Tobias Scheible, M.Eng.

IT-Forensik

Spurensuche in der digitalen Welt

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

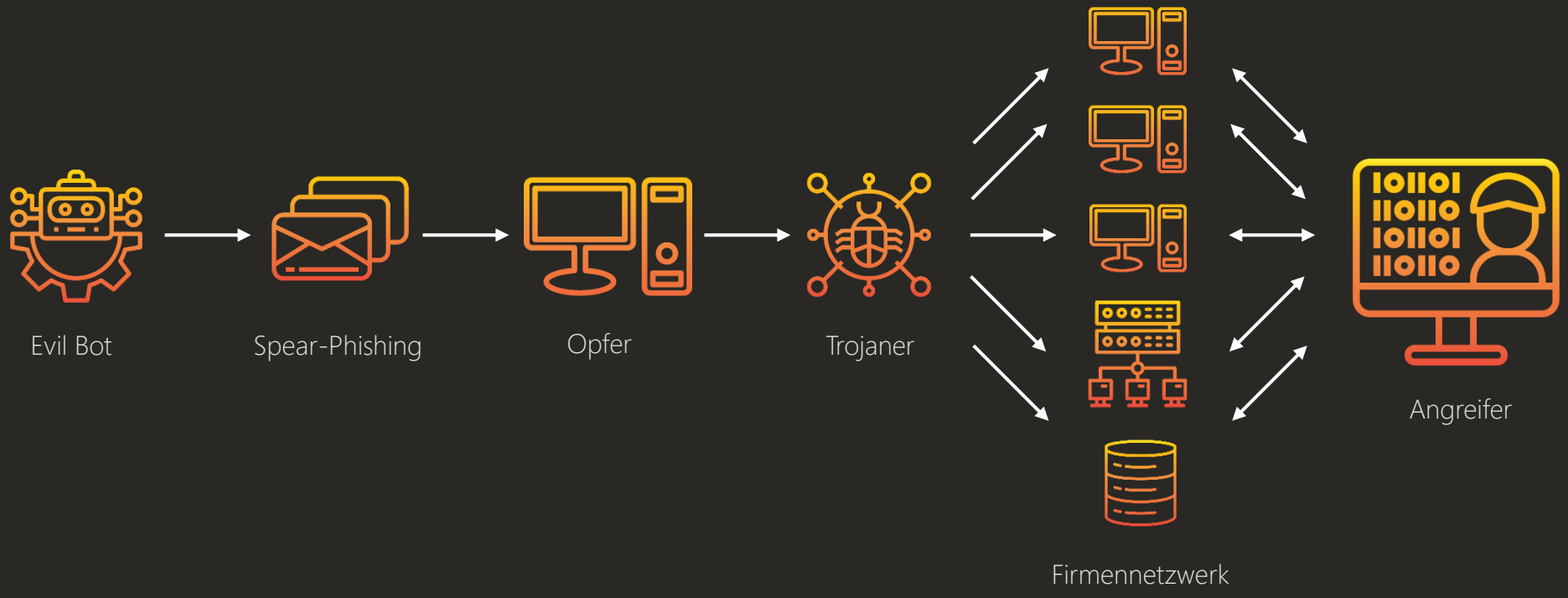
- IT-Forensik
  - Einführung
  - Grundprinzipien
  - Analysemethoden
  - Fachdisziplinen
  - Spezialdisziplinen
- IT-Forensik in Unternehmen
  - Einsatzszenarien
  - Spannungsfeld
  - Herausforderungen
- Untersuchung
  - Firefox Webbrowser

Hinweis

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

IT-Forensik

Cyber Security Vorfall



IT-Forensik

Grundprinzipien

- Digitale Spuren
- Forensische Untersuchungen
- Prozesse und Modelle

Analysemethoden

- Post-Mortem Analyse
- Live-Analyse

Basisdisziplinen

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

Spezialdisziplinen

- Mobilgeräte-Forensik
- Multimedia-Forensik
- Cloud-Forensik
- Hardware-Forensik

IT-Forensik

- Bei der IT-Forensik, auch als digitale Forensik bzw. Computer Forensik bezeichnet, geht es um die Untersuchung eines Rechnersystems nach einem Vorfall.
- Das Ziele ist die Analyse und Auswertung von digitalen Spuren zur Aufklärung von Vorfällen.
- Es geht darum, rechtswidrige oder schädliche Handlungen zu verstehen und nachzuweisen.

IT-Sicherheit vs. IT-Forensik

IT-Sicherheit

Was könnte passieren?

IT-Forensik

Was ist passiert?

IT-Forensik

Grundprinzipien

- Digitale Spuren
- Forensische Untersuchungen
- Prozesse und Modelle

Analysemethoden

- Post-Mortem Analyse
- Live-Analyse

Fachdisziplinen

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

Spezialdisziplinen

- Mobilgeräte-Forensik
- Multimedia-Forensik
- Cloud-Forensik
- Hardware-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

Digitale Spuren

Quelle: flickr.com (1)

Forensische Untersuchungen

- 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.

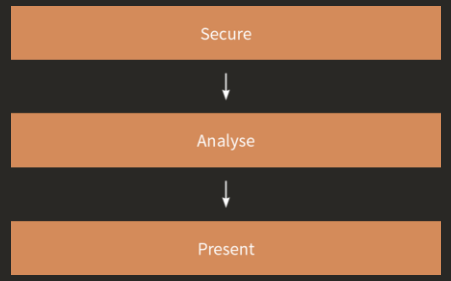
- Ermittlungen wegen:
  Tötungsdelikten, Terrorismus, Kinderpornographie, Betrug, Diebstahl, Copyright-Verletzung, Datendiebstahl, Schadsoftware, Garantiefälle, Versicherungsnachweis, Audits, …

Prozesse und Modelle

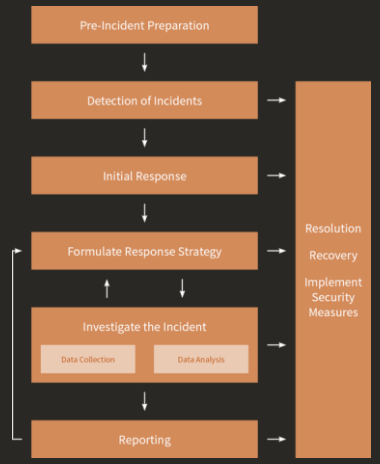
- Anforderung an die Prozesse
  - Akzeptanz & Glaubwürdigkeit
  - Nachvollziehbarkeit & Wiederholbarkeit
  - Vollständigkeit & Integrität
- Allgemein anerkannte Standards: z.B. ISO/IEC 27035 ISO/IEC 27037

- Vorgehensmodelle

Secure-Analyse-Present Model



Incident Response Model



Investigative Process Model

IT-Forensik

Grundprinzipien

- Digitale Spuren
- Forensische Untersuchungen
- Prozesse und Modelle

Analysemethoden

- Post-Mortem Analyse
- Live-Analyse

Fachdisziplinen

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

Spezialdisziplinen

- Mobilgeräte-Forensik
- Multimedia-Forensik
- Cloud-Forensik
- Hardware-Forensik

Post-Mortem Analyse

Bei der 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

Live-Analyse

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

IT-Forensik

Grundprinzipien

- Digitale Spuren
- Forensische Untersuchungen
- Prozesse und Modelle

Analysemethoden

- Post-Mortem Analyse
- Live-Analyse

Fachdisziplinen

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

Spezialdisziplinen

- Mobilgeräte-Forensik
- Multimedia-Forensik
- Cloud-Forensik
- Hardware-Forensik

Datenspeicher-Forensik

Das Ziel der Datenspeicher-Forensik ist im ersten Schritt die forensische Sicherung des kompletten Datenträgers, um anschließend die Analyse aller Daten zu ermöglichen.

- Forensische Sicherung von kompletten Datenspeichern (1:1 Kopie)
- Analyse von verborgenen Datenbereichen
- Wiederherstellung von gelöschten Daten (File Carving)
- Identifizierung von heruntergeladenen Dateien (Zone.Identifier)

Betriebssystem-Forensik

Das Ziel der Betriebssystem-Forensik ist die Extraktion von Informationen zur Bestimmung der Systemkonfiguration, der Nutzeraktivitäten und der installierten Anwendungen.

- Entfernung bzw. Filterung aller unveränderten Standarddateien
- System (Version, Installationsdatum, Hardware, Log-Dateien, …)
- Benutzer (Welche Benutzer, wann angelegt, letzter Login, …)
- Anwendungen (Welche Software, Installationsdatum, …)

Anwendungs-Forensik

Das Ziel der Anwendungs-Forensik ist es, individuelle Anwendungs-spuren zu identifizieren und die Erhebung aller durch die Anwendungen gespeicherten Daten.

- Identifizierung der relevanten Anwendungen
- Sammeln der Daten, die durch die Anwendungen gespeichert werden
- Interpretation der Daten (auch proprietäre Formate)
- Rekonstruktion der Nutzung der Anwendung

Netzwerk-Forensik

Das Ziel der Netzwerk-Forensik ist die stattgefundene Kommunikation in einem Netzwerk zu rekonstruieren und nachzuvollziehen, welche Übertragungen stattgefunden haben.

- Übersicht der Zielnetzwerke und Netzdienste erstellen
- Datenströme durch Konfigurationen nachvollziehen
- Spuren von Protokollen wie HTTP und DNS auswerten
- Zeitlichen Ablauf rekonstruieren

IT-Forensik

Grundprinzipien

- Digitale Spuren
- Forensische Untersuchungen
- Prozesse und Modelle

Analysemethoden

- Post-Mortem Analyse
- Live-Analyse

Fachdisziplinen

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

Spezialdisziplinen

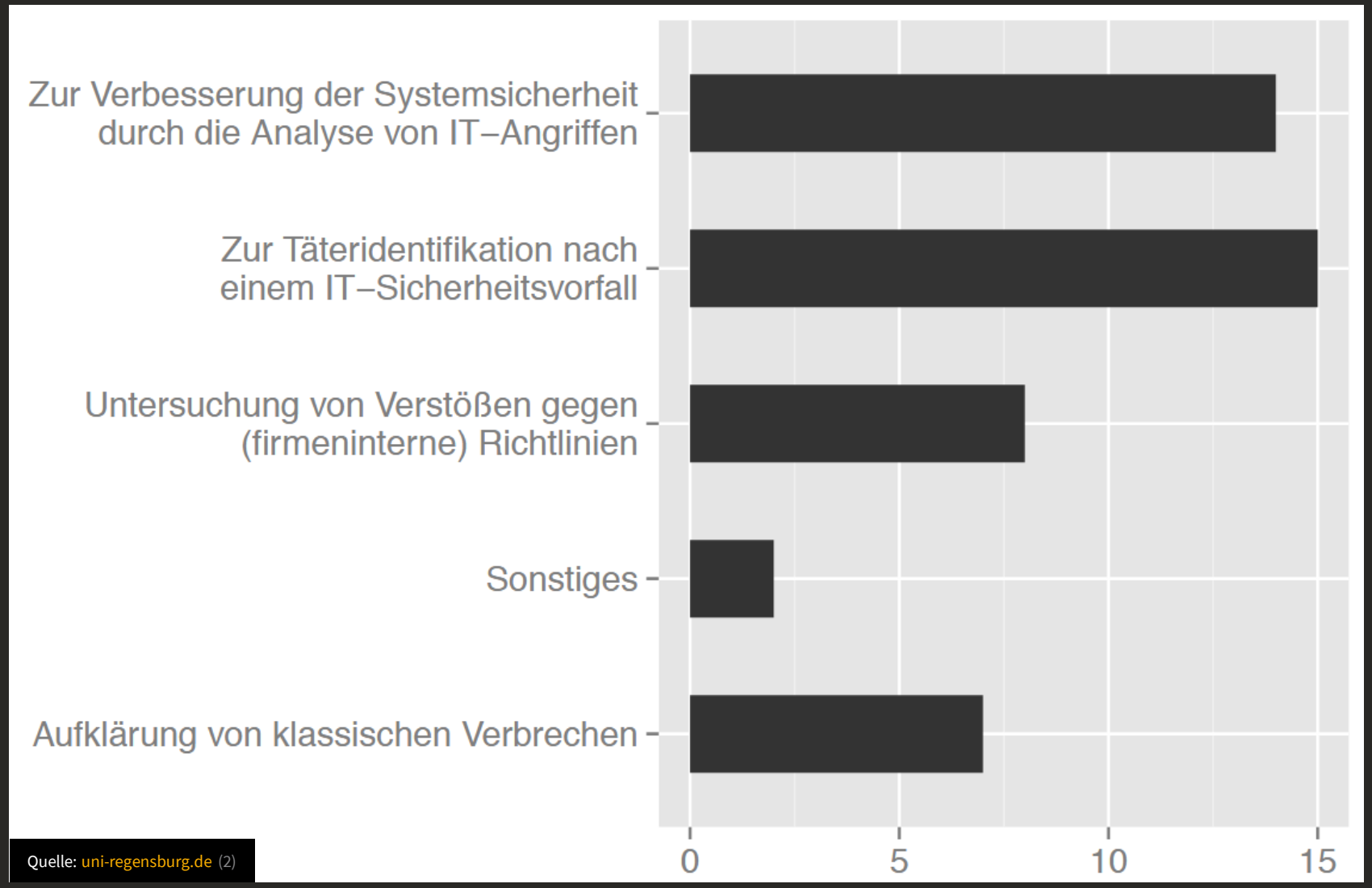
- Mobilgeräte-Forensik
- Multimedia-Forensik
- Cloud-Forensik
- Hardware-Forensik

Spezialdisziplinen

- Mobilgeräte-Forensik
  - Smartphones fassen alle Daten zusammen (Mail, Messenger, GPS, Web, …)
  - Herausforderung: Verschlüsselung der Geräte „Katz-und-Maus-Spiel“
- Multimedia-Forensik
  - Analyse von Fotos und Videoaufnahmen (Manipulationen, Zuordnung, …)
  - Möglichkeiten von verschleierten Kommunikationen – Bsp. Steganographie
- Cloud-Forensik
  - Verlagerung der Systeme und Daten in die Cloud
  - Zugriffe über Schnittstellen und Analyse der Daten wie gewohnt
- Hardware-Forensik
  - Drucker, Network Attached Storage und Automobile erzeugen viele Daten
  - IoT wird in Zukunft eine immer größere Bedeutung spielen

IT-Forensik in Unternehmen

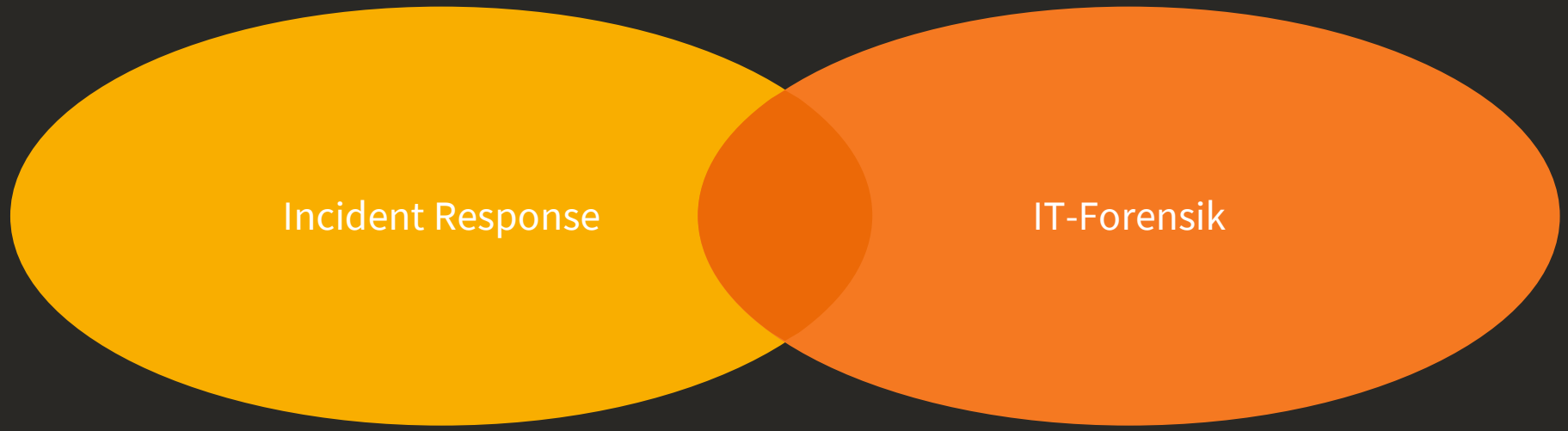
Einsatzszenarien



Quelle: uni-regensburg.de (2)

Spannungsfeld

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

Forensic Readiness

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

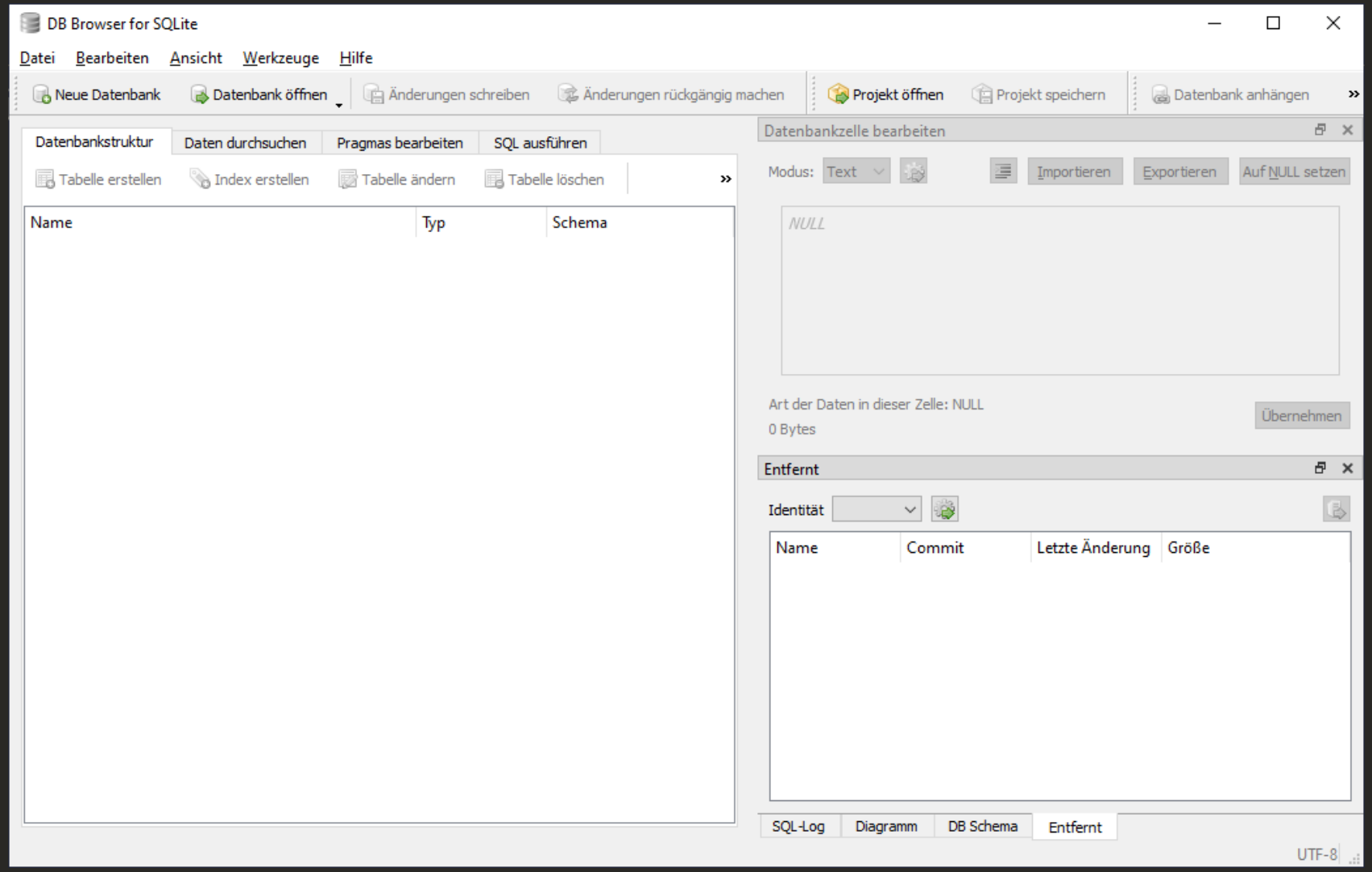
- Welche Daten müssen im Notfall verfügbar sein?
- Wie sehen die organisatorischen Maßnahmen dafür aus?
- Wie sehen die technischen Maßnahmen dafür aus?

Herausforderungen

- Outgesourcte IT
  - Unterschiedliche Auslegung eines Vorfalls
  - Zusammenarbeit mit externen Partnern muss koordiniert werden
- Shared Services
  - Beweissicherungsverfahren tangieren u. U. Daten anderer Nutzer
  - Datenschutzrecht
- Internationalität
- Neue Technologien
  - Dateiformate, Komprimierung, …
- Große Datenmengen
- Geschlossene Systeme
  - Smartphones, Tablets, …
- Verschlüsselte Datenträger
  - Zweitschlüssel vorhanden?
- Externe Systeme – Cloud
- BYOD: IoT, Wearables, „Smart“…

Untersuchung

Live Webbrowser Verlauf



Fragen?

Präsentation online unter: https://scheible.it

Quellen

1) My home office, https://www.flickr.com/photos/paladin27/2277420652, abgerufen am 16.06.2020

2) Digitale Forensik in Unternehmen, Stefan Meier, Seite 82, https://epub.uni-regensburg.de/35027/1/Dissertation_Veroeffentlichung_Stefan_Meier_A5_digital.pdf, abgerufen am 16.06.2020