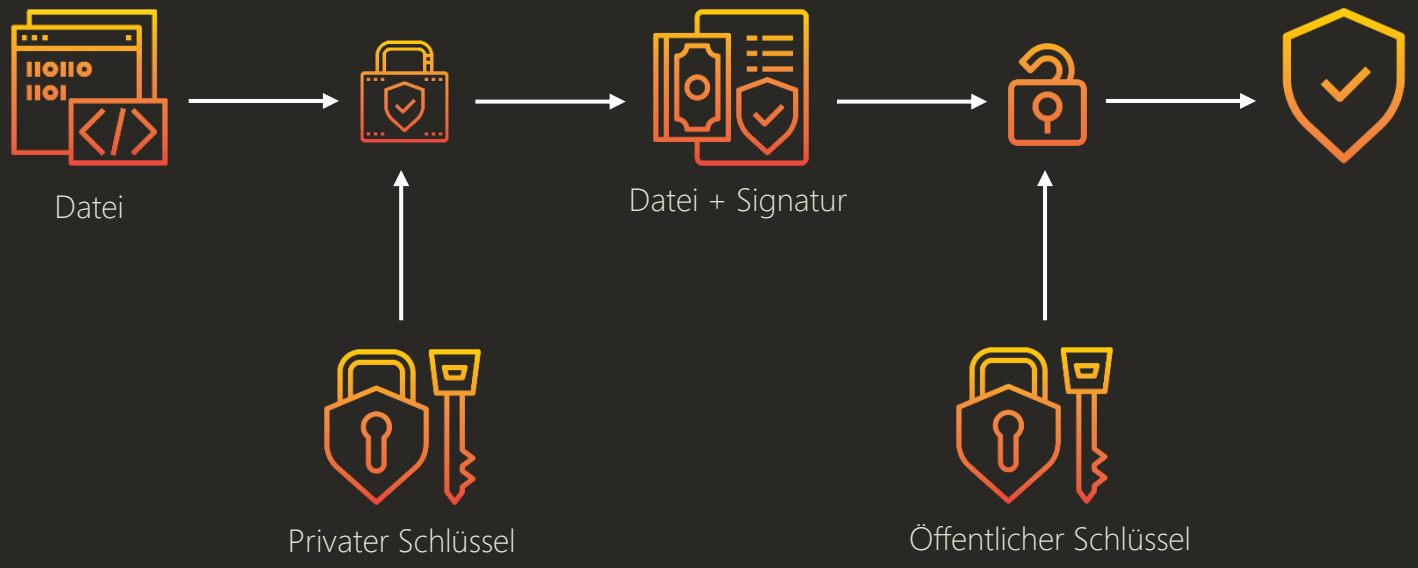
Integritätsverifiaktion

- Mittels Integritätsverifiaktion wird eine Veränderung ausgeschlossen
- Dokumentierte und sichere Prozesse sind dafür die Grundlage
- Hash Chaining: Dateien werden mit Hashes verknüpft



Digitale Signaturen

- Daten können mittels digitalen Signaturen geschützt werden
- Ein Angreifer kann die Daten nicht mehr manipulieren
- Hierfür kann OpenSSL eingesetzt werden



Fazit

Digitale Spurensuche im Tatort Software

- Wird bereits bei der Planung einer Anwendung die Softwarearchitektur unter dem Gesichtspunkt Forensic Readiness entworfen, kann eine spätere IT-Forensik-Untersuchung deutlich fungierter erfolgen.
- Mit einem manipulationssicheren und umfangreichen Logging kann die IT-Forensik Spuren effizient erfassen und auswerten.
- Dabei reichen schon kleine Veränderungen wie das zentrale Speichern von umfangreichen Logs aus, um einen großen Effekt zu erzielen.

Vielen Dank!

Fragen: Saal 2: Q&A

Präsentation online unter: https://scheible.it