HOCHSCHULE
HANNOVER
UNIVERSITY OF
APPLIED SCIENCES
AND ARTS
–
Fakultät IV
Wirtschaft und
Informatik

Die Grundlagen der Computer-Forensik

Seminar-Arbeit im Studiengang
„Angewandte Informatik“

Schehat Abdel Kader und Detijon Lushaj, 12 Mai 2022

Inhaltsverzeichnis

Einleitung und Begriffserklärung

Begriffserklärung Computer-Forensik

Begriffserklärung

- Analyse und Aufklärung von Sicherheitsvorfällen
- Die suche nach digitalen Spuren die Hinweise auf Verbrechen liefern sollen

Beispiele: Hackerangriffe, Datenschutzverletzungen durch Insider

Ziele

- Erkennen der Methode oder der Schwachstelle
- Ermittlung des entstandenen Schadens
- Identifikation des Angreifers
- Sicherung der Beweise für weitere juristische Aktionen

Inhaltsverzeichnis

Bedrohungssituation

Grundlagen

Bedrohung

„Mit Bedrohung ist der potenzielle Auslöser für ein unerwünschtes Ereignis gemeint, das sich auf das betroffene IT-System oder die gesamte Organisation schädlich auswirken kann. “ [*1, S.11]

1 Alexander Geschonneck. Computer-Forensik : Computerstraftaten erkennen, ermitteln, aufklären. dpunkt. Verlag GmbH, 2014. ISBN: 978-3-86490-133-1. [S.11]

Bedrohungssituation

Risikoverteilung

maßgeblichen Parameter, um das Risiko einzuschätzen:

- Eintrittswahrscheinlichkeit
- Schadenshöhe

- **Angriffstechniken werden immer komplexer**
  - Zugänglichkeit werden einfacher
  - Bedienung solcher Tools werden immer einfacher

Bedrohungssituation

Identifikation des Angreifers

Motive:

- finanzieller Gewinn
- Wettbewerbsvorteile
- Vergeltungsmaßnahmen
- der Wunsch nach Anerkennung und Öffentlichkeit

Ursprung der Angriffe:

- Außentäter und Außentäterinnen
- Innentäter und Innentäterinnen

Inhaltsverzeichnis

Anforderungen an den Ermittlungsprozess

Einleitung

Grundaspekte

- Präsentation der Ergebnisse
- Angemessene Wahl der Methoden und Werkzeuge
- Entscheidungstragende sind keine Fachleute

Spurensuche und Analyse

- Unvoreingenommene Einstellung
- Einbruchsanalyse und Schadensfeststellung
- Analyse der Angriffstools
- Weitere Beweissuche in Dateien

Anforderungen an den Ermittlungsprozess

Grundaspekte der Ermittlung

Methoden und Werkzeuge

- anerkannt
- glaubwürdig
- Ergebnisse reproduzierbar
- Ursache und Wirkung ersichtlich

Integrität der Spuren

Dokumentation

Anforderungen an den Ermittlungsprozess

Einbruchsanalyse und Schadensfeststellung 1/2

Aufklärung über Ausmaß des Schadens

- Wahl der Sicherheitsmechanismen und Wiederherstellung

Identität des Angreifers bestimmen

- InnentäterIn oder AußentäterIn
- Methoden und Werkzeuge

Anforderungen an den Ermittlungsprozess

Einbruchsanalyse und Schadensfeststellung 2/2

Motive bestimmen

- Gezielter oder zufälliger Angriff
- Weiteres Vorgehen des Angreifers einschätzen
- Angriff beobachten

Feststellen auf welche Daten theoretisch Zugriff

- Lokale und benachbarte Systeme
- Versteckten Hintertüren und installierter Werkzeuge

Anforderungen an den Ermittlungsprozess

Analyse der Werkzeuge

Benutzte Werkzeuge können Angreifende einordnen

- Erfahrene AngreiferIn oder Script Kiddies

Rootkits

- Sammlung von Softwarewerkzeugen
- Verdecktes operieren auf dem kompromittierten System
- Können Ermittlungsergebnisse manipulieren

Glaubwürdigkeit der Ermittlungsergebnisse sicherstellen

Anforderungen an den Ermittlungsprozess

Weitere Beweissuche in Dateien 1/2

Logdateien-Einträge

- Zuverlässigkeit prüfen
- Angriff und verwendete Schwachstelle kann nachvollzogen werden

Zutrittskontrollsysteme und Videoüberwachungsmaterial

- Frühzeitig sichern bei InnentäterInnen
- Frühzeitig Befugnis auf diese Dateien klären

Anforderungen an den Ermittlungsprozess

Weitere Beweissuche in Dateien 2/2

Datenträger genau analysieren

- Spurensuche hängt vom Sicherheitsvorfall ab
- Anwendungen hinterlassen meistens Spuren

Angreifende versuchen ihre Spuren zu verwischen

Gegenstand der Ermittlung

- Nachweis gelöschter Dateien
- Finden Versteckter Dateien und Partitionen

Inhaltsverzeichnis

Einführung in die Computer-Forensik

Einleitung

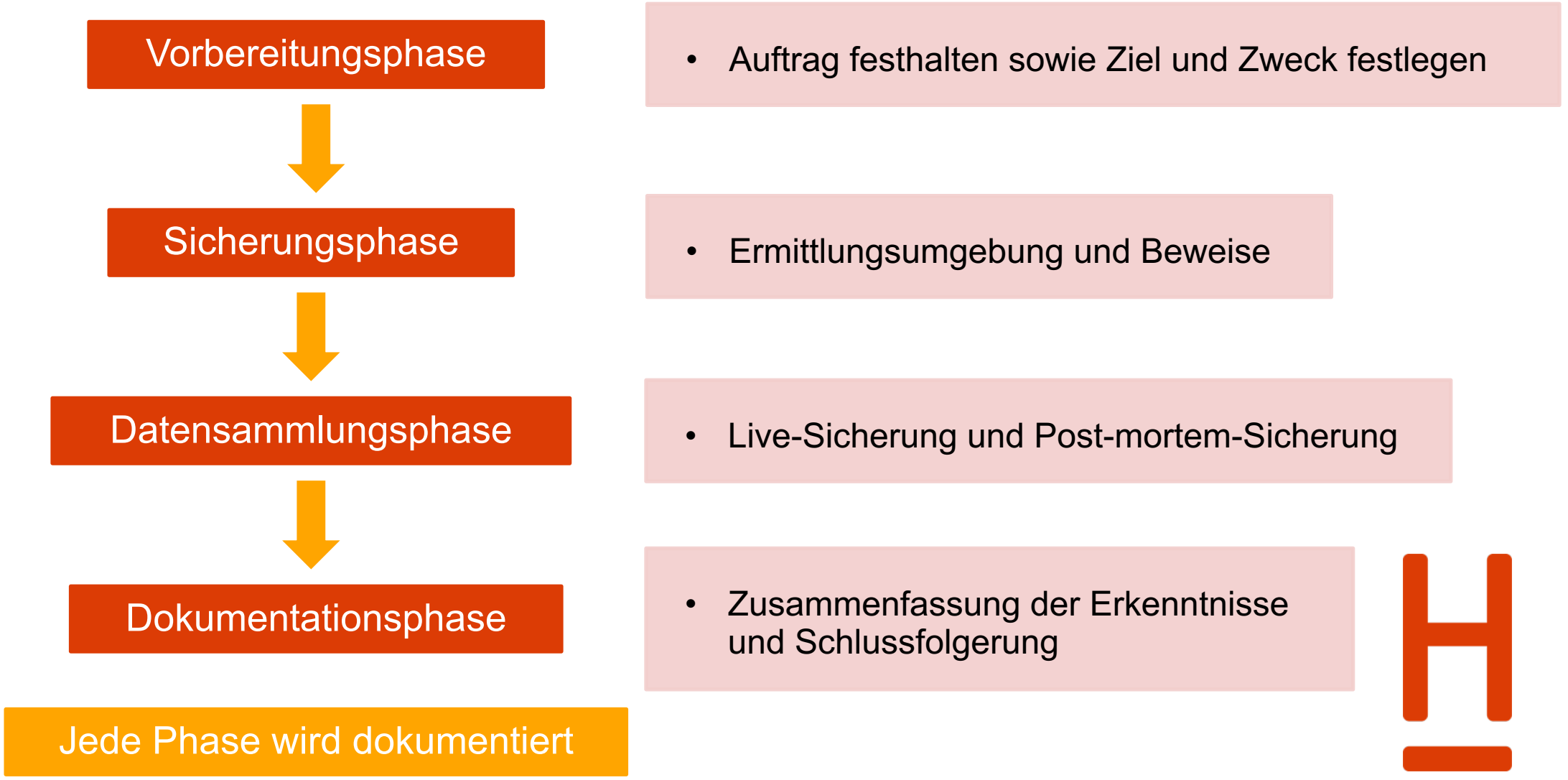
Digitale Spuren

- Leicht manipulierbare Daten
- Locard’sche Austauschprinzip
- Alle Spuren vernichten nicht praktikabel

Austauschprinzip gilt auch für Ermittelnde

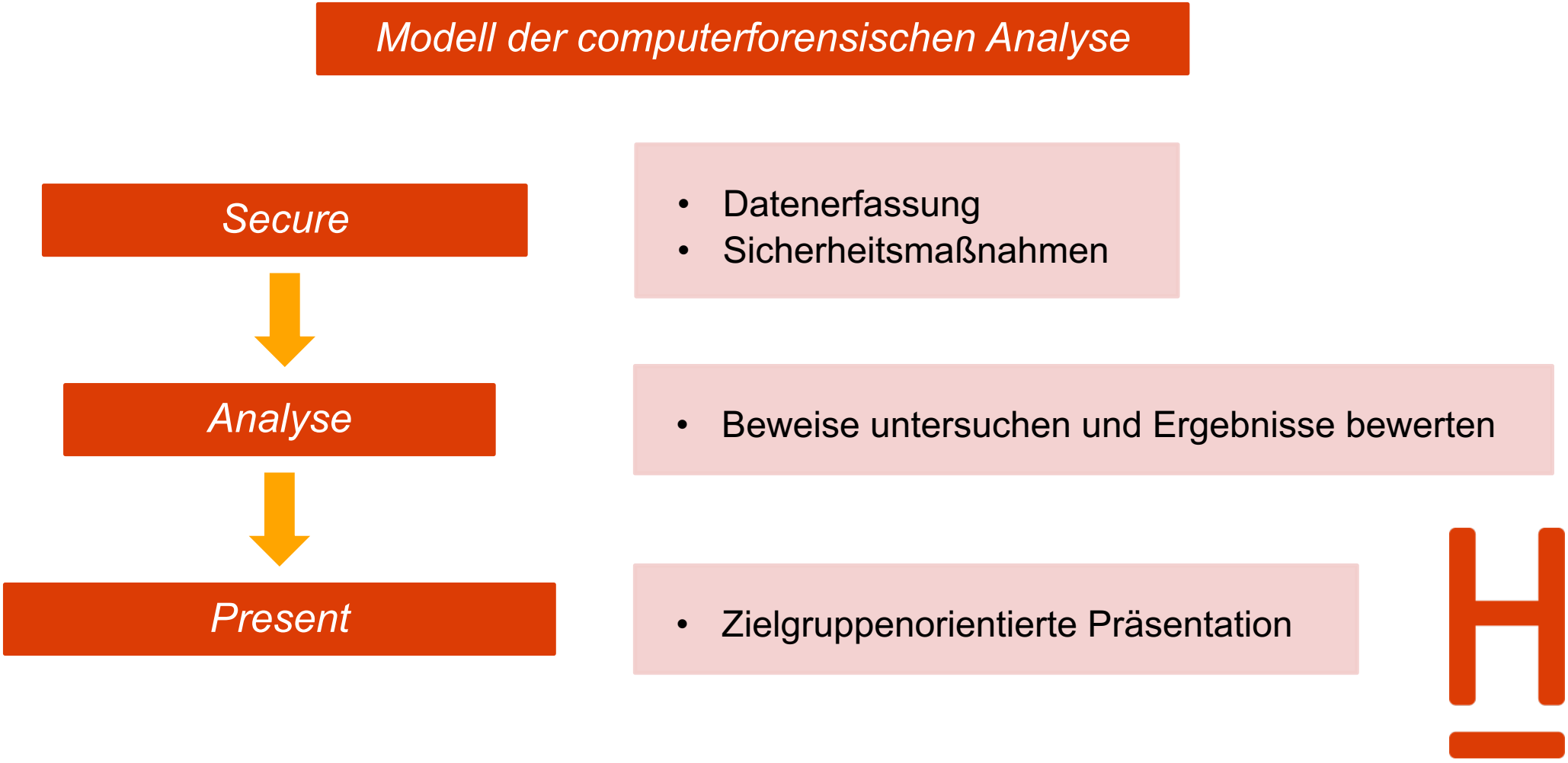
Einführung in die Computer-Forensik

Phasen der Ermittlung



Einführung in die Computer-Forensik

SAP-Modell



Einführung in die Computer-Forensik

Digitale Spurensicherung – Beweissammlung Vorgehen 1/2

Aktuelle Uhrzeit dokumentieren

- Vergleich von Zeitstempeln
- Zeitstempeländerungen vermeiden

Liste laufender Prozesse erstellen

- Keine Prozesse beenden
- Wertvolle Informationen im *\proc* Verzeichnis

Alle Befehle protokollieren

Einführung in die Computer-Forensik

Digitale Spurensicherung – Beweissammlung Vorgehen 2/2

Keine vertrauensunwürdigen Werkzeuge benutzen

- Nicht auf die Ausgabe verlassen
- Eigene Werkzeuge benutzen

Logdateien auf ein anderes System schreiben

- Nicht auf das kompromittierte System
- Beweise können zerstört werden, z.B. im File-Slack

Einführung in die Computer-Forensik

Digitale Spurensicherung – Live-Sicherung

Daten im laufenden System sichern

Vorteile

- Auf kompromittiertem System laufen kritische Anwendungen
- Repräsentation des Zustands des System nah am Sicherheitsvorfall
- Flüchtige Daten sichern möglich

Nachteil

- Beweise manipulieren oder vernichten

Einführung in die Computer-Forensik

Digitale Spurensicherung – Post-mortem-Sicherung 1/2

Persistente Daten im ausgeschalteten System sichern

Verfahren: Forensische Duplikation

- Bitweise Kopie des Datenträgers

Writeblocker

- Blockieren physischen Schreibzugriff auf Datenträger
- Verhindern versehentliches überschreiben
- Mobile und stationäre Writeblocker

Quelle: Alexander Geschonneck. Computer-Forensik : Computerstraftaten erkennen, ermitteln, aufklären [S. 92]

Einführung in die Computer-Forensik

Digitale Spurensicherung – Post-mortem-Sicherung 2/2

Vorteile

- Rootkits resistent
- Keine Gefahr Beweise zu vernichten oder zu manipulieren
- Parallele Analysen

Inhaltsverzeichnis

Juristische Beweisführung

Grundlagen

Grundlagen

- Die häufigsten Spuren sind digitale
  - bei unsachgemäßer Behandlung verlieren die ihren Beweiswert
- sorgfältige Dokumentation der Aktivitäten ist wichtig
- Sachverhalte verständlich und nachvollziehbar darstellen

Juristische Beweisführung

Datenschutz

Bundesdatenschutzgesetz a.F. § 3a

- Datenvermeidung
- Datensparsamkeit
- Systemdatenschutz als Gesamtziel
- Anonymisierung
- Pseudonymisierung

Juristische Beweisführung

Datenschutz

Ausnahmen für Behörden

- **Das Gesetz gibt Behörden das Recht** Informationen zu sammeln auf die sie aufgrund des Datenschutzes **eigentlich keinen Zugriff haben**

  → **Datenschutz sollte kein Tatenschutz/Täterschutz sein**

- Wenn der Eigentümer der Daten daher vor Gericht als Zeuge oder Zeugin geladen wird, **muss er Auskunft über diese Daten geben**

Juristische Beweisführung

Daten die erfasst werden

flüchtige Daten

- Informationen, die beim Ausschalten verloren gehen

Beispiel: Inhalt von Cache und Hauptspeicher, laufende Prozesse

persistente Daten

- Daten auf der Festplatte
- deren Zustand kann sich beim Zugriff ändern

→ »Sterile« Datenträger verwenden

Juristische Beweisführung

Bewertung der Beweisspuren

Beweisspuren, die […]

- […] eine bestimmte Theorie untermauern
- […] gegen eine bestimmte Theorie sprechen
- […] keine bestimmte Theorie unterstützen/wiederlegen

Juristische Beweisführung

Aktionen dokumentieren

Alle durchgeführten Maßnahmen müssen dokumentiert werden

→ Dokumentenformat zu definieren

jede einzelne Maßnahme sollte dokumentiert werden

- weshalb die einzelnen Vorgehensschritte durchgeführt wurden
- welche Erkenntnisse daraus zu erwarten sind

- **In jedem Fall sollten verdächtige Dateien zur späteren Analyse kopiert werden**

Juristische Beweisführung

Aktionen dokumentieren

Lfd. Nr.	Zeit	Befehl	MD5 der Ergebnisdatei	Kommentar
1	16:17:10	netstat –n|nc 10.0.0.1 8000	902afd8e6121e153bbc8cb9 3013667fd	Anzeige der aktiven Netzverbin-dungen
2	16:17:30	netstat –an|nc 10.0.0.1 8000	cd6783f8d9a109ffe8399126 74e2f3cf	Anzeige der offenen Ports
3	16:17:55	nbtstat –c|nc 10.0.0.1 8000	931b672fabcdb2145ae51e2 885e9b685	Anzeige des Cache von NBT-Verbindungen
[...]				
6	17:30	Sicherstellung des verdächtigen PC im Raum B102	Rechnername/ IP-Adresse: lapBER49, 192.168.7.69 Inventarnummer: BER4543.A3 Modell: TA-349 Festplatte (Typ,Größe, S/N): RPA-0802, 80GB, 34567783-A-34546	Anwesende Personen: Herr Müller (Hauptbenutzer des PC) Herr Schulz (Revision, Special Investigation) Herr Meier (IT-Security)

Quelle: Alexander Geschonneck. Computer-Forensik : Computerstraftaten erkennen, ermitteln, aufklären. dpunkt. Verlag GmbH, 2014. ISBN: 978-3-86490-133-1. [S. 84]

Juristische Beweisführung

Beweise dokumentieren

Alle gefundenen Beweise sind auf einem Beweiszettel zu vermerken

- Es sollte nachvollziehbar sein, **wer, wann** und **wie** auf diese Nachweise Zugriff hat
- es darf kein Zweifel über **Herkunft**, **Besitztum** und **Integrität** aufkommen

jede einzelne Maßnahme sollte dokumentiert werden

- Eigentümer des Objekts
- ausführliche Objektbeschreibung
- wer wann und aus welchem Grund Zugriff auf die Beweise hatte
- wo es gefunden wird

Juristische Beweisführung

Beweise dokumentieren

Beweiszettel				Fall:
Datum: Uhrzeit		Standort/Fundort		ID:
Ermittler		Zeuge		
Unterschrift Ermittler		Unterschrift Zeuge		
Gegenstand	Anzahl	Beschreibung (Typ, Hersteller, Farbe, Seriennummer, Identifikationsmerkmale, Inventarnummer, ggffs. Wert etc.)		
Ausgabevermerk				
Gegenstand	Dat./Uhrzeit	Herausgabe durch	Empfang durch	Grund
		Name Organisation Unterschrift	Name Organisation Unterschrift	
		Name Organisation Unterschrift	Name Organisation Unterschrift	
		Name Organisation Unterschrift	Name Organisation Unterschrift	

Schlussübergabe	Empfänger, Zeuge		
Durchgeführte Aktionen: (Rückgabe an Besitzer, Archivierung, Zerstörung etc.)	Name	Unterschrift	Datum
	1.)		
	2.)		
	3.)		
	4.)		

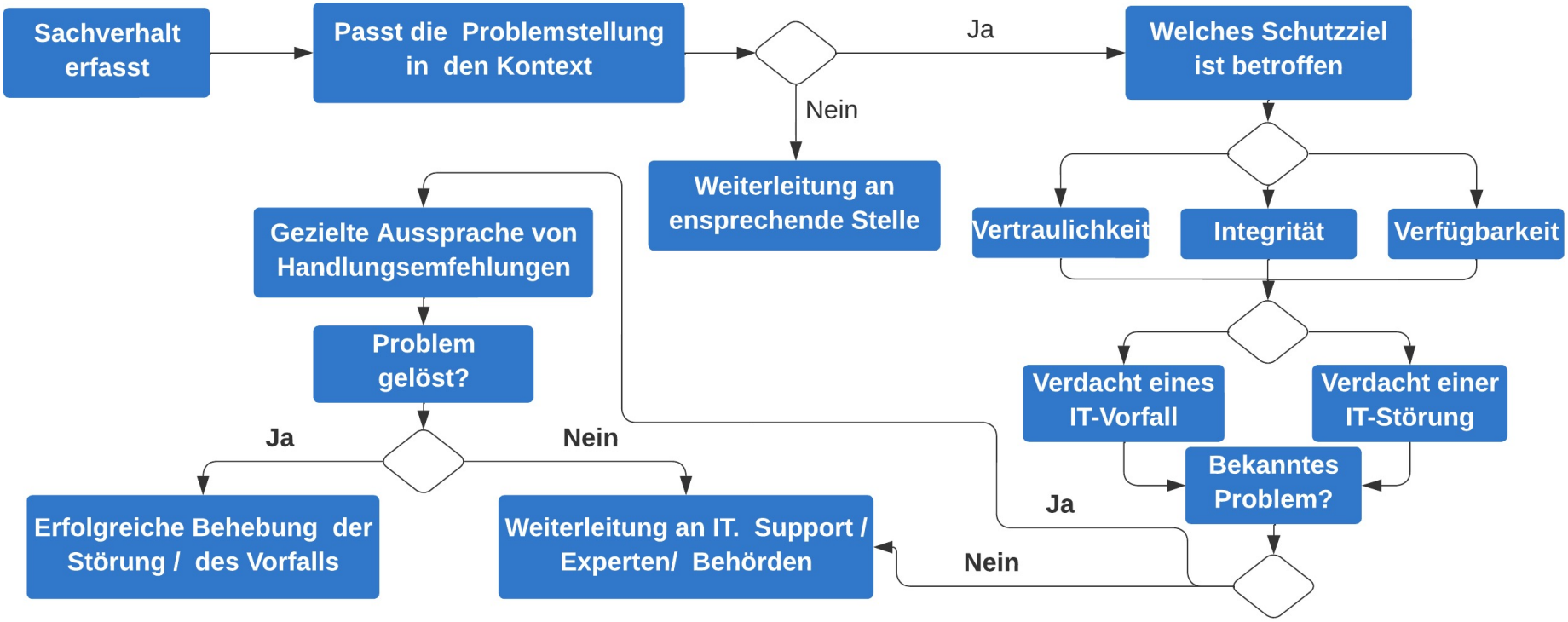
Quelle: Alexander Geschonneck. Computer-Forensik : Computerstraftaten erkennen, ermitteln, aufklären. dpunkt. Verlag GmbH, 2014. ISBN: 978-3-86490-133-1. [vgl. S. 85].

Inhaltsverzeichnis

Sicherstellung des Systems

Entscheidungsprozesse und Entscheidungsmatrix

- Jeder Sicherheitsvorfall ist individuell



Quelle: BSI. Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Digitale Ersthelfer. url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CSN/210712_ Leitfaden_Digitaler_Ersthelfer.pdf (besucht am 10. 04. 2022). [vgl. S. 53].

Schluss

Anforderungen an Ermittlung

- Methoden und Werkzeuge anerkannt, glaubwürdig, reproduzierbar
- Integrität der Spuren und Dokumentation

SAP-Modell

- Secure: Datenerfassung
- Analyse: Beweise untersuchen und bewerten
- Present: zielgruppenorientierte Präsentation

Live-Sicherung und Post-mortem-Sicherung

Herausforderungen

- Datenschutz
- Beweise in kausalen und zeitlichen Zusammenhang stellen

Vielen Dank für Ihre Aufmerksamkeit!

Offene Fragenrunde