



---

# BACHELOR ARBEIT

---

Herr

**Thomas Willnat**

## **Beweiskraft sichern**

**Forensic Readiness erhöhen durch Regelbackups**

Mittweida, 2024

Fakultät Angewandte Computer-  
und Biowissenschaften

---

## **BACHELOR ARBEIT**

---

### **Beweiskraft sichern**

**Forensic Readiness erhöhen durch Regelbackups**

Autor:  
**Herr**

**Thomas Willnat**

Studiengang:  
**IT-Forensik/Cybercrime**

Seminargruppe:  
**CC17w1-B**

Erstprüfer:  
**Prof. Dr. rer. pol. Ronny Bodach**

Zweitprüfer:  
**M. Sc. Florian Göhler**

Einreichung:  
**Mittweida, 18.07.2024**

Fakultät Angewandte Computer-  
und Biowissenschaften

---

## **BACHELOR THESIS**

---

# **Increase forensic readiness through regular backups**

author:  
**Mr.**

**Thomas Willnat**

course of studies:  
**IT-Forensik/Cybercrime**

seminar group:  
**CC17w1-B**

first examiner:  
**Prof. Dr. rer. pol. Ronny Bodach**

second examiner:  
**M. Sc. Florian Göhler**

submission:  
**Mittweida, 18.07.2024**

**Bibliografische Beschreibung:**

Willnat, Thomas:

Beweiskraft sichern - Forensic Readiness erhöhen durch Regelbackups. - 2024. - 6, 41 ,  
29 S. Mittweida, Hochschule Mittweida, Fakultät Angewandte Computer-  
und Biowissenschaften, Bachelor Arbeit, 2024

**Referat:**

Erarbeitung eines Anforderungskatalogs zur Erhöhung des forensischen Wertes regulärer Backups.

# Inhalt

## Inhalt V

|                                                        |             |
|--------------------------------------------------------|-------------|
| <b>Abbildungsverzeichnis .....</b>                     | <b>VII</b>  |
| <b>Tabellenverzeichnis .....</b>                       | <b>VIII</b> |
| <b>Tabellenverzeichnis Anhang .....</b>                | <b>IX</b>   |
| <b>Abkürzungsverzeichnis .....</b>                     | <b>X</b>    |
| <b>1 Übersicht.....</b>                                | <b>1</b>    |
| 1.1 Vorwort.....                                       | 1           |
| 1.2 Einleitung .....                                   | 1           |
| 1.3 Motivation und Ziel .....                          | 2           |
| 1.4 Aufbau der Arbeit .....                            | 2           |
| 1.5 Grenzen dieser Arbeit .....                        | 3           |
| <b>2 Sondierung der Anforderungen .....</b>            | <b>4</b>    |
| 2.1 Evaluierung forensischer Frameworks.....           | 4           |
| 2.1.1 Methodik der Literatursuche .....                | 4           |
| 2.1.2 Ergebnis der Literatursuche .....                | 6           |
| 2.2 Evaluierung der gerichtlichen Verwertbarkeit.....  | 8           |
| 2.3 Evaluierung des Regelbackups .....                 | 12          |
| 2.3.1 Methodik der Literatursuche .....                | 12          |
| 2.3.2 Ergebnis der Literatursuche .....                | 13          |
| 2.4 Ergebnis der Anforderungssondierung .....          | 14          |
| <b>3 Forensischer Wert eines Regelbackups .....</b>    | <b>15</b>   |
| 3.1 Definition des Forensischen Wertes .....           | 15          |
| 3.2 Ableitung der Metrik .....                         | 15          |
| 3.3 Bewertung eines regulären Backups .....            | 16          |
| <b>4 Erhöhung des Forensischen Wertes .....</b>        | <b>20</b>   |
| 4.1 Methodik zur Erhöhung des forensischen Wertes..... | 20          |

|                                                               |                                                               |             |
|---------------------------------------------------------------|---------------------------------------------------------------|-------------|
| 4.2                                                           | <i>Thema 1: Integritätsnachweis gegenüber der Quelle.....</i> | 21          |
| 4.3                                                           | <i>Thema 2: Eigenschaften des Werkzeugs .....</i>             | 23          |
| 4.4                                                           | <i>Thema 3: Eigenschaften des Systems .....</i>               | 26          |
| 4.5                                                           | <i>Thema 4: Vollständigkeit der Datensicherung .....</i>      | 26          |
| 4.6                                                           | <i>Thema 5: Dokumentation .....</i>                           | 28          |
| 4.7                                                           | <i>Thema 6: Nachvollziehbarkeit .....</i>                     | 28          |
| 4.8                                                           | <i>Thema 7: Schutz der Datenquelle .....</i>                  | 29          |
| 4.9                                                           | <i>Thema 8: Datenhaltung.....</i>                             | 30          |
| 4.10                                                          | <i>Thema 9: Chain of Custody.....</i>                         | 31          |
| <b>5</b>                                                      | <b>Bewertung und Diskussion .....</b>                         | <b>32</b>   |
| 5.1                                                           | <i>Eigenschaften des forensischen Backups .....</i>           | 32          |
| 5.2                                                           | <i>Limitierungen des forensischen Backups .....</i>           | 33          |
| 5.3                                                           | <i>Bewertung des forensischen Backups.....</i>                | 33          |
| 5.4                                                           | <i>Einordnung in die gerichtliche Verwertbarkeit.....</i>     | 37          |
| <b>6</b>                                                      | <b>Fazit.....</b>                                             | <b>39</b>   |
| 6.1                                                           | <i>Implikationen .....</i>                                    | 39          |
| 6.2                                                           | <i>Ausblick.....</i>                                          | 39          |
| 6.3                                                           | <i>Fazit .....</i>                                            | 40          |
| <b>Literatur</b>                                              |                                                               | <b>43</b>   |
| <b>Anlagen</b>                                                |                                                               | <b>51</b>   |
| <b>Anlagen, Kapitel 2: Sondierung der Anforderungen .....</b> |                                                               | <b>I</b>    |
| <b>Anlagen, Kapitel 3: Forensischer Wert .....</b>            |                                                               | <b>IX</b>   |
| <b>Selbstständigkeitserklärung .....</b>                      |                                                               | <b>XXVI</b> |

# Abbildungsverzeichnis

|                                                              |    |
|--------------------------------------------------------------|----|
| Abbildung 1: Erstellen einer Prüfsumme über .vmdk-Datei..... | 22 |
| Abbildung 2: Abzug einer Arbeitsspeicher-Sicherung .....     | 27 |

## Tabellenverzeichnis

|                                                                            |    |
|----------------------------------------------------------------------------|----|
| Tabelle 1: Aktivitäten der Phase Reconnaissance .....                      | 6  |
| Tabelle 2: relevante Frameworks BSI & NIST forensische Sicherung.....      | 8  |
| Tabelle 3: Anforderungen für gerichtliche Verwertbarkeit .....             | 12 |
| Tabelle 4: relevante Frameworks BSI & NIST Backup.....                     | 13 |
| Tabelle 5: Bewertung reguläres Backup .....                                | 19 |
| Tabelle 6: Katalogisierung Backuptools im Katalog forensischer Tools ..... | 25 |
| Tabelle 7: Eigenschaften forensisches Backup .....                         | 32 |
| Tabelle 8: Bewertung forensisches Backup .....                             | 36 |
| Tabelle 9: Einordnung der gerichtlichen Verwertbarkeit.....                | 37 |

## Tabellenverzeichnis Anhang

|                                                                                  |       |
|----------------------------------------------------------------------------------|-------|
| A_ 1: Suchstrategie nach Metastudien in wissenschaftlichen Datenbanken .....     | I     |
| A_ 2: Suchstrategie nach Metastudien in wissenschaftlichen Journalen.....        | II    |
| A_ 3: Anforderungen forensische Sicherung: BSI Leitfaden IT-Forensik .....       | IV    |
| A_ 4: Anforderungen forensische Sicherung: BSI: Grundsatz Kompendium (DER.2.2) . | V     |
| A_ 5: Anforderungen forensische Sicherung: NIST: SP 800-86.....                  | V     |
| A_ 6: Anforderungen forensische Sicherung NIST: IR 8387 .....                    | VI    |
| A_ 7: Digitale Daten als Beweismittel im Strafverfahren .....                    | VII   |
| A_ 8: Anforderungen reguläres Backup: NIST SP 800-53 .....                       | VII   |
| A_ 9: Anforderungen reguläres Backup: NIST SP 800-34 .....                       | VII   |
| A_ 10: Anforderungen reguläres Backup: CON.3 Datensicherungskonzept .....        | VIII  |
| A_ 11: Konsolidierte Anforderungen reguläres Backup .....                        | XIII  |
| A_ 12: : Konsolidierte Anforderungen forensische Sicherung .....                 | XXI   |
| A_ 13: Zuordnung Anforderung forensische Sicherung zum Thema.....                | XXII  |
| A_ 14: Metrik zur Beurteilung der forensischen Güte.....                         | XXIII |
| A_ 15: Zusammenfassende Übersicht der Backup-Anforderungen .....                 | XXIV  |

## Abkürzungsverzeichnis

|              |                                                     |
|--------------|-----------------------------------------------------|
| ZPO          | Zivilprozessordnung                                 |
| StPO         | Strafprozessordnung                                 |
| SAP <Modell> | Secure Analyse Present Modell                       |
| NIST         | National Institute of Standards and Technology      |
| BSI          | Bundesamt für Sicherheit in der Informationstechnik |
| SP           | Special Paper                                       |
| ID           | identifizier                                        |
| API          | Application Programming Interface                   |
| ESXI         | Elastic Sky X integrated                            |
| IaaS         | Infrastructure-as-a-Service                         |
| IT           | Informationstechnik                                 |
| VM           | virtuelle Maschine                                  |
| VADP         | VMware vStorage API for Data Protection             |
| VSS          | Volume Shadow Copy Service                          |
| vmdk         | Virtual Machine Disk                                |
| vbk          | Veeam Backup File                                   |
| MD5          | Message Digest Algorithm 5                          |
| SHA          | Secure Hash Algorithm                               |
| vmem         | virtual Memory                                      |
| CMS          | Configuration Management System                     |
| SSH          | Secure Shell                                        |
| ISMS         | Information Security Management System              |
| DFIF         | Digital forensic investigation frameworks           |

# 1 Übersicht

## 1.1 Vorwort

In einem malerischen Dorf hoch in den Bergen lebten Zwerge, deren präzise Handwerkskunst weit und breit berühmt war. Jeder Einzelne von ihnen ging mit Liebe und Hingabe seinem Tagwerk nach, bis eines Tages ein schockierendes Ereignis ihre friedliche Idylle durchbrach: Der wertvolle Dorfschatz war gestohlen. Zunächst bemerkte niemand den Verlust, doch als die Erkenntnis dämmerte, wurde das Dorf in Aufruhr versetzt.

Die besten forensischen Experten wurden sofort herbeigerufen, um den Tatort zu sichern. Ihre Funde waren jedoch spärlich und die Hoffnung schwand. Erst als der gründliche NetZwerg die regelmäßigen Backups der Überwachungssysteme auf den alten Magnetbändern kleinlaut hervorholte, entstand neue Zuversicht. Trotz des missbilligenden Blicks des DSGVO-Zwergs bekamen sie endlich Hinweise auf den Täter und stellten den Dieb - ein übelgesinnter Troll, der den privaten Schlüssel des Bitcoin-Schatzes in seiner Höhle versteckt hatte.

Als die Sonne hinter den Bergen versank, saßen die Zwerge zusammen am Lagerfeuer und grillten den Troll. Während sie einen neuen PDCA-Zyklus (Plan-Do-Check-Act) einleiteten, dachten sie nach: „Es müsste doch eigentlich Synergien zwischen dem regulären Backup und forensischen Sicherungen geben...“

So ähnlich entstand die Idee für diese Bachelor-These.

## 1.2 Einleitung

Für eine konsistente IT-Sicherheitsstrategie spielen sowohl forensische Sicherungen als auch reguläre Backups eine entscheidende Rolle. Beide Verfahren verfolgen das gemeinsame Ziel, Daten zu sichern und sie wiederherstellbar unter Einhaltung der Schutzziele der Informations-/IT-Sicherheit zu verwahren. Schaut man sich klassische Grenzen der forensischen Analyse (Recht, fehlende Daten, Aufwand/Kosten)<sup>[01]</sup> an, sind die beiden letzteren Punkte Elemente, in denen reguläre Backups ihre Vorteile bieten, da sie vollautomatisch regelmäßig Daten sichern. Es erscheint in der Vorüberlegung verwunderlich, wie getrennt die forensischen Sicherungen von regulären Backups betrachtet werden.

## 1.3 Motivation und Ziel

Gelänge es die Verfahren des regulären Backups und die forensische Sicherung zusammenzuführen, ergäben sich daraus große Vorteile für die zwei Anwendungsfälle der Sicherung. Der IT-Betrieb, dessen Interesse unter anderem eine hohe Verfügbarkeit <sup>[02]</sup> ist, wäre zur IT-Forensik auskunftsfähig ohne Rückwirkungen auf die Produktivsysteme. Die regelmäßig gewonnenen Abbilder könnten als transportfähige Backups für Analysen weitergereicht werden. Da die Backups ohnehin im Rahmen der Retention vorgehalten werden, wären sie automatisch zur forensischen Verwertung geeignet. Auf der anderen Seite profitierten Forensiker von der hohen Sicherungsdichte bei gleichzeitig geringerem Aufwand. Zeitlinien ließen sich anhand der vorhandenen regelmäßigen Backups genauer nachvollziehen, gelöschte Dateien sich bestenfalls direkt oder von vormals noch nicht erneut überschriebenen Sektoren zurückgewinnen, auch wenn sie im aktuellen System verloren sind.

Angesichts dieser einfach aufgeworfenen Überlegungen, welche sich auch komplexer weiterführen ließen, wie zum Beispiel über die Rekonstruktionsmöglichkeiten flüchtiger Zustände aus der Vergangenheit, geht diese Arbeit der Frage nach, inwiefern reguläre Backups bereits in häufig angewandten Konfigurationen forensische Anforderungen erfüllen und welche Eigenschaften sie haben müssten, um forensisch wertvoller zu werden oder gar als vollständige forensische Sicherung angesehen werden zu können.

Ziel der Arbeit soll ein Anforderungskatalog sein, der operationalisierbare Anforderungen listet, die ergänzend zu bestehenden Backup-Standards als Teil der strategischen Vorbereitung und somit zur Erhöhung der Forensic Readiness umgesetzt werden können.

## 1.4 Aufbau der Arbeit

Dafür wird zuerst im Kapitel 2 nach bereits vorhandenen und allgemein akzeptierten Standards gesucht, um einen möglichst umfangreichen Regelkatalog zur Erstellung von regulären Backups, forensischen Sicherungen und der gerichtlichen Auswertbarkeit von Beweisen zu bekommen. Es soll hierfür auf Studien zurückgegriffen werden, welche den Einfluss und die Reichweite einzelner Standards untersuchten. Aus diesen Standards werden die Anforderungen für die weitere Analyse exzerpiert. Das Ergebnis ist jeweils ein konsolidierter Anforderungskatalog für reguläre Backups, forensische Sicherungen und Anforderungen für die gerichtliche Verwertbarkeit. Mit dem Forensischen Wert wird anschließend ein Maß zur Ermittlung der Güte einer Datenakquise im Verhältnis zu einer forensischen Sicherung im Kapitel 3 eingeführt. Anhand dieses Maßes wird ein reguläres Backup gemessen, um es am Ende mit einem forensischen Backup vergleichen zu können. Eigenschaften eines forensischen Backups werden im Kapitel 4 in neun Themenbereichen erarbeitet. Die Arbeit schließt inhaltlich im Kapitel 5 mit der Bestimmung des Mehrwerts eines forensischen Backups gegenüber eines regulären Backups. Grenzen der Betrachtung und Unschärfen werden andiskutiert. Ergebnis der Arbeit ist ein 11-Teiliges

Regelset, welches die Anforderungen an reguläre Backups ergänzt und als Teil der strategischen Vorbereitung vorgesehen ist.

## 1.5 Grenzen dieser Arbeit

Um ein realistisches Bild der Aussagekraft der Arbeit zu vermitteln, müssen folgende drei Einschränkungen gemacht werden. Sie zeigen jeweils eigene Forschungsperspektiven auf und würden den Rahmen dieser Arbeit überschreiten

- Um bis zum eigentlichen Forschungsgegenstand und den praktischen Verbesserungen des Regelbackups vorzustoßen, wird auf etablierte IT-Standards zurückgegriffen. Obwohl diese inhaltlich möglichst breit gewählt wurden, ist die Vollständigkeit kein Untersuchungsgegenstand dieser Arbeit. Anforderungen innerhalb der Frameworks wurden inhaltlich übernommen und erst im Anschluss bewertet.
- Diese Arbeit beschränkt sich im Schwerpunkt auf die Datenakquise, wohlwissend, dass zur Auswertung eines digitalen Artefaktes weitere Schritte im forensischen Prozess nachgelagert sind und sich auch hieraus Anforderungen ergeben.
- Die Metrik zur Bestimmung des Forensischen Wertes ist sehr einfach aufgebaut. Nach erfolgloser Recherche zu bereits bestehenden Metriken wurde hier auf die annähernd Einfachmöglichste zurückgegriffen. Innerhalb der Arbeit wird das akzeptiert, da die Ergebnisse lediglich relativ zueinander verglichen werden. Außerhalb wird sie nicht anwendbar sein.

## 2 Sondierung der Anforderungen

Es soll in diesem Kapitel die möglichst praxisnahe Synthese aus den Anforderungen an eine forensische Sicherung, ein reguläres Backup und die gerichtliche Auswertbarkeit gelingen. Dafür wird im ersten Schritt möglichst nach relevanten Anforderungen aus den drei Bereichen gesucht und diese werden gelistet. Den vertiefenden Schwerpunkt stellt hierbei die forensische Sicherung dar. Aus ihren Anforderungen soll das Maß für den Forensischen Wert gebildet werden.

### 2.1 Evaluierung forensischer Frameworks

Um eine Grundlage zu bilden, wurde untersucht, welche Frameworks oder Best Practices eine größtmögliche Relevanz haben, um daraus Anforderungen abzuleiten. Dafür wurde nach Metastudien zur Relevanz konkreter Frameworks und Best Practices im Zeitraum vom 28.02. bis 11.03.2024 recherchiert.

#### 2.1.1 Methodik der Literatursuche

Es sollen Arbeiten gefunden werden, die im besten Fall die Relevanz unterschiedlicher forensischer Frameworks und Best Practices bereits untersucht haben. Gibt es diese nicht, dann soll zumindest eine hergeleitete Listung existierender Frameworks und Best Practices untersucht werden, um daraus Gemeinsamkeiten abzuleiten. Diese Listung soll priorisierte Relevanz für Deutschland haben, da sich die regulatorischen Vorgaben zwischen den Ländern unterscheiden können.

#### **Genutzt wurden folgende wissenschaftliche Datenbanken und Suchmaschinen:**

- IEEE Explore als digitale Bibliothek der IEEE. Sie wurde durchsucht als Quelle für wissenschaftliche Artikel, Konferenzberichte, Standards und Bücher, unter anderem aus dem Bereich der Informatik.
- ACM Digital Library ebenfalls eine renommierte Bibliothek als zusätzliche Resource der zuvor genannten Inhalte.
- Die Suchmaschine Google Scholar komplettiert die Suche als breites Suchinstrument für wissenschaftliche Literatur ab.

Zum Zeitpunkt der Literaturrecherche war die DBLP-Datenbank entweder nicht vollständig durchsuchbar oder es sind wenige Werke zur IT Forensik in ihr enthalten, sodass sie für diese Arbeit keine relevanten Ergebnisse lieferte.

#### **Genutzt wurden folgende wissenschaftliche Journale**

Für eine tiefere Literaturrecherche wurden die 50 höchstgewerteten Journale, gemessen am SCImago Journal Rank (SJR), durchsucht. Das SJR bewertet Journale basierend auf verschiedenen Metriken wie der Anzahl der Zitate, die Veröffentlichungen erhalten, und dem Prestige der zitierenden Quellen. Es wird angenommen, dass diese Bewertungen eine Einordnung über die wissenschaftliche Qualität und den Einfluss verschiedener Akteure in der Forschungswelt bieten. Gesucht wurde nach Journalen aus dem Bereich „Computer Science“ die nach ihrem Titel die Möglichkeit enthalten, IT-Forensische Themen zu behandeln.<sup>[5]</sup>

### Suchstrategie Metastudien

- Relevant sind alle Treffer mit den Strings [„Digital Forensic“ oder „IT Forensic“ oder „IT Forensik“] im Abstrakt. Dies soll das Thema der Arbeit eingrenzen. Es sollen hiermit sowohl englische als auch deutsche Ergebnisse einbezogen werden. Das Abstrakt als Suchziel schränkt potenzielle Treffer ein, unter der Annahme, dass wenn diese Themen Relevanz in der Arbeit haben, dies sich auch im Abstrakt niederschlägt. Dies öffnet das Suchspektrum gegenüber einer reinen Titelsuche, engt es aber gegenüber einer Volltextsuche ein.
- Relevante Treffer müssen zudem im Abstrakt die Strings [framework oder „Best Practice“] beinhalten
- Relevante Treffer müssen zudem aus dem Titel ersichtlich ergeben, dass es sich um vergleichende Arbeiten handelt. Dies wird bei folgenden Strings angenommen: „comparative“ oder „review“ oder „survey“ oder „vergleich“. Auch hier werden Arbeiten sowohl auf Englisch als auch auf Deutsch adressiert.
- Die Arbeiten sollen innerhalb der letzten zehn Jahre erstellt worden sein (2014 – 03/2024).
- Im Anschluss fand ein Relevanz-Screening der Ergebnisse statt. Dies berücksichtigte in der ersten Stufe die Prüfung der Überschrift und anschließend die Sichtung des Abtrakts. Als Treffer werden potenziell relevante Arbeiten bezeichnet, welche dabei identifiziert wurden.

Die Suchstrings zu den unterschiedlichen wissenschaftlichen Datenbanken können der Tabelle [A\_1] entnommen werden.

In den Treffern wurden Arbeiten zum Thema Cloudforensik in die relevanten Artikel aufgenommen, da ein OnPremise Backup der Cloud-Daten aus verschiedenen Gründen [Herstellerunabhängigkeit, Datensicherheit, Misstrauen gegenüber Verfügbarkeit und Weitere] nicht unüblich ist <sup>[03] [04] [05]</sup>. IoT Forensik wird hier nicht betrachtet, da sich die Untersuchung und Sicherung stark gegenüber klassischen IT-Systemen unterscheidet.

### Suchstrategie erweitert: Journale

In den Journalen selbst wurde nach einem Filter analog zur Suche in wissenschaftlichen Datenbanken recherchiert [vgl. Kapitel Suchstrategie Metastudien]. Da die Kriterien in der ersten Iteration zu eng erschienen, wurden sie erweitert. Zu finden sind die angepassten Filter in der Tabelle [A\_2] im Anhang.

## 2.1.2 Ergebnis der Literatursuche

DB\_01\_01 (Kumar Shanu Singh; Annie Irfan; Neelam Dayal)

### Cyber Forensics and Comparative Analysis of Digital Forensic Investigation Frameworks<sup>[06]</sup>

In der Arbeit DB\_01\_01 werden 15 unterschiedliche Digital forensic investigation frameworks, DFIF, aus einem Zeitraum zwischen 2003 und 2019, inhaltlich untersucht. Ausgangspunkt ist die zum Erstellungszeitpunkt aktuelle OWASP-Auswertung aus dem Jahr 2017 und der Cyber Crime Report von EY aus dem Jahr 2018. Aus ihnen werden Trends zu Cyberangriffen abgeleitet. Es wird aus den identifizierten DFIF eine Liste mit einer Phasenunterteilung [Readiness, Reconnaissance/Footprinting, Investigation, Presentation, Incident Closure] der forensischen Untersuchung erstellt. Diesen Phasen werden Prozesse oder Aktivitäten zugeordnet <sup>[07]</sup>.

Die Phase Reconnaissance/Footprinting ist durch die Sammlung und das Handling des Beweismaterials definiert<sup>[08]</sup>. Innerhalb dieser Phase sind Prozesse/Aktivitäten identifiziert, welche abstrakt sind, sich dadurch aber eignen, konkrete Anforderungen zu gruppieren. So ergeben sich aus dieser Arbeit zwei methodische Elemente, welche hier in der Arbeit aufgenommen werden:

- 1.) Beschränkung der Untersuchung auf die Phase: Reconnaissance/Footprinting
- 2.) Prozess/Aktivität innerhalb der Phase<sup>[07]</sup>:

| ID     | Aktivitäten                                                            |
|--------|------------------------------------------------------------------------|
| Akt_01 | Bestimmen potenzieller digitaler Beweise und potenzieller Quellen      |
| Akt_02 | Bestimmen der physikalischen Verortung des Beweises                    |
| Akt_03 | Überführung des Beweises in Daten                                      |
| Akt_04 | Sicherstellung der Authentizität und Integrität des digitalen Beweises |
| Akt_05 | Aufbewahrung des digitalen Beweises in einer sicheren Umgebung         |
| Akt_06 | Isolierung des digitalen Beweises zum Schutz vor Manipulation          |
| Akt_07 | Erstellen von Kopien des digitalen Beweises durch Standardprozeduren   |

**Tabelle 1: Aktivitäten der Phase Reconnaissance**

Ziel dieser Arbeit ist die inhaltliche Zusammenführung bestehender Frameworks. Dabei ist die Relevanz oder Autorität der einzelnen Arbeiten unberücksichtigt und kann nicht direkt abgeleitet werden.

DB\_01\_02 (Ummer Farooq; Arslan Shaukat; Wasi Haider Butt; Ali Hassan)

### **A Systematic Literature Review of Latest Cloud Forensic Frameworks, Tools and Challenges<sup>[09]</sup>**

Das Ziel der Arbeit DB\_01\_02 ist die Erstellung einer Literaturübersicht zu Cloudforensik-Frameworks, das Aufzeigen der Herausforderungen in diesem Bereich und die Listung von Tools zur Cloudforensik<sup>[10]</sup>. Dazu wurde eine systematische Literaturrecherche durchgeführt, unter anderem zu der Forschungsfrage 1 <sup>[11]</sup>:

“What are the latest frameworks and methods used in cloud forensics from 2010 to 2022?” <sup>[12]</sup>

Als Ergebnis werden in Summe 36 Methoden, Frameworks und Prozesse tabellarisch aufgeführt und deren Inhalt einzelnen Phasen einer forensischen Untersuchung zugeordnet [Incident Identification & reporting, Case Initiation & Planning, Evidence Collection & Acquisition, Evidence Examination & Analysis, Presentation & Legal Proceeding]. Innerhalb dieser Phasen wird dargestellt, welche Aktivitäten vom jeweiligen Paper gedeckt sind <sup>[13]</sup>. So ergibt sich eine recht aktuelle Übersicht über Methoden, Frameworks und Prozesse der Cloudforensik sowie Anhaltspunkte zu deren Inhalt.

Setzt man DB\_01\_02 in ein Verhältnis zu DB\_01\_01 entspräche die Phase Evidence Collection & Acquisition der Phase Reconnaissance/Footprinting. Innerhalb dieser sind die Aktivitäten in DB\_01\_02 teilweise zwar ausdifferenzierter (zb: raw data gathering; Live/static data acquisition; collection, versus [Akt\_07] Erstellen von Kopien des digitalen Beweises durch Standardprozeduren), was aber auf die fehlende Normalisierung der Aktivitäten zurückzuführen ist. Ersichtlich wird dies dadurch, dass in Zeile 21 DB\_01\_01 selbst aufgeführt ist, die aufgeführten Aktivitäten allerdings Framework spezifisch bleiben. Dies, obwohl sie auf der angewandten Abstraktionsebene trivial zu konsolidieren wären. Andersherum betrachtet kann dies als Indiz für die Allgemeingültigkeit der Kategorisierung aus DB\_01\_01 gewertet werden. Ein Rückschluss auf die Verbreitung oder Autorität der einzelnen Frameworks ist aus dieser Quelle nicht möglich.

DB\_03\_01 (Fakeeha Jafar, Rabail Shafique Satti)

### **Comparative analysis of digital forensic models<sup>[14]</sup>**

In der Arbeit DB\_03\_01 wird davon ausgegangen, dass unangemessene forensische Methoden zu fehlenden oder unvollständigen Beweisen führen können<sup>[15]</sup>. Daher bedarf es eines systematischen Ansatzes<sup>[16]</sup>. Um Fehler vorzubeugen, werden acht Frameworks jeweils kurz beschrieben und aus Sicht der Autoren die Vor- und Nachteile umrissen. Kernstück der Arbeit ist ein ausdifferenziertes Inhaltsmodell (20 Steps), das mit dem Inhalt der untersuchten Frameworks abgeglichen wird. Dies geschieht auf binärer Basis (Eigen-

schaft vorhanden/nicht vorhanden)<sup>[17]</sup>. Das Paper schließt mit dem Ergebnis, das „Systematic digital forensic investigation model“ sei auf Basis der untersuchten Attribute das passendste Modell für forensische Analysen, da es komplette und konkrete Schritte zur Durchführung von forensischen Sicherungen beinhalte und als einziges Modell „exploratory testing“ biete<sup>[18]</sup>. Die Autoren selbst schreiben in ihrer Zusammenfassung unspezifisch, das sie einige digitale Frameworks untersucht hätten, („This paper reviewed some common forensics investigation models [...]“<sup>[19]</sup>) ohne die Relevanzkriterien zu benennen. Aus ihrer Analyse ist daher die Verbreitung oder Anwendung nicht ableitbar.

### Auswahl und Auswertung von Frameworks zur forensischen Sicherung

In der Literaturrecherche ist es nicht gelungen, wissenschaftliche Arbeiten zur Bestimmung der Relevanz einzelner Frameworks zu bestimmen. Um trotz der fehlenden wissenschaftlichen Quellen eine Auswahl an relevanten Frameworks zu erhalten, greife ich auf nationale Cyber-Security Institutionen zurück, welche sich durch ihre Autorität anbieten. Aufgrund dieser wird die praktische Relevanz, auch in Ermangelung belastbarer Quellen, weiterführend angenommen. Da eine grundlegende Konsistenz in den Publikationen innerhalb einer Agentur anzunehmen ist, werden jeweils zwei möglichst weitreichende Dokumente als Grundlage verwendet.

| ID    | Name                                                                                             | Anlage |
|-------|--------------------------------------------------------------------------------------------------|--------|
| FR_01 | BSI: Leitfaden IT-Forensik <sup>[20]</sup>                                                       | A_3    |
| FR_02 | BSI: Grundschutz Kompendium mit Baustein: DER.2.2 <sup>[21]</sup> : Vorsorge für die IT-Forensik | A_4    |
| FR_03 | NIST: SP 800-86 Guide to Integrating Forensic Techniques into Incident Response <sup>[22]</sup>  | A_5    |
| FR_04 | NIST: IR 8387 Digital Evidence Preservation <sup>[23]</sup>                                      | A_6    |

**Tabelle 2: relevante Frameworks BSI & NIST forensische Sicherung**

Die als relevant identifizierten Frameworks aus dem vorherigen Kapitel wurden nach Anforderungen durchsucht und diese aus dem Kontext oder direkt entnommen. Da es sich teilweise um Fließtexte handelt oder Anforderungen nicht atomar sind, werden Anforderungen in dieser Arbeit neu indexiert. Mindestens auf die Kapitel wird in der Quelle der Anforderung referenziert. Zudem werden die Anforderungen inhaltlich, soweit es sinnvoll erschien, abstrahiert und frameworkübergreifend gruppiert, sofern sie sich inhaltlich deckten. Innerhalb der Frameworks wurde gefiltert auf die Phase Reconnaissance/Footprinting aus DB\_01\_01 und sie wurden nach Aktivitäten [Akt\_01 - Akt\_07] gruppiert, um Konsolidierungsschritte nachvollziehbarer zu gestalten, da sie in kleineren Einheiten geschehen. Die Anforderungen sind aufgetragen in den Tabellen A\_03, A\_04, A\_05 und A\_06.

## 2.2 Evaluierung der gerichtlichen Verwertbarkeit

Die forensische Sicherung dient der Konservierung von digitalen Spuren. Diese können vor Gericht, qualifiziert durch einen Sachverständigen oder vor einem qualifizierten Gericht, als Sachbeweise Verwendung finden. In diesem Kapitel wird untersucht, welche

Probleme es bei der Beweiswürdigung vor Gericht auf dem aktuellen Forschungsstand gibt. In Ermangelung einer juristischen Ausbildung des Autors wird sich in diesem Kapitel auf Sekundärquellen berufen, welche die juristischen Herausforderungen bei der Beweiswürdigung von digitalen Daten und Datenverarbeitungsmethoden benennen. Aus diesen Herausforderungen werden Anforderungen abgeleitet, die dann in den Katalog der Anforderungen für forensische Backups aufgenommen werden. Grundlage der Untersuchung bildet dabei die Habilitation von Christian Rückert „Digitale Daten als Beweismittel im Strafverfahren“ aus dem Oktober 2023<sup>[24]</sup>. In der Annahme, dass die Zivil- und die Strafprozessordnung (ZPO, StPO) am Ende auf dieselben Probleme stoßen, wird die Verengung auf Strafverfahren akzeptiert. In beiden Fällen hat das Gericht unter Berücksichtigung des Inhalts der Verhandlung nach seiner freien Überzeugung über das Ergebnis der (etwaigen) Beweisaufnahme zu entscheiden (§ 286 Abs. 1 ZPO, § 261 StPO).

Nach Rückert gebe es drei „digitale Grundrechte“ [Telekommunikationsgeheimnis, Recht auf informationelle Selbstbestimmung, Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme], in die eine Beweisdatengewinnung eingreife<sup>[25]</sup>. Die juristische Argumentation mit europa- und verfassungsrechtlicher Abwägung wird im Rahmen dieser Arbeit ausgeklammert. Im Gegensatz zu US-amerikanischen Gerichten, wo auf verschiedene präjudizierte Standards zurückgegriffen werden kann, wie zum Beispiel der Frye- oder Daubert-Standard<sup>[46]</sup>, erzwingt die StPO keine starren Beweisregeln<sup>[26]</sup>. Rückert schließt seine gut 800-seitige Habilitation mit „Kapitel 8: Zentrale Probleme der Verwendung von Daten und Datenanalysen als Beweismittel in der Hauptverhandlung“<sup>[27]</sup>. Dieses Kapitel fasst die „praxisbedeutsamen und zentralen Probleme“ bei der Verwendung digitaler Beweismittel zusammen<sup>[28]</sup>.

Probleme werden aus der Arbeit von Rückert hier in ihren Überkapiteln benannt, anschließend kurz beschrieben und je Kapitel technisch/organisatorische Anforderungen abgeleitet. Das entspricht dem Vorgehen aus dem vorherigen Kapitel, nur dass es sich hier nun um eine Sekundärquelle handelt, die sich juristisch begründet.

### **Das Übersetzungsproblem: Daten, Informationen und der Grundsatz des sachnäheren Beweismittels<sup>[29]</sup>**

Er zeigt auf, dass in der Rechtspraxis oft qualitativ minderwertigere Beweise wie Ausdrucke oder Bildschirmbeweise (visuelle Informationen) Anwendung finden<sup>[30]</sup>. Diese stünden den höherwertigen Originaldaten bzw. der Kopie derer gegenüber<sup>[31]</sup>. Originaldaten bedingen allerdings ein Gutachten oder den Augenschein eines qualifizierten Tatgerichts<sup>[31]</sup>. Ob der Augenscheinbeweis sachfernerer Beweismittel hinreicht, sei abhängig vom Einzelfall<sup>[34]</sup>. Es leite sich aus der Pflicht zur Ermittlung der materiellen Wahrheit ab, dass zur Beweiswürdigung die objektiv tragfähige Tatsachengrundlage zu bilden sei<sup>[31]</sup>. Rückert führt deren Bedingungen für das Tatgericht (StPO) auf<sup>[32]</sup>. Abgeleitete Anforderungen sind der Anlage Anlage A\_7 zu entnehmen. Im Konkreten reichten visualisierte [logische] Informationen aus, sofern durch eine IT-Forensische Auswertung keine zusätz-

lichen Erkenntnisse zu erwarten wären. Dies stehe allerdings juristisch im Spannungsfeld zum Verbot der Beweisantizipation des Gerichtes<sup>[33]</sup>.

Für diese Arbeit relevant und übertragen ergibt sich aus dieser Analyse, dass Daten auch auf logischer Ebene in der Rechtspraxis Anwendung finden, dies sogar, wenn eine physische Sicherung vorliegt. Es reicht demnach aus, wenn der digitale Beweis eine objektiv tragfähige Tatsachengrundlage bildet. Um diese Grundlage zu schaffen sind die Anforderungen im Konkreten allerdings fallspezifisch. Allgemeine Anforderungen sind in A\_7 eingeflossen.

### **Flüchtigkeit und Manipulierbarkeit: IT-forensische Standards und strafprozessuales Beweisrecht<sup>[34]</sup>**

Wegen der leichten Manipulierbarkeit und Flüchtigkeit digitaler Daten sei der Nachweis über die Unverändertheit und Ursprungsechtheit entscheidend für die Beweiskraft<sup>[35]</sup>. In diesem Kapitel leitet Rückert aus dem Beweisrecht her, warum das Gericht die Authentizität und Integrität der Daten berücksichtigen muss<sup>[36]</sup>. Dies sei ableitbar aus dem Grundsatz der Lückenlosigkeit der Beweiswürdigung, vor allem, um den Beweiswert des einzelnen Artefaktes zu erhöhen. Zudem könnte bei Nichtwahrung forensischer Grundsätze die Perspektive des Gerichtes verzerrt werden<sup>[36]</sup>. Beide Punkte zusammen widersprechen dem Prinzip der vollständigen und erschöpfenden Beweiswürdigung.

Die forensischen Grundsätze werden aufgezählt und sind in A\_7 aufgegangen.

### **Beweiswert und Beweiswürdigung von Datenanalyseergebnissen<sup>[37]</sup>**

Dieses Kapitel richtet sich vor allem auf (komplexe) Datenanalysen, welche unstrittig einen Beweiswert hätten<sup>[38]</sup>. Der Beweiswert hänge von den verwendeten forensischen Methoden ab. Erkenntnisse seien für die Beweiswürdigung bindend, sofern die verwendete Methode sogenannte gesicherte wissenschaftliche Erkenntnisse gewährleiste<sup>[38]</sup>. Dies seien insbesondere deterministische, abgeschwächt auch statistische Methoden<sup>[39]</sup>. Aus Erfahrungsgrundsätzen abgeleitete Erkenntnisse, hätten eine geminderte Bindungswirkung<sup>[39]</sup>. In Ermangelung einer breit akzeptierten, standardisierten Analysemethodik und revisionsrechtlicher Rechtsprechung obliege dem jeweiligen Tatgericht die Prüfung der angewandten Methode, was hohe Darstellungsanforderungen bedinge, weil Richtigkeitswahrscheinlichkeiten fallspezifisch beurteilt werden müssten<sup>[40]</sup>.

Eingeordnet in das SAP-Modell geht es in diesem Kapitel vornehmlich um den Analyse-Schritt in der forensischen Untersuchung, weniger um "Secure" (SAP-Modell), dem Reconnaissance/Footprinting aus DB\_01\_01. Trotzdem wurden die Merkmale einer gesicherten wissenschaftlichen Erkenntnis in die Anforderungen übernommen, um die Grundlage einer Analyse bilden zu können, mit möglichst hohem Bindungswert für das Tatgericht. Hier geht es vor allem um die Sicherungsmethode, welche denselben Anforderungen wie einer Analysemethode unterworfen werden soll. Dies erscheint übertragbar, weil in dem Kapitel vor allem methodische Anforderungen beschrieben werden.

**Das Blackbox-Problem und strafprozessuales Beweisrecht<sup>[41]</sup>**

Hat das Tatgericht kein Verständnis für die eingesetzten Methoden oder Techniken der Datenverarbeitung, sei es ihm nicht möglich, die Verlässlichkeit der Ergebnisse exakt zu bestimmen<sup>[42]</sup>. Dies könne umso mehr ein Problem darstellen, wenn bei der Datenanalyse [oder auch Akquise] Tools eingesetzt werden, die auch für den Gutachter selbst nicht vollständig transparent arbeiten, weil zum Beispiel Quellcodes oder Funktionsweisen Betriebsgeheimnisse des Herstellers sind<sup>[43]</sup>. Zudem gebe es Techniken, zum Beispiel Machine-Learning oder KI-Anwendungen mit prinzipiellen Nachvollziehbarkeitsmängeln<sup>[44]</sup>. Es seien aus diesem Grund Tools mit bekannter Funktionalität grundsätzlich bevorzugt zu verwenden<sup>[45]</sup>. Sollten andere Tools im konkreten Fall besser geeignet sein, ergebe sich aus der Aufklärungspflicht die Verwendung des bestmöglichen und sachnächsten Beweismittels unter Ausschöpfung aller möglichen Mittel<sup>[45]</sup>. Dies schließe auch Blackbox-Tools ein, also Werkzeuge, deren Techniken und konkrete Methoden nicht vollständig transparent sind<sup>[45]</sup>.

Für die deutsche StPO ergebe sich die gerichtliche Verwertbarkeit aus der Anforderung, dass nach Möglichkeit ein Tool mit bekannter Funktionalität verwendet werden soll. Dies wird in A\_7 ergänzt. Der US-Amerikanische Ansatz diese Problematik zu lösen ist die Standardisierung mittels des Computer Forensics Tool Testing Programs der NIST.

**Auswertung der gerichtlichen Auswertbarkeit**

Aus diesen Problemen lassen sich grundlegende Anforderungen für ein digitales Beweismittel im Strafprozess ableiten. Um es für den juristisch nicht ausgebildeten Autor und Leser greifbarer zu machen, werden die Begrifflichkeiten in einen für den Autor zugänglicheren Sprachgebrauch überführt. Dies passiert im Bewusstsein sprachliche Genauigkeit im juristischen Sinn einzubüßen.

Die Eigenschaften des Beweises unterscheiden sich dabei, ob sie Attribut des Artefaktes selbst oder der Analyse sind. Analytische Eigenschaften der gerichtlichen Verwertbarkeit spielen in der Betrachtung dieser Arbeit, ebenso wie die Objektivität der Betrachtung, keine Rolle, da sie Teil des Ergebnisses der Begutachtung bzw. eine Eigenschaft des Gutachters sind. So verbleiben Eigenschaften, die dem Artefakt inhärent sind. Diese zusätzliche Kategorisierung ist notwendig geworden, da sich herausstellte, dass die Aktivitäten aus DB\_01\_01 für die gerichtliche Verwertbarkeit nicht hinreichend sind, um für diese Arbeit relevante Eigenschaften herauszustellen.

| ID    | Eigenschaft                                                                                                           | Attribut     |
|-------|-----------------------------------------------------------------------------------------------------------------------|--------------|
| GR_01 | Relevanz, es muss direkt die strittige Frage adressieren                                                              | Analyse      |
| GR_02 | Herkunft und Verbleib müssen lückenlos nachvollziehbar sein.                                                          | Beweismittel |
| GR_03 | Authentizität/Integrität des Beweismittels muss nachgewiesen werden können                                            | Beweismittel |
| GR_04 | Adäquanz, das Beweismittel muss ausreichend sein die behauptete Tatsache in angemessener Stärke zu stützen            | Analyse      |
| GR_05 | Vollständigkeit des erfassten Beweismittels muss gegeben sein                                                         | Beweismittel |
| GR_06 | Kontext des Beweismittels sollte für Gutachter transparent sein,                                                      | Analyse      |
| GR_07 | Rechtl. Zulässigkeit des Beweismittels muss gegeben sein. Dies gilt sowohl für die Erhebung als auch die Verarbeitung | Beweismittel |
| GR_08 | Unbefangenheit beschreibt das Verhältnis des Gutachters zum Begutachtungsgegenstand und zum Fall.                     | Analyse      |

**Tabelle 3: Anforderungen für gerichtliche Verwertbarkeit**

## 2.3 Evaluierung des Regelbackups

### 2.3.1 Methodik der Literatursuche

Analog zur Methodik aus dem Kapitel 2.1 „Evaluierung forensischer Frameworks“ wird auch in diesem Kapitel davon ausgegangen, dass Frameworks, Regelwerke und Best Practices im Normalfall die Anforderung eines Regelbackups bilden. So werden hier ebenso aus dem Fließtext oder gelistete Anforderungen aus unterschiedlichen Quellen zusammengetragen, um einen Überblick über Anforderungen an reguläre Backups zu bekommen. Aufgenommen in die Anforderungsliste werden Anforderungen, die sich der Phase Reconnaissance/Footprinting aus DB\_01\_01 zuordnen lassen. Zur Erhöhung der Übersichtlichkeit werden Anforderungen mit dem Fokus des Kernthemas der Arbeit zusammengefasst oder abstrahiert. Zur Nachvollziehbarkeit ist jede Anforderung auf die Originalquelle referenziert. Zur leichteren Zuordnung werden zudem „gutmütig“ die Aktivitäten aus DB\_01\_01 den einzelnen Anforderungen versucht zuzuordnen. Dies gibt bereits einen ersten überblicksartigen Indikator über die Ähnlichkeit zwischen dem regulären Backup und forensischen Sicherungen und wird am Ende des Kapitels kurz diskutiert.

Analog zur Methodik 2/2 des Kapitel 2.1 sollen Publikationen der beiden nationalen Behörden, des NISTs und des BSIs die Grundlage der Anforderungen bilden.

Gesucht werden, ebenso analog zum Kapitel 2.1, Special Publications der NIST und Veröffentlichungen des BSI. Aus der Erfahrung hat sich gezeigt, dass Backup-Anforderungen zwischen spezifischen Richtlinien, Best Practices, Standards und Empfehlungen stark konvergieren. So wird hier auf eine Suche nach Meta-Betrachtungen verzichtet. Es werden jeweils zwei Auszüge der Agenturen als repräsentativ betrachtet.

Ausgewählt wurden diese nach ihrem allgemeingültigen Charakter um möglichst weitreichend Anforderungen berücksichtigt anzunehmen. Aus dieser Allgemeingültigkeit ergeben

sich umfangreiche Dokumente. Deshalb werden, wo nötig, zudem die konkreten Kapitel hier bereits gelistet. Auf US-amerikanischer Seite werden Special Publications der NIST herangezogen, auf Seiten des BSI das Grundsatzkompodium.

| ID    | Veröffentlichung                                                                                        | Relevante Kapitel                                                       |
|-------|---------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| BK_01 | NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations <sup>[47]</sup> | CP-9 System Backup<br>CP-10 System Recovery and Reconstitution          |
| BK_02 | NIST SP 800-34: Contingency Planning Guide for Federal Information Systems <sup>[48]</sup>              | 3.4.1 Backup & Recovery<br>3.4.2 Backup Methods and Offsite Storage     |
| BK_03 | BSI - IT-Grundsatz-Kompodium <sup>[49]</sup>                                                            | CON.3 Datensicherungskonzept                                            |
| BK_04 | Umsetzungshinweise zum Baustein CON.3 Datensicherungskonzept <sup>[50]</sup>                            | Vollständig, wird herangezogen zur Anforderungsspezifizierung von BK_03 |

**Tabelle 4: relevante Frameworks BSI & NIST Backup**

### 2.3.2 Ergebnis der Literatursuche

BK\_01 (NIST SP 800-53)

#### **Security and Privacy Controls for Information Systems and Organizations <sup>[50]</sup>**

Diese Publikation vereint unterschiedliche Anforderungsdokumente und stellt einen breiten Katalog, der Konsistenz zu anderen NIST-Dokumenten vorgibt. Das NIST SP 800-53 ist im Schwerpunkt ein umfangreiches Controlset, welches Sicherheits- und Datenschutzstandards für US-Amerikanische Bundesbehörden festlegt und bei der Risikobewertung hilft. Es wurde entwickelt, um den Schutz von Informationen und Systemen zu verbessern, indem konkrete Anforderungen formuliert sind. Sie bilden verbindliche, regulatorische Vorgaben für US-Bundesbehörden. Es werden 20 „Security and Privacy Control Families“ definiert, welche die einzelnen Themen clustern. Backup-Anforderungen sind in der Contingency Planning zusammengefasst.

Konkrete Anforderungen für diese Arbeit werden aus den Controlsets CP-9 System Backup und CP-10 System Recovery and Reconstitution entnommen. Jede Anforderung trägt unter anderem die Teile „Base Controls“, „Discussion“ und „Control Enhancements“. Die Anforderungen für diese Arbeit werden aus den Base Controls übernommen. Ergeben sich aus dem „Discussion“ oder den „Control Enhancement“ bemerkenswerte Anforderungen, werden auch diese im Einzelfall in den Anforderungskatalog A\_8 ergänzt. Innerhalb von BK\_01 sind Anforderungen mit Platzhaltern versehen, die kontextbezogen durch den Anwender zu füllen sind. Diese Platzhalter innerhalb der einzelnen Controls wurden in dieser Arbeit generisch gefüllt.

BK\_02 (NIST SP 800-34)

#### **Contingency Planning Guide for Federal Information Systems <sup>[51]</sup>**

Diese Richtlinie bietet einen Rahmen für Organisationen, um Maßnahmen zur Sicherstellung der Kontinuität ihrer IT-Dienste zu entwickeln, zu implementieren und zu verbessern.

Sie behandelt verschiedene Aspekte wie Risikoanalyse und Bewertung, Kontinuitätsplanung und Implementierung und Tests.

Es eignet sich diese Arbeit als Ergänzung für BK\_01, weil sie den Anspruch einer “real-world guideline” erhebt. Dies ist wichtig, da die Anforderungen aus den Dokumenten als praktische Umsetzung angenommen werden sollen. Über die Kontinuitätsplanung findet das Thema Backup Eingang in das Special Paper. Das Kapitel 3.4.1 ist allerdings recht abstrakt gehalten und beschreibt eher einen strategischen Ansatz. Die Ausführungen zur Wiederherstellung sind in dieser Arbeit zwar relevant, aber nicht maßgebend, sodass sie hier nur grob in [A\_1] erfasst werden.

BK\_03 & BK\_04

### **BSI - IT-Grundschutz-Kompendium**

#### **Umsetzungshinweise zum Baustein CON.3 Datensicherungskonzept <sup>[52]</sup> <sup>[53]</sup>**

Diese beiden Quellen können zusammengefasst werden, weil sie auf einer Basis, dem CON.3 existieren, wobei die Umsetzungshinweise BK\_03 konkretisieren. Auch hier wurden nach Sichtung die Anforderungen, welche im Kompendium aufgeführt werden, teilweise bereits abstrahiert oder zusammengezogen. Grundlage bilden die Standard-Anforderungen. Beschaffung und Informationsverpflichtungen werden dabei nicht beachtet, da sie für diese Arbeit keine Relevanz haben.

Anforderungen aus der Analyse der Dokumente wurden in Tabellen A\_8, A\_09 und A\_10 zusammengestellt.

## **2.4 Ergebnis der Anforderungssondierung**

Es wurden 129 Anforderungen an ein forensisches Backup identifiziert, wovon 110 grob den Aktivitäten aus DB\_01\_01 zugeordnet werden konnten. Dies entspricht einer Deckungsquote von etwas mehr als 85% (110/129), was allerdings eine verzerrte Darstellung ist, weil die forensischen Anforderungen hier Teil des Basiswertes sind. Nimmt man lediglich die Anforderungen vom regulären Backup und hält sie gegen die Aktivitäten der forensischen Sicherung, erhält man eine hohe Deckungsquote von etwas mehr als 73% (19/26). Außerhalb dieser liegen betriebliche Themen wie regelmäßige Tests oder die Festlegung der Häufigkeit und Scope der Sicherung. Der Anteil der gerichtlichen Anforderungen gegenüber den gutmütig zuzuordnenden Aktivitäten beschränkt sich auf die Anforderungen an das forensische Vorgehen. Mit einer Deckungsquote von rund 26% (4/15) weichen die gerichtlichen Anforderungen von den forensischen ab. Dies verwundert nicht weiter, weil hier methodisch bedingt die Anforderungen des Beweisstückes im Zentrum stehen und weniger die Datenerhebung. So bilden für die weitere Bearbeitung die Anforderungen aus den Tabellen [Forensische Anforderungen: A\_03, A\_04, A\_05, A\_06; Gerichtliche Verwertbarkeit: A\_07; Backup: A\_8, A\_09, A\_10] die Grundlage.

## 3 Forensischer Wert eines Regelbackups

### 3.1 Definition des Forensischen Wertes

Der forensische Wert soll in dieser Arbeit den zentralen Begriff bilden. Dafür soll in diesem Kapitel eine Arbeitsdefinition deklariert werden. Der Forensische Wert quantifiziert, wie wertvoll ein erhobenes Datum für die forensische Analyse ist. Er ist somit ein Maß für die forensische Verwertbarkeit und Güte. Er soll möglichst umfassend alle Dimensionen greifen, die eine forensische Sicherung zu einer guten Sicherung macht. Als gut wird eine Sicherung angenommen, die im Allgemeinen relevant, authentisch, integer, nachvollziehbar und gerichtlich verwertbar ist. Im Konkreten ergibt sich der Forensische Wert aus Anforderungen an eine forensische Sicherung, wie sie im Anhang A\_12 hergeleitet wurde. Um einen Vergleich zu ermöglichen, muss der forensische Wert abstufbar sein. Ihm wird deshalb eine Skala von 0 – 100 zugeordnet, die den Prozentsatz der erreichten gegenüber den maximal zu erreichenden Punkten beschreibt.

### 3.2 Ableitung der Metrik

Für die Bewertung, inwiefern eine Sicherung forensische Anforderungen erfüllt, wird eine Metrik angelegt. Ergebnis dieser Bewertung ist der Forensische Wert. Den Ausgangspunkt zur Bestimmung des Forensischen Wertes bilden die Anforderungen an eine forensische Sicherung. Da diese Anforderungen aus unterschiedlichen Frameworks und Kontexten zusammengetragen wurden, bedürfen die Anforderungen untereinander einer Normalisierung, welche Dopplungen, unterschiedliche Wortverständnisse oder verschiedene Beschreibungen konsolidiert. Um dies systematisch umzusetzen, sollen aus der Analyse der Anforderungen, welche in Kapitel 2 geschah, nun die Ergebnisse aufgearbeitet werden.

Ziele dabei sind:

- Möglichst atomare Anforderungen, mindestens nicht sinnvoll trennbar
- Zusammenfassende Beschreibung und Konsolidierung von geforderten Funktionen, Leistungsmerkmalen, Sicherheitsanforderungen und organisatorischen Anforderungen.
- Vereinheitlichen der Abstraktionsebene zwischen den Anforderungen
- Gruppierung der Anforderungen in die forensischen Dimensionen
- Nachvollziehbarkeit der Konsolidierungs- und Normalisierungsschritte
- Gewichtung der einzelnen Anforderungen innerhalb der Metrik

Das Ergebnis dieser Synthese ist eine Liste von normalisierten und konsolidierten Anforderungen, die sich aus den Quell-Frameworks ergeben. Sie ist der Tabelle [A\_12] des

Anhangs zu entnehmen. Neben der reinen Aufzählung der Anforderungen erscheint auch eine Gewichtung dieser notwendig. Es gibt Anforderungen, welche häufiger in den unterschiedlichen Frameworks Erwähnung finden als andere. Die Anzahl der Frameworks, welche die Anforderung beinhalten, soll das Gewicht der einzelnen Anforderung bilden. Dabei soll die Erwähnung je Framework wie eine zusätzliche Anforderung zählen. Die Anzahl aller Anforderungen (und Erwähnungen/Framework) aufsummiert, ergeben die maximale Punktzahl. Diese maximale Punktzahl (wird erreicht, wenn alle Anforderungen einer forensischen Sicherung umgesetzt sind) bildet einen Forensischen Wert von 100. Abgestuft wird dieser Wert in Abhängigkeit der Anzahl der erreichten Punkte.

Die beschriebene Tabelle als Bewertungsgrundlage zur Bestimmung des Forensischen Wertes befindet sich im Anhang als Tabelle [A\_14]. Die ID ist dabei der Tabelle A\_12 entnommen. Vorsortiert wurden die Anforderungen nach der forensischen Dimension, innerhalb dieser nach der Anzahl der Erwähnungen in unterschiedlichen Frameworks, also dem Gewicht der einzelnen Anforderung. In ihr sind auch Eigenschaften, die nicht direkt der Sicherung zuzuschreiben sind, vielmehr dem Umgang mit ihm.

### 3.3 Bewertung eines regulären Backups

Hierfür werden die Anforderungen einer forensischen Sicherung gegen eine fiktive Implementierung eines regulären Backups gesetzt. Zur Erlangung eines Basiswertes für den Forensischen Wert eines regulären Backups wird angenommen, dass umgesetzte Anforderungen aus dem Backup-Kontext auch die inhaltlich sehr ähnlichen forensischen Anforderungen umsetzen. Dies ist eine Unschärfe in der Arbeit, die in Kauf genommen werden muss, solange sie allgemeingültig sein soll. In dem Modell wird die komplette Umsetzung aller Backup-Anforderungen angenommen. Bei der Analyse stellte sich heraus, dass Anforderung L\_12 unterteilt werden musste, da sie nicht atomar formuliert wurde und aus der Backup-Last nur teilweise umgesetzt werden würde.

Die folgende Tabelle stellt die forensischen Lasten (L\_11 bis L\_30) in den linken Spalten den Backup Lasten (L\_01 bis \_10) auf der rechten Seite gegenüber. Verknüpft sind sie über den Faktor der Gewichtung (Spalte x). Im Tabellenfuß erfolgt die Auswertung.

| ID   | Forensik Last                                                                                                                                          | x | Backup Last                                                                                                                                                                                                                                                                                                              | ID           |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| L_11 | Analyseauslösendes Event muss dokumentiert sein                                                                                                        | 1 |                                                                                                                                                                                                                                                                                                                          |              |
| L_12 | Forensische Werkzeuge sollen in einem Katalog begründet vorausgewählt und verfügbar sein.                                                              | 4 | Es soll ein Datensicherungskonzept erstellt werden, das mindestens beinhaltet: [...] <ul style="list-style-type: none"> <li>• welche Hard- und Software eingesetzt wird.</li> </ul> Das Backup soll [...] nach dem Datensicherungskonzept durchgeführt werden.                                                           | L_01<br>L_08 |
| L_0a | Forensische Werkzeuge sollen eine Fehlererkennung implementiert haben, die Ungenauigkeit, Unvollständigkeit oder Missinterpretation sichtbar macht.    | 4 |                                                                                                                                                                                                                                                                                                                          |              |
| L_13 | Bei Werkzeugen muss sichergestellt sein, dass diese nicht manipuliert wurden                                                                           | 3 |                                                                                                                                                                                                                                                                                                                          |              |
| L_14 | Die Datensammlung soll auf allen potenziell betroffenen Komponenten durchgeführt werden, ggf. auch außerhalb des phys. Zugriffs                        | 2 | Es soll ein Datensicherungskonzept erstellt werden, das mindestens beinhaltet: [...] <ul style="list-style-type: none"> <li>• welche IT-Systeme und welche darauf befindlichen Daten durch welche Datensicherung gesichert werden,</li> </ul> Das Backup soll [...] nach dem Datensicherungskonzept durchgeführt werden. | L_01<br>L_08 |
| L_15 | Abänderungen der forensischen Sicherung gegenüber der Datenquelle sollen konkret nachvollziehbar sein.                                                 | 1 |                                                                                                                                                                                                                                                                                                                          |              |
| L_16 | Forensische Sicherungen sollen priorisiert nach Wert, Flüchtigkeit und Aufwand erfolgen                                                                | 2 |                                                                                                                                                                                                                                                                                                                          |              |
| L_17 | Es sollen die eingesetzte Methode und die einzelnen Schritte zur Datengewinnung dokumentiert werden, ebenso wie Eigenschaften des gesicherten Systems. | 3 | Es soll ein Verfahren geben, das für jedes IT-System bestimmt, welche Daten wie gesichert werden. Es soll mindestens Kritikalität der Daten und Einflussfaktoren berücksichtigen                                                                                                                                         | L_02         |
| L_18 | Aufrufparameter und Rückgaben der verwendeten Tools sollten integritäts- und authentizitätsgeschützt gespeichert werden.                               | 1 |                                                                                                                                                                                                                                                                                                                          |              |

|      |                                                                                                                                                    |   |                                                                                                                                                                                                                          |      |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|
| L_19 | Die originale Datenquelle soll durch den Prozess der forensischen Sicherung nachweisbar nicht geändert worden sein.                                | 2 | In virtuellen Umgebungen soll geprüft werden, ob das System durch Snapshot-Mechanismen der Virtualisierungs-umgebung gesichert werden kann                                                                               | L_03 |
| L_20 | Es sollen Schreibblocker eingesetzt werden, um die Integrität der originalen Datenquelle zu schützen                                               | 1 |                                                                                                                                                                                                                          |      |
| L_21 | Eine forensische Sicherung soll als physische Kopie des Datenträgers erstellt werden und diesen vollständig, inkl. reservierter Bereiche, abbilden | 3 |                                                                                                                                                                                                                          |      |
| L_22 | Über ein kryptographisches Verfahren soll nach der forensischen Sicherung das exakte Duplikat gegenüber dem Original nachgewiesen werden.          | 4 | Die Wiederherstellung soll in einen nachvollziehbaren Zustand geschehen. Dieser definiert sich über eine Integritätsprüfung und einen Konfigurationsstand                                                                | L_10 |
| L_23 | Forensische Sicherungen sollen auf zuverlässig gelöschten Medien gespeichert werden.                                                               | 2 |                                                                                                                                                                                                                          |      |
| L_24 | Forensische Sicherungen sollen nach einer zuvor festgelegten Zeit sicher gelöscht werden.                                                          | 2 |                                                                                                                                                                                                                          |      |
| L_25 | Forensische Sicherungen sollen in mehreren Kopien an unterschiedlichen Orten vorgehalten werden.                                                   | 2 | Eine Kopie der Backupdaten soll an einer Offsite-Location gehalten werden                                                                                                                                                | L_05 |
| L_26 | Ruhende forensische Sicherungen sollen verschlüsselt werden.                                                                                       | 2 | Sicherungsdateien sollen kryptografisch gesichert vor Manipulation, unbefugter Offenlegung, geschützt vor unberechtigtem Zugriff auf Medien in einer zugangsgeschützten, umweltskontrollierten Umgebung gehalten werden. | L_06 |
| L_27 | Foren. Sicherungen sollen im rechtlich/regulatorischen Rahmen erstellt werden                                                                      | 1 |                                                                                                                                                                                                                          |      |
| L_28 | Es soll sichergestellt sein, dass die [schriftlich] dokumentierten Prüfsummen nicht verändert werden können                                        | 1 |                                                                                                                                                                                                                          |      |
| L_29 | Es soll ein Zeuge bestätigen, wie bei der forensischen Sicherung vorgegan-                                                                         | 2 |                                                                                                                                                                                                                          |      |

|        |                                                                                                                                                      |    |                                                                                                                                       |      |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------|----|---------------------------------------------------------------------------------------------------------------------------------------|------|
|        | gen wurde, und die Prüfsummen beglaubigen                                                                                                            |    |                                                                                                                                       |      |
| L_30   | Im Umgang mit den Beweismitteln soll eine Chain of Custody gewahrt bleiben. Diese umfasst im Besonderen Verwahrung, Einsichtnahme, Quelle und Umgang | 4  | Es soll für Backupmedien und Backupdateien die physische Verortung, ein Namensschema, Retention und Transportmethode festgelegt sein. | L_04 |
| -      | Keine forensische Entsprechung                                                                                                                       | 0  | Das Backup soll in regelmäßiger Frequenz und zu festgelegten Zeitpunkten nach dem Datensicherungskonzept durchgeführt werden.         | L_01 |
| -      | Keine forensische Entsprechung                                                                                                                       | 0  | Bei Löschung von Backups soll ein Vieraugenprinzip herrschen.                                                                         | L_07 |
| -      | Keine forensische Entsprechung                                                                                                                       | 0  | In regelmäßigen Tests soll die Funktionalität der Sicherung und der Wiederherstellung in angemessener Zeit getestet werden.           | L_09 |
| Summe: |                                                                                                                                                      | 23 | /47 *100 =<br><b>Forensischer Wert = 49</b>                                                                                           |      |

Tabelle 5: Bewertung reguläres Backup

Legende:

|                              |                                |               |
|------------------------------|--------------------------------|---------------|
| Erfüllt, direkte Anforderung | Erfüllt, abgeleitete Umsetzung | Nicht erfüllt |
|------------------------------|--------------------------------|---------------|

Im Ergebnis erreicht ein reguläres Backup einen Forensischen Wert von 49. Es setzt die oben genannten Prämissen voraus, dass Anforderungen vollständig übertragbar und umgesetzt sind. An dieser Stelle wurden keine „mitgenommenen“ Punkte berücksichtigt, da sie keine explizite Anforderung an ein reguläres Backup sind.

Bemerkenswerterweise gibt es für die Regelbackups keine direkten Authentizitätsanforderungen. Im zuvor beschriebenen Modell wurde die **Authentizität** stillschweigend angenommen, ist aber nicht zwangsläufig nachweisbar. Authentizität ist jedoch für eine forensische Sicherung von einer solchen herausragenden Bedeutung, dass ohne diese nachweisen zu können bereits der Ansatz unbrauchbar sein kann, vgl. Kapitel 2.2 „Flüchtigkeit und Manipulierbarkeit“.

**Eine unvollständige Umsetzung** der forensischen Anforderungen hat zur Folge, dass Sicherungen zwar zu Analysen dienen können, zur gerichtlichen Verwertbarkeit ggf. jedoch nicht oder nur mit geschmälerter Bindungswirkung, vgl. „Beweiswert und Beweiswürdigung von Datenanalyseergebnissen“ im Kapitel 2.2. So hat die Vollständigkeit der Umsetzung einen erheblichen Einfluss auf die anschließende Verwertbarkeit. Dies ist in der eingeführten Metrik nicht berücksichtigt.

## 4 Erhöhung des Forensischen Wertes

Im folgenden Kapitel werden Ansätze untersucht, den Forensischen Wert von regulären Backups zu erhöhen. Ziel ist die Ableitung von Anforderungen für forensische Backups. Unter einem forensischen Backup wird ein reguläres Backup verstanden, das auf forensische Belange optimiert wurde. Virtuelle Maschinen (VM) bieten sich für beispielhafte Untersuchungen an, da mit ihnen das Filesystem gesichert wird, welches einer forensischen Sicherung unter üblichen Backup-Methoden am nächsten kommt. Die Anforderungen hierzu entsprechen der Tabelle A\_11. Um diese konkreter durchdenken zu können, wird eine Musterumgebung angenommen. Sie besteht aus einem ESXI-Cluster, einigen VMs und einem Backup-Service. In ihm werden die Anforderungen aus dem Kapitel zuvor komplett umgesetzt angenommen. Backups sollen über die vSphere Storage API über ein "Snapshotverfahren" (L\_03) ausgeführt und blockbasiert umgesetzt werden. Dies dürfte, wenn auch eine klassische, so doch eine (noch) häufige Szenerie sein. Es bietet sich an, die Erkenntnisse über die Musterumgebung hinaus anwendbar zu formulieren. Deshalb werden sie für beliebige IaaS-Umgebungen abstrahiert formuliert. Dies ermöglicht auch die Übertragung in ein Cloudsystem. Das hierbei zu Tage tretende Blackbox-Problem, das komplexe Infrastrukturen vor dem Anwender (oder Ermittler) versteckt, ist ungelöst. So wurde zum Beispiel zusammengefasst: "Currently, relying on the cloud service provider is unavoidable as the required cloud data resides in a virtual instance." <sup>[51]</sup>. Im Ergebnis dieses Kapitels soll geprüft worden sein, welche Anforderungen ein reguläres Backup erweitern können, um ein forensisches Backup zu begründen.

### 4.1 Methodik zur Erhöhung des forensischen Wertes

Es wurden die forensischen Anforderungen (Tabelle A12) in Themen zusammengefasst, die jeweils betrachtet werden. Die Zuordnung der Anforderungen zu den Themen ist der Tabelle A\_13 zu entnehmen. Innerhalb der Themen werden identifizierte Probleme aufgenommen und diskutiert. Teilweise werden Gedanken im Labor verifiziert. Jedes Thema schließt, falls notwendig, mit formulierten Anforderungen. Diese Anforderungen ergänzen die Anforderungen der regulären Backups. Diese ergänzenden Anforderungen zusammen mit jenen des regulären Backups stellen die Anforderungen eines Forensischen Backups dar.

## 4.2 Thema 1: Integritätsnachweis gegenüber der Quelle

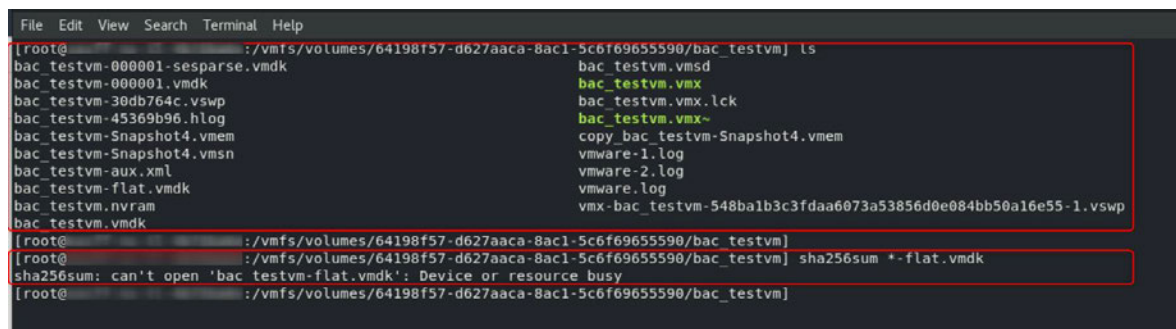
Wie bei der Evaluierung der gerichtlichen Verwertbarkeit gezeigt (Kapitel 2.2) ist die nachweisbare Integrität entscheidend für den forensischen Prozess und die Verwertbarkeit des Beweises vor Gericht. Die Anforderung L\_22 verlangt ein kryptografisches Verfahren, welches die Gleichheit des Abbildes gegenüber der Quelle belegt. Grundsätzlich gibt es zwei Möglichkeiten den kryptografischen Nachweis zu führen. Im klassischen Vorgehen wird von „außen“ auf die Quelle zugegriffen und lesend die Prüfsumme und das Image gebildet. Dies entspricht zum Beispiel dem Verfahren aus dem Leitfaden „IT-Forensik“. In der Cloudforensik gibt es Ansätze, von „innen“ Images zu synthetisieren. Dies geschieht aus Ermangelung des Zugangs zum originalen Medium. So gelingt die integrale Sicherung aus einer IaaS-Umgebung über einen Client<sup>[61]</sup>. Er läuft auf der VM und hat Zugriff auf die gesamte logische, Festplatte. Gestartet wird die VM aus einem forensischen Image. Das forensische Image besitzt eine bekannte Prüfsumme. Fortan werden vom Client die Änderungen auf der Festplatte mitgeschrieben und gehasht. Somit bleibt der Zustand der Festplatte und damit der Maschine über jeden Zeitpunkt nachweisbar. Dies entspricht einem transaktionsbasierten Verfahren und ermöglicht die Erstellung eines nachweisbar integren Images über die Maschine. Es ermöglicht eine forensische Sicherung unabhängig der unterliegenden Infrastruktur.

Analog zur klassischen forensischen Sicherung gibt es für die Sicherung von Backups in der Funktion ähnliche Verfahren. So kann bei entsprechender Schnittstelle zum Hypervisor von Außen die Festplatte „abgezogen“ werden. Dafür bieten verschiedene Hypervisoren unterschiedliche APIs (zB: ESXI-Hosts: VMware vSphere Storage APIs - Data Protection" (VADP)<sup>[59]</sup>, Hyper-V-Hosts: Hyper-V VSS Writer<sup>[60]</sup>). Diese APIs setzen ein Vertrauen in die Rückgaben des Hypervisors voraus, denn es ist von außen nicht ersichtlich, ob die übermittelten Festplattendateien integer und authentisch sind. Daraus ergibt sich, dass die Integrität erst innerhalb der Verwaltung der Backup-Systeme nachweisbar wird. Die Authentizität des erzeugten Abbildes muss entweder aus dem Vertrauen des Hypervisors heraus gewonnen oder durch eine Eigenschaft innerhalb der Maschine (zb. Privater Schlüssel) belegt werden. Üblicherweise ist die Authentizität des Hypervisors gegenüber dem Backup-System über den Abgleich des öffentlichen Schlüssels sichergestellt und wird als konfiguriert angenommen.

Für rein logische Sicherungen kommen auch in Backupsystemen Clients zum Einsatz. Sie sind aber nicht in der Lage, komplette Maschinen zu sichern, vielmehr geht es bei ihnen um filebasierte Backups. So können Ordnerstrukturen oder einzelne Dateien gesichert werden, jedoch keine Festplattendateien rekonstruiert werden. Bootfähige Medien zur Wiederherstellung entstammen nicht der direkten Sicherung, sondern einer Nachbildung. Der forensische Wert beschränkt sich hier auf das Vorhandensein von Dateien, ggf. ihren Metadaten. Weiterführend werden sie nicht näher betrachtet<sup>[57]</sup>.

### Problembeschreibung:

In klassischen Backup-Systemen beginnt die Integritätsprüfung nach dem Erstellen der Backup-Dateien. Integrität kann nachgewiesen werden vom Zeitpunkt des Abschlusses der Sicherung, über die Dateien der Sicherung bis zu ihrer Benutzung für die Wiederherstellung. Es werden nicht die gesicherten Dateien gegen die Wiederhergestellten geprüft. Dies ist hinreichend, um das Schutzziel der Integrität für die Sicherung zu gewährleisten, verlässt sich aber beim Erstellen und Wiederherstellen auf den Hypervisor. Um dies zu umgehen, wäre eine von außen angestoßene Prüfsummenbildung naheliegend. Sie ermöglichte den Abgleich der gesicherten und wiederhergestellten Festplattendatei. Da jedoch die Festplattendateien während des Betriebes der virtuellen Maschine hoch volatil sind, ist ein sinnvolles Erstellen einer Prüfsumme nicht möglich. Ein Herunterfahren der Maschine, um die Festplatte in einen statischen Zustand zu versetzen, wird in den meisten Umgebungen nicht hinnehmbar sein.



```

File Edit View Search Terminal Help
[root@ :/vmfs/volumes/64198f57-d627aaca-8ac1-5c6f69655590/bac_testvm] ls
bac_testvm-000001-sesparse.vmdk      bac_testvm.vmsd
bac_testvm-000001.vmdk               bac_testvm.vmx
bac_testvm-30db764c.vswp             bac_testvm.vmx.lck
bac_testvm-45369b96.hlog             bac_testvm.vmx~
bac_testvm-Snapshot4.vmem            copy_bac_testvm-Snapshot4.vmem
bac_testvm-Snapshot4.vmsn            vmware-1.log
bac_testvm-aux.xml                   vmware-2.log
bac_testvm-flat.vmdk                 vmware.log
bac_testvm.nvram                     vmx-bac_testvm-548ba1b3c3fdaa6073a53856d0e084bb50a16e55-1.vswp
bac_testvm.vmdk
[root@ :/vmfs/volumes/64198f57-d627aaca-8ac1-5c6f69655590/bac_testvm]
[root@ :/vmfs/volumes/64198f57-d627aaca-8ac1-5c6f69655590/bac_testvm] sha256sum *.flat.vmdk
sha256sum: can't open 'bac_testvm-flat.vmdk': Device or resource busy
[root@ :/vmfs/volumes/64198f57-d627aaca-8ac1-5c6f69655590/bac_testvm]

```

Abbildung 1: Erstellen einer Prüfsumme über .vmdk-Datei

In Abbildung 1 ist der erfolglose Versuch erkennbar, aus einer .vmdk-Datei eine Prüfsumme zu bilden. Ein Erstellen der Prüfsumme über die Festplattendatei ist auch im Snapshot nicht möglich.

### Beispiellösung (für die Musterumgebung):

Nach der Literatur-Recherche und Kontaktaufnahme sowohl zu VMware, Inc als Hersteller von VMware als auch zu veeam, als "leader" im Magic Quadrant for Enterprise Backup and Recovery Software Solutions von Gartner <sup>[52]</sup> und Bacula Systems SA als bedeutende OpenSource Anbieter wurde bestätigt, dass die Integrität und Authentizität erst nach der Erstellung und lediglich über die Backupdateien möglich ist. Technisch hänge dies mit der bereitgestellten API zusammen. Es scheint für dieses Schnittstellenproblem keine direkte Lösung zu geben. Daraus ergibt sich, dass akzeptiert werden muss, dass die Integrität (und Authentizität) der Backupdateien innerhalb des Backup-Systems lediglich nachgewiesen werden kann, nicht aber die Ursprungsdatei gegen die Wiederhergestellte.

**[L\_31] Integritätsnachweis: Allgemeine Anforderung forensisches Backup**

- Es soll ein Verfahren etabliert werden, dass mittels Kryptografie die Gleichheit zwischen gesicherten Systemen zum Zeitpunkt des Backups und der Wiederherstellung belegen kann. Anderenfalls muss akzeptiert werden, dass Integrität nur für die Backup-Dateien, nicht aber gegenüber den Original-Dateien, nachgewiesen werden kann.

### 4.3 Thema 2: Eigenschaften des Werkzeugs

Die benötigten Eigenschaften wurden aus der Tabelle A\_12 entnommen. Da in diesen Anforderungen lediglich die Akquise betrachtet wird, folgt, dass zur Auswertung der forensischen Backups eine Schnittstelle zwischen den Werkzeugen der Datenakquise und der Datenanalyse zusätzlich betrachtet werden muss.

Eigenschaften der Werkzeuge:

- **[L\_12]** Forensische Werkzeuge sollen in einem Katalog begründet vorausgewählt und verfügbar sein.
- **[L\_0a]** Forensische Werkzeuge sollen eine prozessbegleitende Dokumentation unterstützen
- **[L\_15]** Abänderungen der forensischen Sicherung gegenüber der Datenquelle sollen konkret nachvollziehbar sein
- **[neu ergänzt 01]** Werkzeuge sollen eine Schnittstelle zu etablierter forensischer Analyse-Software aufweisen.

Das forensische Werkzeug soll begründet und vorausgewählt werden [L\_12]. Dies ist eine Anforderung, die auf den breiten Szenarien-Katalog einer vollständigen forensischen Analyse zielt. Unter der Annahme, das Backup-System solle Teil der forensischen Software werden, müsste die Backup-Software in dem Katalog der forensischen Werkzeuge geführt werden. Um zu überprüfen, ob die Eigenschaften von Backup-Systemen sich auf den Katalog der forensischen Werkzeuge übertragen lassen, wurden exemplarisch die beiden zuvor erwähnten Tools [Veeam Backup & Replication; Bacula Enterprise] in den Kategorien des Computer Forensic Tools & Techniques Catalog der NIST (vgl. Tabelle 6) aufgeführt. Dies soll eine Möglichkeit der Attributierung über den Katalog zeigen und inhaltlich für diese beiden Tools einen Eindruck über ihre formale Eignung geben. Zur Begründung der Tool-Auswahl sollen die drei weiteren Anforderungen aus diesem Kapitel [L\_0a; L\_15; neu ergänzt 01] dienen.

**Problembeschreibung:**

**[L\_0a]** Backup-Tools sind ausgelegt zur regelbasierten, unbeaufsichtigten Ausführung von Aufgaben. Daraus ergibt sich, dass die prozessbegleitende Dokumentation auf eine automatisch erstellte Dokumentation beschränken muss. Einen Anhaltspunkt, über den benötigten Umfang bietet FR\_01\_Anf\_23. Dies wird als Grundlage genommen, muss aber

im Verständnis transferiert werden.

**[L\_15]** Änderungen werden von Backup-Tools schwerlich erkannt, wohl aber Fehler in der Erstellung.

**[neu ergänzt 01]** Das Format in dem Backuptools ihre Sicherungen ablegen ist häufig nicht direkt durch forensische Analysetools lesbar (zum Beispiel Veeam: vbk, vib, vbm<sup>[60]</sup>).

### **Beispiellösung (für die Musterumgebung):**

**[L\_0a]** Wie zuvor geschrieben soll FR\_01\_Anf\_23, eine Anforderung aus dem Leitfaden "IT-Forensik"<sup>[12]</sup>, als Basis für die Dokumentation genommen werden. Sie fordert prozessbegleitend folgende Punkte zu dokumentieren:

- Name und Versionsnummer des verwendeten Programms
- Kommandozeilenparameter des Aufrufs
- Forensische Absicherung dieses Werkzeugs
- Erfahrung des Untersuchenden mit diesem Werkzeug
- Motivation zur Auswahl dieses Werkzeugs

Wenn auch nicht zwangsläufig prozessbegleitend, können Name und Versionsnummer des verwendeten Werkzeugs zur forensischen Sicherung organisatorisch gesichert dokumentiert werden. Dies könnte über Dokumentationsanforderungen der Umgebung oder der Prozesse sichergestellt werden. Dies erlaubt indirekte Schlüsse, welches Werkzeug für eine konkrete Sicherung verwendet wurde. Überdies kann geprüft werden, ob die Logeinstellungen des jeweiligen Herstellers der Backup-Software eine Version angeben können. Dies ist gängige Praxis und wird bei den beiden untersuchten Produkten im Standard mitgeschrieben. Somit ist die erste dokumentarische Anforderung erfüllt.

In Backupsystemen werden Attributierungen nicht zwangsläufig durch Kommandozeilenparameter vorgenommen. Gängig ist auch die Konfiguration über Dateien oder ein grafisches Interface. Daher wird hier Kommandozeilenparameter des Aufrufs als Attributierung des Jobs angenommen. Eigenschaften der Jobs sollten über das Konfigurationsmanagement [OPS.1.1.7.A14] vorgehalten werden. Da die ausgeführten Jobs in der Regel statisch konfiguriert sind, wird deren Parametrisierung im Konfigurationsmanagement nachvollzieh- und rückverfolgbar. In Kombination mit den Logs, welche spezifisch für den jeweils ausgeführten Job geschrieben wurden, ergibt sich so eine Dokumentation, die prozessbegleitend die dynamischen Inhalte protokolliert. Die letzten drei dokumentarischen Anforderungen sollen hier nicht weiter betrachtet werden. Die Absicherung des Werkzeugs ist Voraussetzung für dessen Betrieb. Die Erfahrung des Untersuchenden ist Eigenschaft des Analysten. Mit der Motivation über die Auswahl des Werkzeugs schließt dieses Kapitel nach dem nächsten Absatz.

**[L\_15]** Einen konkreten, forensisch gültigen Nachweis über Änderungen gegenüber der Quelle gibt es für die physische Sicherung lediglich auf Bit-Ebene der Festplatte. Hierauf

zielt die Anforderung. Dies können die beiden überprüften Backupsysteme nicht leisten. Allerdings haben sie Schutzmechanismen gegenüber Datenkorruption. Zufällige Änderungen werden erkannt. Ist ein Backup nicht zuverlässig erstellbar, wird die Erstellung fehlerhaft terminiert. Im Umkehrschluss können Sicherungen, die fehlerfrei beendet werden als gültige Sicherungen angenommen werden. **[neu ergänzt 01]:** Für die Übergabe an ein forensisches Tool bietet sich im Rahmen des forensischen Backups eine Wiederherstellung der Festplattendatei (.vmdk) an. Es ist ein etabliertes Verfahren, Festplatten (Dateien) in forensische Analyse-Tools zu laden, welche von dort genutzt werden können. Dieses Vorgehen kann auch zur direkten Auswertung von .vmdk-Dateien genutzt werden<sup>[54]</sup>.

Zur Schließung des Kapitels soll nun noch die Motivation für die Auswahl der Tools untersucht werden. Es wäre unüblich, würden Backup-Tools nach forensischen Kriterien ausgesucht. Betriebliche Anforderungen stehen im Vordergrund, wodurch forensische Eigenschaften jedoch gedeckt sein können. Es bleibt im Regelfall die Beschreibung der Backup-Werkzeuge in forensischen Kategorien, um die (nachrangigen?) Anforderungen zu prüfen. Beispielhaft für die Aufnahme in den Katalog forensischer Werkzeuge wurde überprüft, inwiefern die beiden bisherigen Tools sich in Kategorien des Computer Forensic Tools & Techniques Catalog der NIST<sup>[56]</sup> zuordnen lassen. Für Bacula wird der Einsatz des vsphere-Plugins angenommen, für Veeam Backup die Enterprise Version.

| Forensic Functionality: Disk Imaging                            | Veeam® Backup & Replication | Bacula Enterprise   |
|-----------------------------------------------------------------|-----------------------------|---------------------|
| Tool host OS / runtime environment                              | Windows                     | Linux               |
| Supported evidence interfaces                                   | VADP                        | VADP                |
| Supported target/destination interfaces                         | VADP                        | VADP                |
| Types of data that may be acquired                              | .vmdk                       | .vmdk               |
| Supported acquisition methods                                   | Virtual Disk                | Virtual Disk        |
| Supported image file formats                                    | .vbk                        | volumes             |
| Support for restoring the contents of an image file to a device | yes                         | yes                 |
| Digest hash algorithm                                           | MD5, SHA-1, SHA-256         | MD5, SHA-1, SHA-256 |
| Data encryption                                                 | optional                    | optional            |

**Tabelle 6: Katalogisierung Backuptools im Katalog forensischer Tools**

Ohne Probleme lassen sich die Eigenschaften der beiden Tools in den Katalog forensischer Werkzeuge übertragen und dort aufnehmen. Da es sich bei einem forensischen Backup um ein optimiertes, reguläres Backup handeln soll, wird im Regelfall nach den Anforderungen der Backup-Software die entsprechende Lösung gesucht. In den hier geforderten Funktionalitäten wird es kaum Unterschiede zwischen den verschiedenen Anbietern geben, da zum einen die verwendeten Mechanismen sich ähneln (VADP), zum anderen die Anforderungen an das Logging keine Außergewöhnlichen sind.

**[L32 - L35] Werkzeugeigenschaften: Allgemeine Anforderung forensisches Backup**

- Es soll geprüft werden, ob das forensische Backup durch dessen Aufnahme in den Katalog der forensischen Werkzeuge einen Mehrwert bringt.
- Es soll eine Nachvollziehbarkeit des eingesetzten Programmes und der verwendeten Jobkonfiguration existieren.
- Fehler beim Erstellen eines forensischen Backups sollen erkannt und sichtbar gemacht werden.
- Das forensische Backupsystem soll die Möglichkeit besitzen, Sicherungen in ein für forensische Analysetools verwertbares Format wiederherzustellen

## 4.4 Thema 3: Eigenschaften des Systems

Sowohl die IT-Systeme als auch darauf laufende Applikationen und deren sicherer Betrieb werden in dieser Arbeit als gegeben angenommen. Mechanismen, die dies sicherstellen, sind unter anderem in den Bausteinen des Grundsatzkompodiums „APP: Anwendungen“ und „SYS: IT-Systeme“ beschrieben und somit keine spezifischen Anforderungen für ein forensisches Backup.

## 4.5 Thema 4: Vollständigkeit der Datensicherung

**[L\_14 ]** Formuliert ist dieser Punkt aus einem Post-Mortem-Blickwinkel, mit dem Ziel: Es sollen alle Komponenten gesichert werden, die möglicherweise betroffen gewesen sind. Da ein forensisches Backup Teil der strategischen Vorbereitung ist, sollen von vornherein alle Komponenten berücksichtigt werden. Dies deckt sich mit L\_02 als Anforderung eines regulären Backups. Es besagt, dass für jedes IT-System festgelegt werden soll, welche Daten gesichert werden sollen. Dies impliziert, dass jedes System berücksichtigt werden soll. **[L\_16]** Sollen die Systeme ganzheitlich auswertbar sein, ist auch der flüchtige Arbeitsspeicher zu betrachten. Informationen wie in L\_31 (lfd. Prozesse, angemeldete User, bestehende Netzwerkverbindungen) gefordert, lassen sich aus ihm extrahieren<sup>[55]</sup>. Auch „file-less“ Attacken können so erkannt werden. Arbeitsspeicher zu sichern, steht in der Abwägung gegen den erhöhten Aufwand und den Speicherbedarf.

### **Problembeschreibung:**

Klassische Post-Mortem-Analysen erlauben nur eingeschränkten Zugriff auf flüchtigen Speicher. Sie beschränken sich auf physische Verfahren zum Auslesen des Arbeitsspeichers oder Auslagerungen in Swap-Partitionen. Es soll untersucht werden, ob ein forensisches Backup in der Lage sein könnte, Arbeitsspeicher als Ressource zur späteren Analyse zu sichern.



## 4.6 Thema 5: Dokumentation

Aufgabe der Dokumentation ist die Beschreibung der eingesetzten Methode und der gesicherten Systeme, überdies die Nachvollziehbarkeit der einzelnen ausgeführten Schritte (vgl. L\_17). Die eingesetzte Methode und die Eigenschaften der gesicherten Maschinen sind dem Backup-Konzept [L\_08] zu entnehmen. Regelbackups werden regelmäßig vordefiniert ausgeführt. Die einzelnen Schritte sind durch die Automatisierung deterministisch vorbestimmt und einheitlich über alle Backups der gleichen Konfiguration beschreibbar. Durch die Konfiguration wird bestimmt, welche Schritte ausgeführt werden. Geführte Logs belegen deren Terminierungsstatus. Somit kann die Kombination aus Konfigurations- und Logdateien eine Ausführung schrittweise belegen, sofern sie nachweisbar verfälschungsfrei vorgehalten wurden. Dies kann im einfachen Fall über ein versioniertes Konfigurationsmanagement (zum Beispiel: OPS.1.1.7.A14) und den Einsatz von Logservern (zum Beispiel: OPS.1.1.5.A6) erfolgen. Der hinreichende Detailgrad der geschriebenen Logs wird im Abschnitt 4.6 Thema 6: „Nachvollziehbarkeit“ behandelt. Somit sind die Anforderungen an die Dokumentation für ein forensisches Backup durch die konzeptionellen Anforderung L\_17 eines regulären Backups zusammen mit den Standardanforderungen des Systemmanagements (OPS) erfüllt.

|                                                                                                              |
|--------------------------------------------------------------------------------------------------------------|
| <b>Dokumentation:</b> Allgemeine Anforderung forensisches Backup                                             |
| Keine gesonderten Anforderungen nötig, sofern Konfigurationsmanagement und zentrales Logging umgesetzt sind. |

## 4.7 Thema 6: Nachvollziehbarkeit

Bei der Nachvollziehbarkeit geht es um den Beleg, dass Methoden und Schritte ausgeführt wurden, wie sie im Rahmen der Dokumentation festgelegt sind. Dies eint die zugeordneten Anforderungen [L\_17, L\_18, L\_28, L29]. Als Teil der Dokumentation wurden reguläre Backups bereits als deterministisch beschrieben. Die Eigenschaften einer Sicherung sind im Vorfeld festgelegt. Wie bereits im Thema 2 verwendet, wird die praktische Gleichheit zwischen der Konfiguration und den Aufrufparametern angenommen. L\_17 verlangt die [nachweisbare] Integrität dieser Aufrufparameter. Hier kann die Revisionssicherheit eines Konfigurationsmanagements (CMS) genutzt werden. Mittels CMS kann ein Konfigurationsstand zu einer bestimmten Zeit einer bestimmten Sicherung nachgewiesen werden, sofern eine Konfiguration mit ihr verknüpft werden kann. Dies sind übliche Log-Informationen und bedürfen normalerweise keiner gesonderten Konfiguration. Die ebenfalls von L\_17 geforderte Authentizität wird in agentenlosen Architekturen, wie Ansible, über SSH-Keys oder bei agentenbasierten Systemen, wie Puppet, über ein Client-Zertifikat gewährleistet. Geht aus den Logdaten hervor, mit welcher Konfiguration der Job aufgerufen wurde, kann rückwirkend nachvollzogen und belegt werden, mit welcher Pa-

rametrisierung eine konkrete Sicherung ausgeführt wurde.

Aus den Anforderungen L\_17 und L\_28 ergibt sich zudem die Notwendigkeit Rückgaben des Programms sicher zu verwahren. Dies gelte für Konsolenausgaben und Prüfsummen. Ziel ist es, beide Arten der Rückgabe in das zentrale Logmanagement zu speisen und dort zu verwahren. Logdaten können bei unbeaufsichtigt ablaufenden Aufgaben als Konsolenausgaben interpretiert werden. Entsprechend wäre dies die originäre Aufgabe eines Logservers und mit dem Baustein Systemmanagement bereits umgesetzt. Prüfsummen, sofern sie außerhalb der Werkzeuge erzeugt werden, sind so auch zum Beispiel über den Befehl „logger“ in das Syslog zu übertragen.

L\_29, die Bezeugung des Vorgehens und die Beglaubigung der Prüfsumme können bei unbeaufsichtigt ausgeführten Jobs lediglich indirekt geschehen, zum Beispiel über die Bezeugung der Erfassungsmethode, der Konfiguration und des Vorgehens der Prüfsummenerzeugung. Über das vorhandene Log kann dann auf das konkrete Vorgehen geschlossen werden.

|                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[L_37, L_38] Nachvollziehbarkeit: Allgemeine Anforderung forensisches Backup</b>                                                                                                                                                                                                                                  |
| <ul style="list-style-type: none"><li>- Es soll sichergestellt werden, dass die erstellten Logdateien über einen Job, eine eindeutige Zuordnung der verwendeten Konfiguration zulassen.</li><li>- Die Prüfsumme von gesicherten Dateien und Logdaten soll in das zentrale Logmanagement übertragen werden.</li></ul> |



## 4.8 Thema 7: Schutz der Datenquelle

Zentrale Forderung der forensischen Sicherung ist der Integritätserhalt der Quelle. Sie soll nachgewiesen werden [L\_19] und über Schreibblocker sichergestellt werden [L\_20]. Letzteres wurde in der Arbeit<sup>[26]</sup> untersucht. In ihr wird gezeigt, dass die beiden untersuchten Tools, Encase und das Forensic Toolkit, in der Lage sind, direkt aus erstellten Snapshots forensische Abbilder zu erstellen. Die Autoren erkennen an, dass für physische Umgebungen Schreibblocker benötigt werden, und untersuchten das Verhalten von Festplattendateien beim Umwandeln der .vmdk-Dateien in das auswertbare RAW-Format. Im Labor glichen sie hierfür die errechneten Prüfsummen aus den beiden Analysewerkzeugen Encase und dem Forensic Toolkit einander ab. Sie waren identisch, woraus geschlossen wurde, dass es zu keiner Veränderung des Inhalts kam. Daraus wurde wiederum gefolgert, dass vmWare Festplatten sicher in Festplattenabbilder des raw/dd Formats umgewandelt werden können, auch ohne Schreibblocker. ("Therefore, we conclude that VM hard disk files can be safely converted to raw/dd images using either tool without relying on a write block device.")<sup>[26]</sup> Problematisch ist der Integritätsnachweis beim Erstellen eines Backups über Snapshotmechanismen, wie in der Backup-Anforderung L\_03 geprüft werden soll.

**Problembeschreibung:**

Während eines Snapshots wird die virtuelle Maschine üblicherweise „quiesced“. Dies ist mit der Erhebungsmethode verbunden und dient dem Schließen offener Schreibvorgänge zur Prävention von Dateninkonsistenz. Dafür werden kurzzeitig Prozesse angehalten, das Dateisystem eingefroren und Speichercaches synchronisiert. Die „Quiescence“ wird durch den Hypervisor in die Gastweiterungen der VM induziert. In der Arbeit von Juan Carlos Flores Cruz „Digital Forensics on a Virtual Machine“ wurden durch das Anlegen eines Snapshots Änderungen in der Windows Registry belegt, womit die eingesetzte Methode zur Datenakquise nicht mehr neutral gegenüber der Quelle ist <sup>[53]</sup>. Daraus ergibt sich, dass gegen die forensische Anforderung [L\_20] während eines forensischen Backups verstoßen werden wird. Snapshotverfahren sind nicht rückwirkungsfrei gegenüber der Datenquelle.

|                                                                                  |
|----------------------------------------------------------------------------------|
| <b>[L_41] Schutz der Datenquelle: Allgemeine Anforderung forensisches Backup</b> |
|----------------------------------------------------------------------------------|

- |                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>- Eine Änderung der Original-Quelle wird im Rahmen der Snapshoterstellung akzeptiert.</li> </ul> |
|-----------------------------------------------------------------------------------------------------------------------------------------|

## 4.9 Thema 8: Datenhaltung

Unter [L\_21] wird gefordert, dass forensische Sicherungen auf sicher gelöschten Datenträgern gespeichert werden. Dies ist für den Analyse-Schritt wichtig, um Fehlinterpretationen zu vermeiden [FR\_01\_Anf\_20]. Da auf den Backup-Medien keine forensischen Analysen ausgeführt werden, ist dieser Punkt für das forensische Backup nicht relevant. Analysen werden erst auf Medien nach der Initialisierung der Daten in ein forensisches Analysesystem vorgenommen. Zuvor werden diese aus den Backup-Dateien, auf Fileebene, wiederhergestellt. Somit kommt es auch bei nicht sicher gelöschten Backupmedien nicht zu Kontamination der wiederhergestellten Daten. Anforderungen einer redundanten Datenhaltung [L\_25] und der verschlüsselte Datenhaltung [L\_26] sind Anforderungen, die sich in den regulären Backups widerfinden [L\_05; L\_06]. Als Löschrufen für forensische Sicherungen sollen die Retention der regulären Backups Anwendung finden. Die Notwendigkeit derer Definition ergibt sich hieraus [L\_24].

|                                                                        |
|------------------------------------------------------------------------|
| <b>[L_39] Datenhaltung: Allgemeine Anforderung forensisches Backup</b> |
|------------------------------------------------------------------------|

- |                                                                                                                                        |
|----------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>- Es sollen Fristen zum sicheren Löschen von forensischen Backups festgelegt werden.</li> </ul> |
|----------------------------------------------------------------------------------------------------------------------------------------|

## 4.10 Thema 9: Chain of Custody

Die „Chain of Custody“ bezieht sich auf die lückenlose Dokumentation und den Nachweis der Verantwortlichkeit für ein Beweisstück während seiner Aufbewahrung und Handhabung im Verlauf einer forensischen Untersuchung. Dieser Prozess stellt sicher, dass Beweise adäquat geschützt und manipulationsfrei bleiben. Konkret fordert [L\_30] Nachvollziehbarkeit der Verwahrung, Einsichtnahme und Quelle des Beweises. Die Quelle lässt sich mittels des öffentlichen Schlüssels belegen, der Teil der Authentizitätsprüfung zwischen Hypervisor und Backupsystem ist. Dies ist bei den untersuchten Lösungen Standard-Konfiguration. Verwahrung und Einsichtnahme können sich hier nur auf die Dateien des forensischen Backups beziehen. L\_06 als Anforderung regulärer Backups fordert bereits Zugangsbeschränkungen und Datensicherheit für die Backup-Dateien. Für das forensische Backup müssten diese um das Zugriffslog ergänzt werden. Die Verwahrung der Dateien wird über Konfigurationen und die physischen Lokation definiert. Schutzmechanismen setzen an diesen beiden Eigenschaften an.

|                                                                                                                                                                              |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[L_40] Chain of Custody: Allgemeine Anforderung forensisches Backup</b>                                                                                                   |
| <ul style="list-style-type: none"><li>- Für die Dateien des forensischen Backups soll der Zugriff und die physische Aufbewahrung der Dateien nachvollziehbar sein.</li></ul> |

## 5 Bewertung und Diskussion

Diese Anforderungen des vorherigen Kapitels sollen hier noch einmal aufgelistet und Limitierungen herausgestellt werden. Anschließend wird untersucht, in welchem Maß das forensische Backup das reguläre Backup im Hinblick auf die forensische Verwertbarkeit verbessert. Mit dem Vergleich der beiden Bewertungen soll diese Arbeit schließen.

### 5.1 Eigenschaften des forensischen Backups

Im Folgenden sind die herausgearbeiteten Ergänzungen zum Regelbackup aufgeführt.

| ID   | Last                                                                                                                                                                                                                                                                                                                                 | Kapitel |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| L_31 | Es soll ein Verfahren etabliert werden, das mittels Kryptografie die Gleichheit zwischen gesicherten Systemen zum Zeitpunkt des Backups und der Wiederherstellung belegen kann. Andernfalls muss akzeptiert werden, dass Integrität nur für die Backup-Dateien, nicht aber gegenüber den Original-Dateien, nachgewiesen werden kann. | 4.2     |
| L_32 | Es soll eine Nachvollziehbarkeit des eingesetzten Programmes und der verwendeten Jobkonfiguration existieren.                                                                                                                                                                                                                        | 4.3     |
| L_33 | Es soll geprüft werden, ob das forensische Backup durch dessen Aufnahme in den Katalog der forensischen Werkzeuge einen Mehrwert bringt.                                                                                                                                                                                             | 4.3     |
| L_34 | Fehler beim Erstellen eines forensischen Backups sollen erkannt und sichtbar gemacht werden.                                                                                                                                                                                                                                         | 4.3     |
| L_35 | Das forensische Backupsystem soll die Möglichkeit besitzen, Sicherungen in ein für forensische Analysetools verwertbares Format wiederherzustellen.                                                                                                                                                                                  | 4.3     |
| L_36 | Es soll im Vorfeld festgelegt werden, welche IT-Systeme und deren Datenträger mit einem forensischen Backup gesichert werden sollen. Es soll geprüft werden, ob Sicherungen von Arbeitsspeicherinhalten als Teil der strategischen Vorbereitung einfließen sollen.                                                                   | 4.5     |
| L_37 | Es soll sichergestellt werden, dass die erstellten Logdateien über einen Job eine eindeutige Zuordnung der verwendeten Konfiguration zulassen.                                                                                                                                                                                       | 4.7     |
| L_38 | Die Prüfsumme von gesicherten Dateien und Logdaten soll in das zentrale Logmanagement übertragen werden.                                                                                                                                                                                                                             | 4.7     |
| L_39 | Es sollen Fristen zum sicheren Löschen von forensischen Backups festgelegt werden.                                                                                                                                                                                                                                                   | 4.9     |
| L_40 | Für die Dateien des forensischen Backups soll der Zugriff und die physische Aufbewahrung der Dateien nachvollziehbar sein.                                                                                                                                                                                                           | 4.10    |
| L_41 | Eine Änderung der Original-Quelle wird im Rahmen der Snapshoterstellung akzeptiert.                                                                                                                                                                                                                                                  | 4.8     |

**Tabelle 7: Eigenschaften forensisches Backup**

## 5.2 Limitierungen des forensischen Backups

Mindestens in der vorherig untersuchten Backup-Methode mit der Sicherung über die Snapshotverfahren sind grundlegende Einschränkungen bezüglich der **Integritätsanforderungen** gegenüber einer forensischen Sicherung hinzunehmen. Es ist zum einen kein Nachweis über die Unveränderlichkeit zwischen Quelle und Ziel möglich. Wird von der Festplatten-Datei als Quelle des Beweises ausgegangen, kann für diese nicht die Integrität nachgewiesen werden. Festplattendateien in virtuellen Umgebungen sind hochvolatil. Sie lassen im laufenden Betrieb, in der untersuchten Methode, kein Erzeugen einer Prüfsumme zu. Dies umso weniger, als dass der Zeitpunkt mit der Erstellung des Snapshots für die Sicherung zusammenfallen müsste. Diskutabel wäre die Definition des "Beweisstücks". Wenn nicht die Festplattendatei, sondern das forensische Backup als Beweisstück betrachtet werden würde, so wäre die Integrität nachweisbar. Dies entrückt allerdings den Beweis von der Quelle. Dieser Gedanke wird beim Abgleich mit den juristischen Anforderungen noch einmal aufgenommen.

Die zweite große, ungelöste Schwäche ist die **Veränderung der Originaldatei bei Datenerhebung**. Es werden bei der Erstellung eines Snapshots Log-Daten innerhalb des Systems erzeugt und dieses für den Zeitpunkt der Snapshoterstellung angehalten. So erfährt zum einen der Festplatteninhalt eine Veränderung und das Verhalten der Maschine wird beeinflusst. Diese Eigenschaften sind der Sicherungsmethode innewohnend. Hier träte ein Zielkonflikt zutage, würden Anforderungen aus der forensischen Sicherung gleichgewichtet mit den betrieblichen Anforderungen, aus denen sich die Eigenschaften eines regulären Backups ergeben. Für diese Arbeit lässt sich der Konflikt zugunsten des regulären Backups lösen, da untersucht wird, inwiefern sich reguläre Backups verbessern lassen. Die Methode ist in dem beschriebenen Szenario sowohl durch den Hersteller vmWare als auch durch die Hersteller der Sicherungssoftware, welche die API nutzen, vorbestimmt. Es müssen so Rückwirkungen auf das zu sichernde System mindestens innerhalb des Szenarios akzeptiert und bei einer forensischen Analyse berücksichtigt werden. Bei einer Gewichtung stärker zugunsten der forensischen Sicherung könnte diese Limitierung ein Ausschlusskriterium der Methode sein. Konsequenz wäre diese Eigenschaften bereits in den Auswahlprozess einfließen zu lassen, da eine spätere Anpassung, nach Festlegung auf Hersteller und damit auf die Methode, nicht trivial möglich ist.

## 5.3 Bewertung des forensischen Backups

Da die Anforderungen eines forensischen Backups sich direkt aus den Anforderungen einer forensischen Sicherung ableiten, ist eine Verbesserung trivial anzunehmen. Diese wird in der folgenden Tabelle quantifiziert. Verwendet wird dieselbe Metrik, wie sie im Kapitel 3 zur Bewertung eines regulären Backups herangezogen wurde. Diese wird nun gegen die Eigenschaften eines forensischen Backups gemessen.

In der folgenden Tabelle wird die forensische Last gegen ein forensisches Backup verglichen. Die mittlere Spalte entspricht dem Gewicht der jeweiligen Anforderung.

| ID   | forensische Last                                                                                                                                   | x | forensisches Backup Last                                                                                                                                                                                                                                                        | ID           |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| L_11 | Analyseauslösendes Event muss dokumentiert sein                                                                                                    | 1 | <gegeben durch Systemanforderung des zentralen Loggings>                                                                                                                                                                                                                        |              |
| L_12 | Forensische Werkzeuge sollen in einem Katalog begründet vorausgewählt und verfügbar sein.                                                          | 4 | Es soll ein Datensicherungskonzept erstellt werden, das mindestens beinhaltet:<br>[...]<br>• welche Hard- und Software eingesetzt wird.<br>Das Backup soll [...] nach dem Datensicherungskonzept durchgeführt werden.                                                           | L_01<br>L_08 |
| L_0a | Forensische Werkzeuge sollen eine Fehlererkennung implementiert haben, die Ungenauigkeit, Unvollständigkeit oder Missinterpretation sichtbar macht | 4 | Es soll eine Nachvollziehbarkeit des eingesetzten Programmes und der verwendeten Jobkonfiguration existieren.<br><br>Fehler beim Erstellen eines forensischen Backups sollen erkannt und sichtbar gemacht werden.                                                               | L_32<br>L_34 |
| L_13 | Bei Werkzeugen muss sichergestellt sein, dass diese nicht manipuliert wurden                                                                       | 3 | <gegeben durch deren sicheren Betrieb, konkret APP.6><br>vgl. Thema 3: Eigenschaften des Systems                                                                                                                                                                                |              |
| L_14 | Die Datensammlung soll auf allen potenziell betroffenen Komponenten durchgeführt werden, ggf. auch außerhalb des phys. Zugriffs                    | 2 | Es soll ein Datensicherungskonzept erstellt werden, das mindestens beinhaltet:<br>[...]<br>• welche IT-Systeme und welche darauf befindlichen Daten durch welche Datensicherung gesichert werden,<br>Das Backup soll [...] nach dem Datensicherungskonzept durchgeführt werden. | L_01<br>L_08 |
| L_15 | Abänderungen der forensischen Sicherung gegenüber der Datenquelle sollen konkret nachvollziehbar sein.                                             | 1 | Fehler beim Erstellen eines Backups sollen erkannt und sichtbar gemacht werden.                                                                                                                                                                                                 | L_34         |
| L_16 | Forensische Sicherungen sollen priorisiert nach Wert, Flüchtigkeit und Aufwand erfolgen                                                            | 2 | Es soll im Vorfeld festgelegt werden, welche IT-Systeme und deren Datenträger mit einem forensischen Backup [...]                                                                                                                                                               | L_36         |
| L_17 | Es sollen die eingesetzte Methode und die einzelnen Schritte zur Datengewinnung dokumentiert werden, eben-                                         | 3 | Es soll ein Verfahren geben, das für jedes IT-System bestimmt, welche Daten wie gesichert werden. Es soll mindestens                                                                                                                                                            | L_02         |

|      |                                                                                                                                                    |   |                                                                                                                                                                                                                     |      |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|
|      | so wie Eigenschaften des gesicherten Systems.                                                                                                      |   | Kritikalität der Daten und Einflussfaktoren berücksichtigen                                                                                                                                                         |      |
| L_18 | Aufrufparameter und Rückgaben der verwendeten Tools sollten integritäts- und authentizitätsgeschützt gespeichert werden.                           | 1 | Die Prüfsumme von gesicherten Dateien und Logdaten soll in das zentrale Logmanagement übertragen werden.                                                                                                            | L_38 |
| L_19 | Die originale Datenquelle soll durch den Prozess der forensischen Sicherung nachweisbar nicht geändert worden sein.                                | 2 | <Umgebungsspezifisch, Snapshot ungeeignet>                                                                                                                                                                          |      |
| L_20 | Es sollen Schreibblocker eingesetzt werden, um die Integrität der originalen Datenquelle zu schützen                                               | 1 | <Umgebungsspezifisch, Snapshot ungeeignet>                                                                                                                                                                          |      |
| L_21 | Eine forensische Sicherung soll als physische Kopie des Datenträgers erstellt werden und diesen vollständig, inkl. reservierter Bereiche, abbilden | 3 | Es soll geprüft werden, ob Abbilder der gesamten Festplatte(n) gesichert werden können.                                                                                                                             | L_37 |
| L_22 | Über ein kryptographisches Verfahren soll nach der forensischen Sicherung das exakte Duplikat gegenüber dem Original nachgewiesen werden.          | 4 | <mit untersuchten Verfahren nicht möglich>                                                                                                                                                                          | L_31 |
| L_23 | Forensische Sicherungen sollen auf zuverlässig gelöschten Medien gespeichert werden.                                                               | 2 | <mit untersuchten Verfahren nicht möglich bzw. außerhalb der Kontrolle>                                                                                                                                             |      |
| L_24 | Forensische Sicherungen sollen nach einer zuvor festgelegten Zeit sicher gelöscht werden.                                                          | 2 | Es sollen Fristen zum sicheren Löschen von forensischen Backups festgelegt werden.                                                                                                                                  | L_39 |
| L_25 | Forensische Sicherungen sollen in mehreren Kopien an unterschiedlichen Orten vorgehalten werden.                                                   | 2 | Eine Kopie der Backupdaten soll an einer Offsite-Location gehalten werden                                                                                                                                           | L_05 |
| L_26 | Ruhende forensische Sicherungen sollen verschlüsselt werden.                                                                                       | 2 | Sicherungsdateien sollen kryptografisch gesichert vor Manipulation, unbefugter Offenlegung, geschützt vor unberechtigtem Zugriff auf Medien in einer zugangsgeschützten, umweltschonenden Umgebung gehalten werden. | L_06 |
| L_27 | Foren. Sicherungen sollen im rechtlich/regulatorischen Rahmen erstellt werden                                                                      | 1 | <entfallen>                                                                                                                                                                                                         |      |

|        |                                                                                                                                                      |    |                                                                                                                                       |              |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------|----|---------------------------------------------------------------------------------------------------------------------------------------|--------------|
| L_28   | Es soll sichergestellt sein, dass die [schriftlich] dokumentierten Prüfsummen nicht verändert werden können                                          | 1  | Die Prüfsumme von gesicherten Dateien und Logdaten soll in das zentrale Logmanagement übertragen werden.                              | L_38         |
| L_29   | Es soll ein Zeuge bestätigen, wie bei der forensischen Sicherung vorgegangen wurde, und die Prüfsummen beglaubigen                                   | 2  | <Nachweis anhand der Jobdefinition>                                                                                                   |              |
| L_30   | Im Umgang mit den Beweismitteln soll eine Chain of Custody gewahrt bleiben. Diese umfasst im Besonderen Verwahrung, Einsichtnahme, Quelle und Umgang | 4  | Es soll für Backupmedien und Backupdateien die physische Verortung, ein Namensschema, Retention und Transportmethode festgelegt sein. | L_04<br>L_36 |
| -      | Keine forensische Entsprechung                                                                                                                       | 0  | Das Backup soll in regelmäßiger Frequenz und zu festgelegten Zeitpunkten nach dem Datensicherungskonzept durchgeführt werden.         | L_01         |
| -      | Keine forensische Entsprechung                                                                                                                       | 0  | Bei Löschung von Backups soll ein Vieraugenprinzip herrschen.                                                                         | L_07         |
| -      | Keine forensische Entsprechung                                                                                                                       | 0  | In regelmäßigen Tests soll die Funktionalität der Sicherung und der Wiederherstellung in angemessener Zeit getestet werden.           | L_09         |
| Summe: |                                                                                                                                                      | 37 | /47 *100 =<br><b>Forensischer Wert = 72</b>                                                                                           |              |

Tabelle 8: Bewertung forensisches Backup

Legende:

|                              |                               |               |
|------------------------------|-------------------------------|---------------|
| Erfüllt, direkte Anforderung | Erfüllt, abgeleitet Umsetzung | Nicht erfüllt |
|------------------------------|-------------------------------|---------------|

So erhöht sich der forensische Wert eines Regelbackups um ungefähr die Hälfte gegenüber einem regulären Backup. Die zuvor erwähnten Schwächen der Metrik bleiben erhalten und somit vergleichbar. Durch den genaueren Blick und die Analyse aus dem Kapitel zuvor wurden nun allerdings auch erfüllte Eigenschaften aus anderen Anforderungen hineingezogen, da sie konkret adressiert werden konnten.

## 5.4 Einordnung in die gerichtliche Verwertbarkeit

Im Kapitel 2 wurden Eigenschaften eines Beweises herausgestellt. Die folgende, verkürzte Liste stellt lediglich dem Beweisstück inhärente Eigenschaften der gerichtlichen Verwertbarkeit dar. Sie sollen anhand einer forensischen Sicherung andiskutiert werden. Dafür wird von der Festplattendatei der virtuellen Maschine als Quelle des Beweisstücks ausgegangen. Alle Anforderungen sind in der forensischen Sicherung aufgegangen, ohne sie explizit hinzugefügt zu haben.

| ID    | Eigenschaft                                                                                                               | Attribut     | ID_for. Backup     |
|-------|---------------------------------------------------------------------------------------------------------------------------|--------------|--------------------|
| GR_02 | Herkunft und Verbleib müssen lückenlos nachvollziehbar sein.                                                              | Beweismittel | L_40               |
| GR_03 | Authentizität/Integrität des Beweismittels muss nachgewiesen werden können                                                | Beweismittel | L_31               |
| GR_05 | Vollständigkeit des erfassten Beweismittels muss gegeben sein                                                             | Beweismittel | L_36               |
| GR_07 | Rechtl. Zulässigkeit des Beweismittels muss gegeben sein. Dies gilt sowohl für die Erhebung als auch für die Verarbeitung | Beweismittel | <nicht betrachtet> |

**Tabelle 9: Einordnung der gerichtlichen Verwertbarkeit**

Die **rechtliche Zulässigkeit** wurde in dieser Arbeit nicht betrachtet und muss den Juristen überlassen sein. Während sich die **Authentizität** von einem Server über asymmetrische Schlüsselpaare oder Secrets nachweisen lässt, stellt der Nachweis der **Integrität** des Beweisstückes in der untersuchten Methode ein ungelöstes Problem dar. Wie in Kapitel 2 ausgeführt, wird hierüber der Beweiswert erhöht und das Gericht stellt die vollständige und erschöpfende Beweiswürdigung sicher. Beides kann für die Festplattendatei als Beweisstück nicht angenommen werden. Sie wurde verändert und die Integrität des wiederhergestellten Systems kann nicht gegen die ursprüngliche Datei nachgewiesen werden. Würde nicht die Festplatte, sondern die Backupdatei als Beweisstück verwendet, könnte die Lücke geschlossen werden, da Integritätsprüfungen durch die Backup-Tools durchgeführt werden. Problematisch ist bei dieser Herangehensweise, dass nicht das Backup, sondern die hieraus wiederhergestellte Festplatte das eigentliche Analyseziel ist. Unter Berücksichtigung des sachnäheren Beweises könnte allerdings auch diskutiert werden, inwiefern ein forensisches Backup zwar zweifelsfrei keine forensische Sicherung ersetzt, es aber rückblickend das sachnächste Beweisstück sein kann und so doch eine Würdigung erfährt. Unter diesem Gesichtspunkt könnte eine Verwertung zwar möglich, aber in der technischen Betrachtung nicht besser als die eines regulären Backups sein. Organisatorisch kann im Rahmen der strategischen Vorbereitung sichergestellt werden, dass die **Herkunft und Verbleib** des potenziellen Beweises schon vor dessen Qualifizierung zum Beweisstück sichergestellt ist. Dies kann über Zugriffsprotokolle und die sichere Verwahrung der Backup-Dateien und –Medien erreicht werden. Dies ist üblicherweise im Rahmen eines ISMS umgesetzt, müsste gegebenenfalls allerdings auf Lückenlosigkeit überprüft werden. Es muss plausibel die Authentizität der gesicherten Maschine nachgewiesen werden, der Verbleib der Backup-Daten und Medien und Zugriffe darauf. Mit der

Wiederherstellung der Maschine und dem Authentizitätsnachweis der übergebenen VM endet die Nachweiskette für die forensischen Backups. Die Bewertung der **Vollständigkeit** wird erst durch das Gericht vollzogen. Die identifizierung von potenziellen Beweisen kann im Vorfeld, im Rahmen der strategischen Vorbereitung stattfinden. Somit können die Qualifizierung zum Beweisstück und die Bewertung der Vollständigkeit unterstützt werden. Das forensische Backup stellt so eine zusätzliche Quelle.

## 6 Fazit

### 6.1 Implikationen

Backups als mögliche Quelle für forensische Analysen zu verwenden, liegt auf der Hand und wird sicherlich auch praktiziert. Der Mehrwert dieser Arbeit besteht darin, Eigenschaften von Backups als Teil der strategischen Vorbereitung zu sehen und diese formuliert zu haben. Mit den herausgearbeiteten Anforderungen ist in **Tabelle 7 Eigenschaften forensisches Backup** ein ausformuliertes Control-Set entstanden, welches in seinem Charakter als Lasten für eine mögliche Umsetzung verwendet werden kann. Es umfasst sowohl organisatorische Anforderungen wie das Festlegen der Zielsysteme (L\_36) oder das Akzeptieren von konkreten Limitierungen (L\_31),(L\_41), aber in der Hauptsache werden technische Anforderungen in der Umsetzung (zB.: L\_37,L\_32), der Datenhaltung (L\_39, L\_40) oder der eingesetzten Software (L\_34, L\_38) betrachtet. Die herausgestellten Anforderungen eines forensischen Backups können Impuls für regulatorische Organe, um Anforderungen an regelmäßige Sicherungen interdisziplinär zu denken, sein. Zudem können IT-Abteilungen den Rahmen ihrer IT-Sicherheitsstrategie hieraus weiten. Auch Hersteller von Virtualisierungs- und Backup-Lösungen sollen sich angeregt fühlen. Der technische Mehraufwand eine Prüfsumme bereits auf dem Hypervisor zu bilden und sie per API zur Verfügung zu stellen dürfte gering sein. Es könnte jedoch die Zuverlässigkeit der Backups erhöhen und das Anwendungsspektrum wie beschrieben erweitern. Ebenso wie die Option des Abziehens von Arbeitsspeicher Sicherungen. Welche Fileless-Attacken nachvollziehbar machen könnten oder Systemzustände aus der Vergangenheit verrieteten.

### 6.2 Ausblick

Aus den am Anfang ausgeklammerten Limitierungen ergeben sich mögliche Vertiefungen, welche die Arbeit explizit offenhält. Zudem bietet sie die Möglichkeit die technische Umsetzung der Anforderungen zu sondieren oder mit den Herstellern an der Umsetzung der Schnittstellen zu arbeiten. Ein offenes Thema ist zudem, die Auswirkung von Snapshots auf die zu sichernde Maschine zu untersuchen und Möglichkeiten zu finden, die Rückwirkungen zu minimieren oder diese zu beschreiben. Das Thema des Integritätsnachweises einer Maschine ohne äußeren Zugriff auf die Festplatte scheint mit zunehmender Cloudnutzung ein notwendiges Forschungsgebiet, welches hier auch die Abhängigkeit von der Anpassung der Herstellersoftware lösen würde. Als letzten Punkt war es erstaunlich, dass keine Möglichkeit zur Bestimmung der Güte einer forensischen Sicherung gefunden wurde. Dies wäre jedoch nicht nur im Kontext dieser Arbeit hilfreich gewesen, es würde auch zum Beispiel Gerichten bei der Beurteilung eines vorliegenden Datums helfen.

## 6.3 Fazit

In der vorliegenden Arbeit wurde untersucht, inwiefern es möglich ist, durch Anpassungen regulärer Backups die gesicherten virtuellen Maschinen sowohl in ihrem Forensischen Wert als auch in ihrer gerichtlichen Verwertbarkeit zu erhöhen.

Dafür wurde im ersten Schritt in einer Literatur-Recherche nach wissenschaftlichen Arbeiten gesucht, welche die Verbreitung von forensischen Frameworks bereits untersuchten. Hiermit wurden zwei Ziele verfolgt: zum einen sollten möglichst breit akzeptierte Frameworks die Anforderungsgrundlage für diese Arbeit bilden und zum anderen sollte so gängige Praxis eingefangen werden. Die identifizierten Arbeiten ließen jedoch wenig Rückschlüsse auf die Verbreitung oder Akzeptanz der Frameworks zu. Vielmehr waren sie häufig vergleichender Natur. Es wurde daraufhin, aufgrund ihrer Autorität, auf Frameworks und Publikationen der nationalen Agenturen BSI und NIST zurückgegriffen. Aus ihnen wurden Anforderungen für die forensische Sicherung und dem regulären Backup aufgenommen und jeweils zusammengeführt. Zur Identifizierung potenzieller Probleme einer gerichtlichen Auswertung wurde sich auf die Habilitation von Christian Rückert "Digitale Daten als Beweismittel im Strafverfahren" gestützt. Die im zweiten Kapitel ermittelte Deckungsquote bildet einen Indikator für die Konvergenz der Anforderungen zwischen den drei Themengebieten (forensische Sicherung, reguläres Backup und gerichtliche Verwertbarkeit). Es zeigte sich große Ähnlichkeit zwischen den Anforderungen der forensischen Sicherung und den regulären Backups (Deckungsquote 73%), methodisch bedingt allerdings weniger gegenüber der gerichtlichen Verwertbarkeit (Deckungsquote 25%). Die Metrik zur Bestimmung des Forensischen Wertes eines Backups wurde für diese Arbeit anhand der Häufigkeit der Erwähnung einer konkreten Anforderung innerhalb der untersuchten Anforderungsdokumente definiert. Es stellte sich jedoch heraus, dass diese naheliegende Bewertung nicht die Praxistauglichkeit abbildet. So werden essenzielle Anforderungen wie Integritätsschutz nicht hinreichend stark gewichtet. Auch oft vorhandene, aber nicht explizit geforderte Eigenschaften bleiben unberücksichtigt. In dem Bewusstsein, dass die Metrik mehr die Anforderungen als das Backup bewertet, ist sie für den relativen Vergleich innerhalb der Arbeit dennoch hinreichend. Auf Ihrer Grundlage wurde ein reguläres Backup bewertet. Anschließend wurde untersucht, inwiefern die Anforderungen einer forensischen Sicherung in das reguläre Backup einer Beispielhaften Umgebung übertragen werden können. Aus diesen Erkenntnissen wurden wiederum Anforderungen formuliert, die unter Berücksichtigung der praktischen Umsetzbarkeit und ergänzend zum regulären Backup die Eigenschaften eines forensischen Backups beschreiben. Es entstand so eine Liste mit insgesamt elf zusätzlichen Anforderungen. Abschließend wurde der forensische Wert des forensischen Backups ermittelt und mit dem regulären Backup verglichen. Durch die zusätzlichen Anforderungen konnte das forensische Backup gegenüber dem regulären Backup seinen Forensischen Wert deutlich erhöhen (23 zu 37). Aus den Anforderungen des forensischen Backups wurden Eigenschaften eines Backups antizipiert, welche abschließend gegen die Anforderungen zur gerichtlichen Verwertbarkeit diskutiert wurden.

Als Ergebnis dieser Arbeit entstand ein Anforderungskatalog, der am praxisnahen Beispiel eine deutliche Verbesserung der forensischen Verwertbarkeit zeigte. Diese Verbesserungen fußen in erster Linie auf organisatorischen Anpassungen und im expliziten Formulieren von Anforderungen, die in anderen Kontexten üblicherweise bereits umgesetzt sind. Es wurden für ein forensisches Backup elf Anforderungen erarbeitet, welche jene des regulären Backups ergänzen.

Es wurden zudem die Limitierungen in der Umsetzung von Integritätsanforderungen und Nachweisen aufgezeigt. Die identifizierten Integritätseinschränkungen stehen zwar antipodal zur forensischen Arbeitsweise, können aber über die juristische Betrachtung, die die Verwendung des sachnächsten Beweises bedingt, eingefangen werden. Über die Würdigung entscheidet das Gericht. Hier ist ein Beweis, selbst wenn er die oben genannten Schwächen hat, besser als kein Beweis.



## Literatur

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [01] | Morgenroth, Lena (2022):<br>Incident Response und Forensik. Seite 10<br>( <a href="https://www.hisolutions.com/fileadmin/user_upload/Infocenter/SecCon/Schulungen/Know-how-to_go/Know-how2go_Response-Wiederanlauf_IR-Forensik_Morgenroth.pdf">https://www.hisolutions.com/fileadmin/user_upload/Infocenter/SecCon/Schulungen/Know-how-to_go/Know-how2go_Response-Wiederanlauf_IR-Forensik_Morgenroth.pdf</a> , verfügbar am: 13. Juni 2024)                          |
| [02] | Müller, Tobias (2024):<br>IT-Abteilung: IT-Teams, Aufgaben und Ziele im Überblick, Abs. Fazit: Die Gamechanger agiler Unternehmen!<br>( <a href="https://deeken-group.com/blog/it-abteilung-it-teams-aufgaben-und-ziele-im-%C3%BCberblick">https://deeken-group.com/blog/it-abteilung-it-teams-aufgaben-und-ziele-im-%C3%BCberblick</a> , verfügbar am 10.06.2024)                                                                                                    |
| [03] | Ionos SE (2023):<br>Backups in der Cloud – die bessere Datensicherung, Seite 1<br>( <a href="https://business-services.heise.de/specials/next-level-hosting-infrastruktur-fuer-profis/infrastruktur/beitrag/backups-in-der-cloud-die-bessere-datensicherung-4488">https://business-services.heise.de/specials/next-level-hosting-infrastruktur-fuer-profis/infrastruktur/beitrag/backups-in-der-cloud-die-bessere-datensicherung-4488</a> , verfügbar am 01.Mai 2024) |
| [04] | Strömer, Bruno (2023):<br>Veeam-Umfrage: Unternehmen stellen bisherige Backup-Strategien infrage, Abs. 3<br>( <a href="https://www.heise.de/news/Backup-Unternehmen-draengen-mit-Datensicherung-in-die-Cloud-7461920.htm">https://www.heise.de/news/Backup-Unternehmen-draengen-mit-Datensicherung-in-die-Cloud-7461920.htm</a> , verfügbar am 01.Mai 2024)                                                                                                           |
| [05] | Lira Atempo (2022):<br>3 Gründe für eine On-Premise-Backup-Lösung, Abs. 1<br>( <a href="https://blog.atempo.com/en/blog/3-grunde-fur-eine-on-premise-backup-losung">https://blog.atempo.com/en/blog/3-grunde-fur-eine-on-premise-backup-losung</a> , verfügbar am 01.Mai 2024)                                                                                                                                                                                        |

|      |                                                                                                                                                                                                                                                                                           |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [06] | Singh Kumar Shanu; Irfan Annie; Dayal Neelam (2019):<br>Cyber Forensics and Comparative Analysis of Digital Forensic Investigation Frameworks.<br>In: 2019 4th International Conference on Information Systems and Computer Networks (ISCON)                                              |
| [07] | vgl. Ebd. S.588                                                                                                                                                                                                                                                                           |
| [08] | vgl. Ebd. S.588                                                                                                                                                                                                                                                                           |
| [09] | Farooq Ummer; Shaukat Arslan; Butt Wasi Haider; Hassan Ali (2023):<br>A Systematic Literature Review of Latest Cloud Forensic Frameworks, Tools and Challenges.<br>In: 2nd International Conference on Emerging Trends in Electrical, Control, and Telecommunication Engineering (ETECTE) |
| [10] | vgl. Ebd. S.2                                                                                                                                                                                                                                                                             |
| [11] | vgl. Ebd. S.2                                                                                                                                                                                                                                                                             |
| [12] | Ebd. S.2                                                                                                                                                                                                                                                                                  |
| [13] | vgl. Ebd. S.5                                                                                                                                                                                                                                                                             |
| [14] | Jafari Fakeeha; Satti Rabail Shafique (2015):<br>Comparative Analysis of Digital Forensic Models.<br>In: Journal of Advances in Computer Networks, Vol. 3, No. 1, March 2015                                                                                                              |
| [15] | vgl. Ebd. S.82                                                                                                                                                                                                                                                                            |

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [16] | vgl. Ebd. S.83                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| [17] | vgl. Ebd. S.85                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| [18] | vgl. Ebd. S.86                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| [19] | Ebd. S.86                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| [20] | Bundesamt für Sicherheit in der Informationstechnik (2011):<br>Leitfaden IT-Forensik<br>( <a href="https://bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Sicherheitspruefungen/IT-Forensik/forensik_node.html">https://bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Sicherheitspruefungen/IT-Forensik/forensik_node.html</a> ), verfügbar am 03.März 2024)                                                                                                                                                                                                                              |
| [21] | Bundesamt für Sicherheit in der Informationstechnik (2020):<br>Grundschutz Kompendium mit Baustein: DER.2.2<br>( <a href="https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/05_DER_Detektion_und_Reaktion/DER_2_2_Vorsorge_fuer_die_IT_Forensik_2023.pdf?__blob=publicationFile&amp;v=3">https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/05_DER_Detektion_und_Reaktion/DER_2_2_Vorsorge_fuer_die_IT_Forensik_2023.pdf?__blob=publicationFile&amp;v=3</a> ), verfügbar am 03.März 2024) |
| [22] | Kent Karen; Chevalier Suzanne; Grance Tim; Dang Hung (2006):<br>SP 800-86 Guide to Integrating Forensic Techniques into Incident Response ( <a href="https://csrc.nist.gov/pubs/sp/800/86/final">https://csrc.nist.gov/pubs/sp/800/86/final</a> , verfügbar am 15.März 2024)                                                                                                                                                                                                                                                                                                             |
| [23] | Guttman Barbara; White Douglas R.; Williams Shannan; Walraven Tracy (2022):<br>IR 8387 Digital Evidence Preservation<br>( <a href="https://www.nist.gov/publications/digital-evidence-preservation-considerations-evidence-handlers">https://www.nist.gov/publications/digital-evidence-preservation-considerations-evidence-handlers</a> , verfügbar am 15.März 2024)                                                                                                                                                                                                                   |

|      |                                                                                                          |
|------|----------------------------------------------------------------------------------------------------------|
| [24] | Rückert, Christian(2023):<br>Digitale Daten als Beweismittel im Strafverfahren<br>Tübingen: Mohr Siebeck |
| [25] | vgl. Ebd. S.4                                                                                            |
| [26] | vgl. Ebd. S. 674                                                                                         |
| [27] | vgl. Ebd. S.651 ff.                                                                                      |
| [28] | vgl. Ebd. S.789                                                                                          |
| [29] | vgl. Ebd. S.653                                                                                          |
| [30] | vgl. Ebd. S.658                                                                                          |
| [31] | vgl. Ebd. S.789                                                                                          |
| [32] | vgl. Ebd. S.790                                                                                          |
| [33] | vgl. Ebd. S.662 ff.                                                                                      |
| [34] | vgl. Ebd. S.665 ff.                                                                                      |
| [35] | vgl. Ebd. S.790                                                                                          |
| [36] | vgl. Ebd. S.791                                                                                          |

|      |                                                                                                                                                                                                                                                                                                                                                 |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [37] | vgl. Ebd. S.673 ff.                                                                                                                                                                                                                                                                                                                             |
| [38] | vgl. Ebd. S.673                                                                                                                                                                                                                                                                                                                                 |
| [39] | vgl. Ebd. S.757                                                                                                                                                                                                                                                                                                                                 |
| [40] | vgl. Ebd. S.794                                                                                                                                                                                                                                                                                                                                 |
| [41] | vgl. Ebd. S.794 ff.                                                                                                                                                                                                                                                                                                                             |
| [42] | vgl. Ebd. S.688                                                                                                                                                                                                                                                                                                                                 |
| [43] | vgl. Ebd. S.689                                                                                                                                                                                                                                                                                                                                 |
| [44] | vgl. Ebd. S.748                                                                                                                                                                                                                                                                                                                                 |
| [45] | vgl. Ebd. S.795                                                                                                                                                                                                                                                                                                                                 |
| [46] | Bnwjournal (2022):<br>Debangana Ray Frye Forensic Standard versus Daubert Forensic Standard ( <a href="https://bnwjournal.com/2022/08/24/frye-forensic-standard-versus-daubert-forensic-standard/#_ftnref1">https://bnwjournal.com/2022/08/24/frye-forensic-standard-versus-daubert-forensic-standard/#_ftnref1</a> , verfügbar am 30.Mai 2024) |
| [47] | National Institute of Standards and Technology (2020):<br>SP 800-53: Security and Privacy Controls for Information Systems and Organizations ( <a href="https://doi.org/10.6028/NIST.SP.800-53r5">https://doi.org/10.6028/NIST.SP.800-53r5</a> , verfügbar am 15.März 2024)                                                                     |

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [48] | <p>Swanson, Marianne; Bowen, Pauline; Phillips, Amy Wohl; Gallup, Dean; Lynes, David (2010):<br/>SP 800-34: Contingency Planning Guide for Federal Information Systems<br/>(<a href="https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final">https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final</a> , verfügbar am 15.März 2024)</p>                                                                                                                                                                                                                                                            |
| [49] | <p>Bundesamt für Sicherheit in der Informationstechnik (2021):<br/>CON.3 Datensicherungskonzept<br/>(<a href="https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/KompendiumEinzelPDFs2021/03CONKonzepteundVorgehensweisen/CON3DatensicherungskonzeptEdition2021.pdf?blob=publicationFile&amp;v=2">https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/KompendiumEinzelPDFs2021/03CONKonzepteundVorgehensweisen/CON3DatensicherungskonzeptEdition2021.pdf?blob=publicationFile&amp;v=2</a><br/>, verfügbar am 15.März 2024)</p>                                     |
| [50] | <p>Bundesamt für Sicherheit in der Informationstechnik (2021):<br/>Umsetzungshinweise zum Baustein CON.3 Datensicherungskonzept<br/>(<a href="https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Umsetzungshinweise/Umsetzungshinweise2021/UmsetzungshinweiszumBausteinCON3Datensicherungskonzept.pdf?blob=publicationFile&amp;v=1">https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Umsetzungshinweise/Umsetzungshinweise2021/UmsetzungshinweiszumBausteinCON3Datensicherungskonzept.pdf?blob=publicationFile&amp;v=1</a><br/>, verfügbar am 15.März 2024)</p> |
| [51] | <p>Alqahtany, Saad; Clarke, Nathan; Furnell, Steven; Reich, Christoph (2014):<br/>A forensically-enabled IAAS cloud computing architecture<br/>In: Australian Digital Forensics Conference<br/>Seite: 77</p>                                                                                                                                                                                                                                                                                                                                                                                |
| [52] | <p>Hoeck, Michael; Donham, Jason; Rodriguez, Rene; Mukhyala, Chandra (2024):<br/>Gartner Magic Quadrant for Enterprise Backup and Recovery Software Solutions<br/>(<a href="https://www.veeam.com/de/gartner-magic-quadrant.html">https://www.veeam.com/de/gartner-magic-quadrant.html</a> , verfügbar am 13.Mai 2024)</p>                                                                                                                                                                                                                                                                  |

|      |                                                                                                                                                                                                                                                                                          |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [53] | Cruz, Juan Carlos Flores; Atkison, Travis (2011):<br>Digital Forensics on a Virtual Machine,<br>In: ACMSE '11: Proceedings of the 49th annual ACM Southeast Conference<br>vgl. Seite 6 ff.                                                                                               |
| [54] | Hirwani, Manish; Pan, Yin; Stackpole, Bill; Johnson, Daryl (2012):<br>Forensic Acquisition and Analysis of VMware Virtual Hard Disks<br>In: SAM'12 - The 2012 International Conference on Security and Management<br>vgl. Seite 14                                                       |
| [55] | Rahman, Shuaibur; Khan, M. N. A. (2015):<br>Review of Live Forensic Analysis Techniques<br>In: International Journal of Hybrid Information Technology<br>vgl. Seite 384                                                                                                                  |
| [56] | Forensic Tools & Techniques Catalog<br>( <a href="https://toolcatalog.nist.gov/">https://toolcatalog.nist.gov/</a> , verfügbar am 14.Mai 2024)                                                                                                                                           |
| [57] | Veeam Help Center User Guide (2023):<br>Types of Backup Files<br>( <a href="https://helpcenter.veeam.com/docs/agentforwindows/userguide/backup_files.html?ver=60">https://helpcenter.veeam.com/docs/agentforwindows/userguide/backup_files.html?ver=60</a> , verfügbar am 27.März 2024)  |
| [58] | Veeam Help Center (2023):<br>Veeam Agent for Microsoft Windows Veeam Agent for Linux Veeam Agent for Mac<br>( <a href="https://www.veeam.com/veeam_agents_feature_comparison_ds.pdf">https://www.veeam.com/veeam_agents_feature_comparison_ds.pdf</a> ,<br>verfügbar am 27.März 2024)    |
| [59] | VMware vSphere Produktdokumentation (2020):<br>vSphere Storage APIs<br>( <a href="https://docs.vmware.com/de/VMware-vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-3FD5AB1E-47B3-">https://docs.vmware.com/de/VMware-vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-3FD5AB1E-47B3-</a> |

|      |                                                                                                                                                                                                                                                                                                                |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | <a href="https://49B5-845E-5224BE062A59.html">49B5-845E-5224BE062A59.html</a> , verfügbar am 15.März 2024)                                                                                                                                                                                                     |
| [60] | Microsoft Learn (2024):<br>Hyper-V-Sicherungsansätze<br>( <a href="https://learn.microsoft.com/de-de/virtualization/hyper-v-on-windows/reference/hypervbackupapproaches">https://learn.microsoft.com/de-de/virtualization/hyper-v-on-windows/reference/hypervbackupapproaches</a> , verfügbar am 15.März 2024) |
| [61] | Alqahtany, Saad; Clarke, Nathan; Furnell, Steven; Reich, Christoph (2014):<br>A forensically-enabled IAAS cloud computing architecture<br>In: Australian Digital Forensics Conference<br>Seite: 79                                                                                                             |

## Anlagen

Anlagen, Kapitel 2: Sondierung der Anforderungen ..... A-I

Anlagen, Kapitel 3: Forensischer Wert eines Regelbackups .....A-IX



## Anlagen, Kapitel 2: Sondierung der Anforderungen

| Tab-ID | Datenbank                          | Suchstring                                                                                                                                                                                                                                                                                      | Treffer              |
|--------|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| DB_01  | IEEE Xplore                        | (((((("Abstract":Digital Forensic*) OR ("Abstract":IT Forensic*) OR ("Abstract":IT Forensik)) AND ((("Abstract":framework) OR ("Abstract":best practice*)) AND ((("Document Title":comparative) OR ("Document Title":review) OR ("Document Title":survey) OR ("Document Title":vergleich*)))))) | DB_01_01<br>DB_01_02 |
| DB_02  | ACM Digital Library                | "query": {Abstract:("digital forensics" or "it forensic" or "it forensik") AND Abstract:("framework" or "best practice") AND Title:("comparative" or "review" or "survey" or "vergleich*")}                                                                                                     | - ohne Passende -    |
| DB_03  | Google Scholar                     | (inabstract:(it OR digital*) AND (forensic* OR forensik)) AND (inabstract:(frameworks OR "best practice")) AND (intitle:(comparative OR review OR survey)))                                                                                                                                     | DB_03_01             |
| DB_04  | DBLP Computer Science Bibliography | Ohne Relevante Treffer selbst bei unspezifischer Suche                                                                                                                                                                                                                                          |                      |

**A\_ 1: Suchstrategie nach Metastudien in wissenschaftlichen Datenbanken**

| Tab-ID  | Journal                                         | Suchstring                                                                                                                                                                         | Treffer  |
|---------|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| Jour_01 | International Journal of Information Management | Title, abstract, keywords: "digital forensic" AND ("Comparative" OR "survey") AND ("framework" OR "best practice")<br>via sciencedirect                                            | - ohne - |
| Jour_02 | Information Fusion                              | Title, abstract, keywords: "digital forensic" AND ("Comparative" OR "survey") AND ("framework" OR "best practice")<br>via sciencedirect                                            | - ohne - |
| Jour_03 | ACM Computing Surveys                           | {Abstract:("digital forensics" or "it forensic" or "it forensik") AND Abstract:("framework" or "best practice") AND Title:("comparative" or "review" or "survey" or "vergleich*")} | - ohne - |
| Jour_04 | Journal of Strategic Information Systems        | Title, abstract, keywords: "digital forensic" AND ("Comparative" OR "survey") AND ("framework" OR "best practice")<br>via sciencedirect                                            |          |
| Jour_05 | GigaScience                                     | "digital Forensic" AND Framework                                                                                                                                                   | - ohne - |
| Jour_06 | Computers and Education                         | Title, abstract, keywords: "digital forensic" AND ("Comparative" OR "survey") AND ("framework" OR "best practice")<br>via sciencedirect                                            | - ohne - |

## A\_2: Suchstrategie nach Metastudien in wissenschaftlichen Journalen

| ID                                                                                                              | Beschreibung/Gruppierung                                                                                                                                                    | Aktivität | Src                   |
|-----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-----------------------|
| <b>Kapitel: Allgemeine Vorgehensweise (Seite 24-26)</b>                                                         |                                                                                                                                                                             |           |                       |
| FR_01_Anf_01                                                                                                    | Analyseauslösendes Event muss dokumentiert sein                                                                                                                             | Akt_01    | Seite 24<br>Abs. 1    |
| FR_01_Anf_02                                                                                                    | Forensische Analyse unterteilt in:<br>• strategische Vorbereitung; • operationale Vorbereitung; • Datensammlung; • Untersuchung; • Datenanalyse; • Dokumentation            | Akt_07    | Seite 24<br>Abs. 2    |
| FR_01_Anf_03                                                                                                    | forens. Werkzeuge müssen identifiziert und bereitgestellt sein                                                                                                              | Akt_03    | Seite 24<br>Abs. 2    |
| FR_01_Anf_04                                                                                                    | Kriterien, nach denen forensische Werkzeuge ausgewählt wurden sollten dokumentiert sein                                                                                     | Akt_03    | Seite 24<br>Abs. 2    |
| FR_01_Anf_05                                                                                                    | Datensammlung findet auf potenziell betroffenen Komponenten statt                                                                                                           | Akt_03    | Seite 24<br>Abs. 3 ff |
| FR_01_Anf_06                                                                                                    | Datensammlung: prinzipiell ist die Durchführung der Datensammlung zu dokumentieren                                                                                          | ??        | Seite 24<br>Abs. 3 ff |
| FR_01_Anf_07                                                                                                    | (idealerweise) Übereinstimmung mit forens. Prinzipien: vollständige Erfassung, keine Verfälschung der Daten durch Sicherung                                                 | Akt_03    | Seite 24<br>Abs. 3 ff |
| FR_01_Anf_08                                                                                                    | werden Daten verändert bzw. nur unvollständig gesichert, muss dies dokumentiert und gerechtfertigt werden, sowie der Verfälschungsgrad und dessen Bedeutung bewertet werden | Akt_04    | Seite 25<br>Abs. 1    |
| FR_01_Anf_09                                                                                                    | Datensammlung: Prinzipiell Daten in Reihenfolge ihrer Flüchtigkeit sammeln                                                                                                  | Akt_03    | Seite 25<br>Abs. 1    |
| FR_01_Anf_10                                                                                                    | Datensammlung: Ein forens. Dublikat sollte von allen betroffenen Massenspeichern gewonnen werden                                                                            | Akt_01    | Seite 25<br>Abs. 1    |
| FR_01_Anf_11                                                                                                    | Datensammlung: Der Ablauf der Datengewinnung muss angemessen dokumentiert werden                                                                                            | Akt_07    | Seite 25<br>Abs. 1    |
| <b>Kapitel: Die beweisichere Anfertigung eines Datenträgerabbilds (forensische Duplikation) (Seite 26 - 28)</b> |                                                                                                                                                                             |           |                       |
| FR_01_Anf_12                                                                                                    | Forensische Duplikation sollte bis auf begründete Ausnahmen im Rahmen der forens. Untersuchung angefertigt werden.                                                          | Akt_04    | Seite 26<br>Abs. 1    |
| FR_01_Anf_13                                                                                                    | Unverändertheit des Dateninhalts eines Datenträgers ist eine abso-                                                                                                          | Akt_04    | Seite 26              |

|                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |        |                      |
|---------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|----------------------|
|                                                                                                   | lute Notwendigkeit, wenn dieser ein Beweisstück eines jurist. Prozesses ist.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |        | Abs. 2               |
| FR_01_Anf_14                                                                                      | Physische Kopie - Von dem Datenträger muss eine physische Kopie hergestellt werden, d. h. der gesamte Sektorinhalt aller Sektoren des Datenträgers wird in die Datei hineingeschrieben                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Akt_04 | Seite 26<br>Abs. 2   |
| FR_01_Anf_15                                                                                      | Fehlerbehandlung - Lesefehler müssen eindeutig erkannt und protokolliert werden und durch vorher festgelegte Füllmuster ersetzt werden;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Akt_04 | Seite 26<br>Abs. 2   |
| FR_01_Anf_16                                                                                      | Anforderung forens. Dublikation:<br>Vollständigkeit des Abbildes - Reservierte Bereiche von Massenspeichern (bspw. HPA und DCO, siehe Kapitel) müssen sicher erkannt werden und für den Zeitpunkt der Abbilderstellung deaktiviert werden, um ein vollständiges Abbild zu erhalten;                                                                                                                                                                                                                                                                                                                                                                | Akt_04 | Seite 26<br>Abs. 2   |
| FR_01_Anf_17                                                                                      | Anforderung forens. Dublikation:<br>Unverändertheit - Die Erstellung des Abbildes muss mit der Berechnung einer kryptographischen Checksumme abgeschlossen werden, um die Unverändertheit des Abbildes nachweisen zu können.                                                                                                                                                                                                                                                                                                                                                                                                                       | Akt_04 | Seite 26<br>Abs. 2   |
| FR_01_Anf_18                                                                                      | Es sollte ein HW-Writeblocker eingesetzt werden                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Akt_03 | Seite 26<br>Abs. 3ff |
| FR_01_Anf_19                                                                                      | Nachdem das Abbild erstellt wurde, muss eine kryptographische Hashsumme sowohl über dem Originaldatenträger als auch über dem Image berechnet werden. Die Übereinstimmung ist die beweissichere Basis                                                                                                                                                                                                                                                                                                                                                                                                                                              | Akt_04 | Seite 27<br>Abs. 1   |
| FR_01_Anf_20                                                                                      | Datenträger für Aufnahme forensischer Daten müssen in einen gelöschten Zustand vor Aufnahme neuer Daten gesetzt werden, um Fehlinterpretationen zu verhindern                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Akt_06 | Seite 28<br>Abs. 3   |
| FR_01_Anf_21                                                                                      | Sicheres Löschen stellt den Datenschutz sicher                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Akt_06 | Seite 28<br>Abs. 3   |
| <b>Kapitel Der abschnittsbasierte Verlauf einer forensischen Untersuchung<br/>(Seite 60 - 65)</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |        |                      |
| FR_01_Anf_22                                                                                      | Prozessbegleitende Dokumentation zeichnet auf, welche Daten beim Durchführen der einzelnen Methoden gewonnen wurden                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Akt_07 | Seite 62<br>Abs. 2   |
| FR_01_Anf_23                                                                                      | Prozessbegleitende Dokumentation protokolliert Parameter der Datensammlung. Parameter können sein: <ul style="list-style-type: none"> <li>• Name und Versionsnummer des verwendeten Programms</li> <li>• Kommandozeilenparameter des Aufrufs</li> <li>• Forensische Absicherung dieses Werkzeugs, notfalls durch externe Schutzmechanismen wie Prüfsummen, Verschlüsselung, Signierung, Hardware-Schreibblocker oder andere Maßnahmen, die geeignet sind, Authentizität, Integrität oder Vertraulichkeit sicherzustellen</li> <li>• Erfahrung des Untersuchenden mit diesem Werkzeug</li> <li>• Motivation zur Auswahl dieses Werkzeugs</li> </ul> | Akt_07 | Seite 62<br>Abs. 2   |
| <b>Kapitel Datensammlung<br/>(Seite 88 - 90)</b>                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |        |                      |
| FR_01_Anf_24                                                                                      | Aus Katalog der forensischen Werkzeuge wird geeignetes Werkzeug ausgewählt                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Akt_07 | Seite 88<br>Abs 3    |
| FR_01_Anf_25                                                                                      | Erfassung der Systemzeit, ggf. Abweichungen zur Referenzzeit müssen dokumentiert werden                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Akt_07 | Seite 88<br>Abs 3    |
| FR_01_Anf_26                                                                                      | Eingestellte Zeitzone muss dokumentiert sein                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Akt_07 | Seite 88<br>Abs 3    |
| FR_01_Anf_27                                                                                      | Über die Ausgabe der eingesetzten forensischen Werkzeuge sollte eine geeignete kryptographische Hashsumme erzeugt werden                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Akt_07 | Seite 89<br>Abs 1    |
| FR_01_Anf_28                                                                                      | Liste der laufenden Prozesse sollte erstellt werden durch statisch kompilierte Programme von schreibgeschützten Datenträgern                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Akt_07 | Seite 89<br>Abs 1    |
| FR_01_Anf_29                                                                                      | Alle am System offenen Netzwerkverbindungen sind zu erfassen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Akt_07 | Seite 89<br>Abs 2    |
| FR_01_Anf_30                                                                                      | Am System angemeldete Nutzer sollten erfasst werden                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Akt_07 | Seite 89<br>Abs 3    |
| FR_01_Anf_31                                                                                      | Daten der forens. Dublikation müssen in ihrem Verbleib und deren Einsichtnahme lückenlos dokumentiert werden                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Akt_06 | Seite 90<br>Abs 1    |

|                                                                                                                       |                                                                                                                                                                                                                                 |        |                    |
|-----------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|--------------------|
| FR_01_Anf_32                                                                                                          | Vertraulichkeit der Daten muss gewährleistet sein                                                                                                                                                                               | Akt_05 | Seite 90<br>Abs 1  |
| FR_01_Anf_33                                                                                                          | Es ist festzulegen wann, die Daten durch sicheres Löschen wieder entfernt werden                                                                                                                                                | Akt_07 | Seite 90<br>Abs 1  |
| FR_01_Anf_34                                                                                                          | Während der Durchführung ist prozessbegleitend zu dokumentieren                                                                                                                                                                 | Akt_07 | Seite 90<br>Abs 1  |
| <b>Kapitel: Forensische Gewinnung von Datenträgerabbildern (forensische Duplikation) (Seite 235 - 238)</b>            |                                                                                                                                                                                                                                 |        |                    |
| FR_01_Anf_35                                                                                                          | Zur Gewinnung des Datenträgerabbildes muss es an einer forensischen Workstation angeschlossen sein oder an einem System betrieben werden das nachweislich während der Erstellung des Abbildes keine Änderungen vorgenommen hat. | Akt_06 | Seite 235<br>Abs 2 |
| FR_01_Anf_36                                                                                                          | Keine Änderung am Originaldatenträger während der Sicherung                                                                                                                                                                     | Akt_04 | Seite 235<br>Abs 3 |
| FR_01_Anf_37                                                                                                          | Keine Änderung am Originaldatenträger durch die Sicherungen                                                                                                                                                                     | Akt_06 | Seite 235<br>Abs 3 |
| FR_01_Anf_38                                                                                                          | Gesamter, erfassbarer Inhalt des Datenträgers wird gesichert                                                                                                                                                                    | Akt_03 | Seite 235<br>Abs 3 |
| FR_01_Anf_39                                                                                                          | Das Original und die Kopie haben denselben Inhalt, sichergestellt durch kryptographische Verfahren                                                                                                                              | Akt_04 | Seite 235<br>Abs 3 |
| FR_01_Anf_40                                                                                                          | Einsatz eines Writeblockers wird empfohlen                                                                                                                                                                                      | Akt_03 | Seite 236<br>Abs 5 |
| <b>Ablaufliste zum Erstellen eines beweissicheren forensischen Abbildes eines Massenspeichers (Seite 337 bis 338)</b> |                                                                                                                                                                                                                                 |        |                    |
| FR_01_Anf_41                                                                                                          | Hardwareverzeichnis für alle Datenträger erstellen                                                                                                                                                                              | Akt_02 | Seite 337<br>Abs 4 |
| FR_01_Anf_42                                                                                                          | Ggf Sicherung flüchtiger Daten planen                                                                                                                                                                                           | Akt_03 | Seite 337<br>Abs 4 |
| FR_01_Anf_43                                                                                                          | Schreibschutz überprüfen                                                                                                                                                                                                        | Akt_03 | Seite 337<br>Abs 4 |

### A\_ 3: Anforderungen forensische Sicherung: BSI Leitfaden IT-Forensik

| ID                                                                                                                                                                                                                                                    | Beschreibung/Gruppierung                                                                             | Aktivität | Src             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|-----------|-----------------|
| Hintergrund dieser Untersuchung ist der Versuch aus den Vorbereitungen für die forensische Analyse Hinweise zu finden, welche Daten wie gesichert werden sollen oder müssen:<br>Wie in der Einleitung beschrieben geht es hier um den Standardschutz. |                                                                                                      |           |                 |
| FR_02_Anf_01                                                                                                                                                                                                                                          | Prüfung rechtlicher und regulatorischer Rahmenbedingungen zur Erfassung und Auswertbarkeit           | Akt_07    | DER.2.2.A<br>1  |
| FR_02_Anf_02                                                                                                                                                                                                                                          | Im Leitfaden sollte beschrieben sein, wie Beweise gesichert werden                                   | Akt_07    | DER.2.2.A<br>5  |
| FR_02_Anf_03                                                                                                                                                                                                                                          | Eingesetzte forensische Werkzeuge sollten geeignet sein                                              | Akt_07    | DER.2.2.A<br>7  |
| FR_02_Anf_04                                                                                                                                                                                                                                          | Bei Werkzeugen muss sichergestellt sein, dass diese nicht manipuliert wurden                         | Akt_04    | DER.2.2.A<br>7  |
| FR_02_Anf_05                                                                                                                                                                                                                                          | Haltezeit von forensisch relevanten Daten sollte im Vorfeld festgelegt werden                        | Akt_07    | DER.2.2.A<br>9  |
| FR_02_Anf_06                                                                                                                                                                                                                                          | Datenträger sollten möglichst komplett dupliziert werden                                             | Akt_04    | DER.2.2.A<br>10 |
| FR_02_Anf_07                                                                                                                                                                                                                                          | Das Duplikat sollte bestenfalls nicht verändert werden, falls nicht möglich, dann möglichst wenig    | Akt_04    | DER.2.2.A<br>10 |
| FR_02_Anf_08                                                                                                                                                                                                                                          | Es sollten schriftlich dokumentierte kryptografische Prüfsummen von den Datenträgern angelegt werden | Akt_04    | DER.2.2.A<br>10 |
| FR_02_Anf_09                                                                                                                                                                                                                                          | Forens. Sicherungen sollten getrennt und in mehreren Kopien aufbewahrt werden.                       | Akt_06    | DER.2.2.A<br>10 |
| FR_02_Anf_10                                                                                                                                                                                                                                          | Es sollte sichergestellt sein, dass die so [schriftlich] doku-                                       | Akt_05    | DER.2.2.A       |

|              |                                                                                                                                                                                           |        |                 |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|-----------------|
|              | mentierten Prüfsummen nicht verändert werden können                                                                                                                                       |        | 10              |
| FR_02_Anf_11 | Damit die Daten gerichtlich verwertbar sind, sollte ein Zeuge bestätigen, wie dabei vorgegangen wurde und die erstellten Prüfsummen beglaubigen.                                          | Akt_07 | DER.2.2.A<br>10 |
| FR_02_Anf_12 | Bei Beweissicherung sollten alle Schritte dokumentiert werden:<br>- lückenlose Nachvollziehbarkeit des Umgangs mit Originalbeweismitteln<br>- welche Methoden wurden eingesetzt und warum | Akt_07 | DER.2.2.A<br>11 |
| FR_02_Anf_13 | Sichere Verwahrung von Originaldatenträgern und Beweismitteln                                                                                                                             | Akt_05 | DER.2.2.A<br>11 |

#### A\_4: Anforderungen forensische Sicherung: BSI: Grundsatz Kompendium (DER.2.2)

| ID                                  | Beschreibung/Gruppierung                                                                                                                                                                    | Aktivität | Src                       |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|---------------------------|
| Aus dem Fließtext wurde extrahiert: |                                                                                                                                                                                             |           |                           |
| FR_03_Anf_01                        | Analysten sollen auch Speicherorte außerhalb des phys. Zugriffs bedenken (zb Cloudspeicher, Mail-Server)                                                                                    | Akt_02    | Kapitel 3.1.1<br>Abs. 1   |
| FR_03_Anf_02                        | Proactive "measures" und Auditrecords können angelegt werden, um Untersuchungen ggf. zu vereinfachen. Diese zentral zu speichern ist hilfreich<br>Userverhalten tracken wird ebenso erwähnt | ??        | Kapitel 3.1.1<br>Abs. 3ff |
| FR_03_Anf_03                        | Sicherung priorisieren nach<br>[Wert; Flüchtigkeit; Aufwand]                                                                                                                                | Akt_03    | Kapitel 3.1.12<br>Abs. 1  |
| FR_03_Anf_04                        | Eine chain of custody sollte definiert und befolgt werden                                                                                                                                   | Akt_07    | Kapitel 3.1.12<br>Abs. 2  |
| FR_03_Anf_05                        | Jeder Schritt zur Datenakquise sollte geloggt werden                                                                                                                                        | Akt_07    | Kapitel 3.1.12<br>Abs. 3  |
| FR_03_Anf_06                        | Wenn möglich, sollte ein "designated the evidence custodian" hinzugezogen werden                                                                                                            | Akt_07    | Kapitel 3.1.12<br>Abs. 3  |
| FR_03_Anf_06                        | Bit Stream Imaging ist dem logical Backup vorzuziehen                                                                                                                                       | Akt_03    | Kapitel 4.2.1<br>Abs. 1   |
| FR_03_Anf_07                        | Analysen sollten auf der Kopie durchgeführt werden                                                                                                                                          | Akt_06    | Kapitel 4.2.1<br>Abs. 1   |
| FR_03_Anf_08                        | Alle Schritte sollten reproduzierbar dokumentiert werden                                                                                                                                    | Akt_07    | Kapitel 4.2.1<br>Abs. 1   |
| FR_03_Anf_09                        | Eigenschaften des zu sichernden Systems sollten aufgenommen werden                                                                                                                          | Akt_01    | Kapitel 4.2.1<br>Abs. 3   |
| FR_03_Anf_10                        | Tool für Imaging sollte CFTT Testig durchlaufen haben                                                                                                                                       | Akt_07    | Kapitel 4.2.1<br>Abs. 3   |
| FR_03_Anf_11                        | Integrität der Original-Datenquelle muss gewährt bleiben, dafür werden Schreibblocker eingesetzt                                                                                            | Akt_03    | Kapitel 4.2.2<br>Abs. 1   |
| FR_03_Anf_12                        | Nach Abschluss der Sicherung sollte das exakte Duplikat über eine Checksumme nachgewiesen werden. (message digest)                                                                          | Akt_04    | Kapitel 4.2.2<br>Abs. 3   |
| FR_03_Anf_13                        | Es sollte SHA-1 genutzt werden als Hashing-Algo                                                                                                                                             | Akt_04    | Kapitel 4.2.2<br>Abs. 3   |
| FR_03_Anf_14                        | Der Hashwert soll über Quell-Datenträger vor der Backup-Erzeugung generiert werden und vergleichend über Sicherung danach                                                                   | Akt_04    | Kapitel 4.2.2<br>Abs. 3   |
| FR_03_Anf_15                        | File Modification, Access & creation Time sollen erhalten bleiben                                                                                                                           | Akt_03    | Kapitel 4.2.3<br>Abs. 1   |

#### A\_5: Anforderungen forensische Sicherung: NIST: SP 800-86

| ID                                  | Beschreibung/Gruppierung                                                                                                                                                                                                                                                                                       | Akt.   | Src                 |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|---------------------|
| Aus dem Fließtext wurde extrahiert: |                                                                                                                                                                                                                                                                                                                |        |                     |
| FR_04_Anf_01                        | Chain of Custody: Dokumentation der Original-Quelle & wie das Image erstellt wurde                                                                                                                                                                                                                             | Akt_07 | Kapitel 3.2. Abs. a |
| FR_04_Anf_02                        | Hashes und digitale Signaturen müssen entweder durch entsprechende Softwaresysteme übernommen werden oder manipulations-sicher vor dem Analysten abgelegt werden.                                                                                                                                              | Akt_05 | Kapitel 3.2. Abs. b |
| FR_04_Anf_03                        | Fehlgeschlagener Hashvergleich:<br>Mehrere Kopien ablegen, sodass defekte Kopie verworfen werden kann<br>Blockhashes verwenden um Fehler einzugrenzen<br>Bei fehlendem Backup muss herausgefunden werden, ob Änderung versehentlich oder absichtlich erzeugt                                                   | Akt_04 | Kapitel 3.2. Abs. c |
| FR_04_Anf_04                        | Fileabsicherung: sollten gehalten werden in einem System, dass nicht mit dem Internet verbunden ist mit strengen Zutritts und Autorisierungskontrollen und Logging                                                                                                                                             | Akt_06 | Kapitel 3.2. Abs. e |
| FR_04_Anf_05                        | Beweise müssen auf zuvor zuverlässig gelöschten Medien liegen                                                                                                                                                                                                                                                  | Akt_06 | Kapitel 3.2.3       |
| FR_04_Anf_06                        | Eine Kopie aller Beweise sollte an anderem Ort, der unwahrscheinlich gleichzeitig betroffen sein wird, gespeichert werden .                                                                                                                                                                                    | Akt_05 | Kapitel 3.2.3       |
| FR_04_Anf_07                        | Für Cloudspeicher beachte Security, Encryption und Transition                                                                                                                                                                                                                                                  | Akt_04 | Kapitel 3.2.3       |
| FR_04_Anf_08                        | Daten sollten on Rest verschlüsselt sein                                                                                                                                                                                                                                                                       | Akt_05 | Kapitel 3.2.5       |
| FR_04_Anf_09                        | Wurde in proprietärem Format gesichert, muss es zugänglich bleiben                                                                                                                                                                                                                                             | Akt_05 | Kapitel 3.2.6       |
| FR_04_Anf_11                        | Hashes müssen an einem sicheren Ort gespeichert werden.<br>- Digitaler Speicher<br>- manueller Speicher<br>- Blockchain                                                                                                                                                                                        | Akt_05 | Kap3.2              |
| FR_04_Anf_13                        | Forensik-Tools sollten folgende Fehlererkennung implementiert haben:<br>Unvollständigkeit<br>Ungenauigkeit:<br>- Werden vom Tool keine Daten ergänzt<br>- Werden vom Tool keine Daten verändert<br>- Werden vom Tool Daten richtig zugeordnet<br>- sicherer Umgang mit korrupten Daten<br>- Missinterpretation | Akt_07 | Kap:4.10            |

### A\_6: Anforderungen forensische Sicherung NIST: IR 8387

| ID                                                                                                               | Beschreibung/Gruppierung                                                                                                                                    | Akt.   | Src          |
|------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|--------------|
| Es werden aus den Anforderungen gegen das Gericht, die Anforderungen für das/die Beweismittel direkt abgeleitet. |                                                                                                                                                             |        |              |
| GR_01_Anf                                                                                                        | Beste Beweismittelart sind die Daten selbst oder eine 1:1 Kopie dieser                                                                                      | GR_03  | s. 789 Abs.3 |
| GR_02_Anf                                                                                                        | Diese 1:1 Kopie sollte von einem IT-Forensischen Sachverständigen erstellt werden                                                                           | GR_03  | s. 789 Abs.3 |
| GR_03_Anf                                                                                                        | Das Beweismittel muss vollständig und erschöpfend dem Tatgericht zur Verfügung stehen, dazu reicht uU eine logische Sicherung als sachferneres Beweismittel | GR_05  | s. 790 Abs.1 |
| GR_04_Anf                                                                                                        | best mögliche > sachnächste > unmittelbarste Beweismittel muss dem Gericht zur Verfügung stehen.                                                            | GR_05  | s. 790 Abs.2 |
| GR_05_Anf                                                                                                        | Die Authentizität und Integrität eines Beweismittels muss gewahrt bleiben                                                                                   | Akt_04 | s. 790 Abs.6 |
| GR_06_Anf                                                                                                        | Daten sollen nach forensischen Standards erhoben werden<br>Errechnung und der Abgleich von Hash-Summen                                                      | Akt_04 | s. 791 Abs.1 |
| GR_07_Anf                                                                                                        | Daten sollen nach forensischen Standards erhoben werden<br>Verwendung von Write-Blockern bei Kopiervorgängen                                                | Akt_03 | s. 791 Abs.1 |

|           |                                                                                                                  |        |              |
|-----------|------------------------------------------------------------------------------------------------------------------|--------|--------------|
| GR_08_Anf | Daten sollen unter Einhaltung der sog. Verwahrkette erhoben werden                                               | Akt_07 | s. 791 Abs.1 |
| GR_09_Anf | Daten sollen nach forensischen Standards erhoben werden<br>engmaschige Dokumentation aller Verarbeitungsschritte | GR_02  | s. 791 Abs.1 |
| GR_10_Anf | Verlässlichkeit der Methode muss nachweisbar sein                                                                | GR_07  | s. 791 Abs.4 |
| GR_11_Anf | Fehlerfreie Anwendung der Methode muss nachgewiesen werden                                                       | GR_07  | s. 791 Abs.4 |
| GR_12_Anf | Durchführende Person muss qualifiziert sein                                                                      | ??     | s. 791 Abs.4 |
| GR_13_Anf | Alle durchgeführten Schritte müssen dokumentiert werden                                                          | GR_07  | s. 791 Abs.4 |
| GR_14_Anf | Der Vorgang muss wiederholbar sein (im Sinne von reproduzierbar mit gleichem Ergebnis)                           | GR_07  | s. 791 Abs.4 |
| GR_15_Anf | Nach Möglichkeit sollte ein transp. Tool verw. werden                                                            | GR_07  | s. 791 Abs.1 |

### A\_7: Digitale Daten als Beweismittel im Strafverfahren

| ID           | Beschreibung/Gruppierung                                                                                                                                                                               | Akt.   | Src       |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|-----------|
| BK_01_Anf_01 | Durchführen von Backups auf<br>Nutzerebene<br>Systemebene<br>Systemdokumentation<br>von festgelegten Systemkomponenten in abgestimmter Häufigkeit                                                      | ??     | CP-9 a, b |
| BK_01_Anf_02 | Verwendung einer Stichprobe von Sicherungsdaten bei der Wiederherstellung ausgewählter Systemfunktionen als Teil der Notfallplanprüfung.                                                               | ??     | CP-9 (2)  |
| BK_01_Anf_03 | Kopien der Backups sollten an nicht colocated Standort mit Produktiv-Systemen gespeichert werden                                                                                                       | Akt_05 | CP-9 (3)  |
| BK_01_Anf_04 | Bei Löschung von Backups sollte ein Vieraugenprinzip herrschen.                                                                                                                                        | Akt_06 | CP-9 (7)  |
| BK_01_Anf_05 | Implementierung kryptografischer Mechanismen zur Verhinderung der unbefugten Offenlegung oder Änderung.                                                                                                | Akt_05 | CP-9 (8)  |
| BK_01_Anf_06 | Systeme sollen in einen bekannten Zustand innerhalb einer zuvor definierten Zeit wiederhergestellt werden können                                                                                       | ??     | CP-10     |
| BK_01_Anf_07 | Transaktionsbasierte Systeme sollten auch transaktionsbasiert gesichert werden                                                                                                                         | ??     | CP-10 (2) |
| BK_01_Anf_08 | Ein sicherer Zustand muss innerhalb einer definierten Zeit wiederhergestellt werden, ein sicherer Zustand definiert sich über konfigurationskontrollierten und integritätsgeprüften Wiederherstellung. | ??     | CP-10 (4) |
| BK_01_Anf_09 | Komponenten, benutzt für die Wiederherstellung müssen geschützt sein.                                                                                                                                  | Akt_06 | CP-10 (6) |

### A\_8: Anforderungen reguläres Backup: NIST SP 800-53

| ID           | Beschreibung/Gruppierung                                                                                                        | Akt.   | Src   |
|--------------|---------------------------------------------------------------------------------------------------------------------------------|--------|-------|
| BK_02_Anf_01 | Wiederherstellungszeiten sollen sich am BCM orientieren                                                                         | ??     | 3.4.1 |
| BK_02_Anf_02 | In der Planung sollten verschiedene Arten des Backups und Restores betrachtet werden und nach Anforderung der Umgebung gewählt. | Akt_03 | 3.4.1 |
| BK_02_Anf_03 | Systemdaten sollten regelmäßig backuped werden                                                                                  | Akt_01 | 3.4.2 |
| BK_02_Anf_04 | Scope und Frequenz der Backups sollte nach Kritikalität und Änderungsfrequenz der Daten festgelegt sein                         | Akt_01 | 3.4.2 |
| BK_02_Anf_05 | Es sollte festgelegte Location, Namensschema, Medienretention und Transportmethode geben.                                       | Akt_04 | 3.4.2 |
| BK_02_Anf_06 | Spezifische Methoden sollten gewählt werden nach Datenverfügbarkeit und Integritätsanforderungen                                | Akt_04 | 3.4.2 |
| BK_02_Anf_07 | Datenbackups sollten in einer Offsite-Location liegen                                                                           | Akt_05 | 3.4.2 |

### A\_9: Anforderungen reguläres Backup: NIST SP 800-34

| ID           | Beschreibung/Gruppierung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Akt    | Src                  |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|----------------------|
| BK_03_Anf_01 | Einflussfaktoren für die Datensicherung müssen erhoben und dokumentiert werden.<br><ul style="list-style-type: none"> <li>• Speichervolumen,</li> <li>• Änderungsvolumen,</li> <li>• Änderungszeitpunkte,</li> <li>• Verfügbarkeitsanforderungen,</li> <li>• Integritätsbedarf sowie</li> <li>• rechtliche Anforderungen.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Akt_03 | CON.3.A1             |
| BK_03_Anf_02 | Der IT-Betrieb muss für jedes IT-System ein Verfahren festlegen, das definiert, welche Daten des IT-Systems wie gesichert werden                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Akt_01 | CON.3.A2             |
| BK_03_Anf_03 | In virtuellen Umgebungen sollte geprüft werden, ob das System durch Snapshot-Mechanismen der Virtualisierungsumgebung gesichert werden kann                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Akt_03 | CON.3.A2             |
| BK_03_Anf_04 | Für die Datensicherungsverfahren müssen Art, Häufigkeit und Zeitpunkte der Datensicherungen auf Basis der Einflussfaktoren bestimmt werden.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Akt_01 | CON.3.A2             |
| BK_03_Anf_05 | Es muss definiert sein, welche Speichermedien benutzt werden und wie der Transport und Aufbewahrungsmodalitäten ausgestaltet sein müssen.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Akt_07 | CON.3.A2             |
| BK_03_Anf_06 | Der IT-Betrieb muss ein Datensicherungskonzept auf Basis der festgelegten Verfahrensweise für die Datensicherung erstellen.<br><ul style="list-style-type: none"> <li>• welche IT-Systeme und welche darauf befindlichen Daten durch welche Datensicherung gesichert werden,</li> <li>• wie die Datensicherungen erstellt und wiederhergestellt werden können,</li> <li>• welche Parameter zu wählen sind, sowie</li> <li>• welche Hard- und Software eingesetzt wird.</li> <li>• Definitionen zu wesentlichen Aspekten der Datensicherung (z. B. zu differenzierende Datenarten), • Gefährdungslage,</li> <li>• Einflussfaktoren je IT-Systeme,</li> <li>• Datensicherungsplan je IT-Systeme sowie</li> <li>• relevante Ergebnisse des Notfallmanagements/BCM, insbesondere die Recovery Point Objective (RPO) je IT-System.</li> </ul> | Akt_07 | CON.3.A4<br>CON.3.A6 |
| BK_03_Anf_07 | Das Minimaldatensicherungskonzept muss festlegen, welche Anforderungen für die Datensicherung mindestens vom IT-Betrieb einzuhalten sind.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Akt_07 | CON.3.A4             |
| BK_03_Anf_08 | Der IT-Betrieb muss regelmäßige Datensicherungen gemäß dem (Minimal-)Datensicherungskonzept erstellen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Akt_01 | CON.3.A5             |
| BK_03_Anf_09 | Die erstellten Datensicherungen müssen in geeigneter Weise vor dem Zugriff Dritter geschützt werden                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Akt_05 | CON.3.A5             |
| BK_03_Anf_10 | Es muss regelmäßig getestet werden, ob die Datensicherungen wie gewünscht funktionieren                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | ??     | CON.3.A5             |
| BK_03_Anf_11 | Es muss regelmäßig getestet werden, ob gesicherte Daten problemlos und in angemessener Zeit zurückgespielt werden können                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | ??     | CON.3.A5             |
| BK_03_Anf_12 | Der IT-Betrieb sollte die Datenträger von Datensicherungen geeignet aufbewahren, sodass diese vor unbefugtem Zugriff geschützt werden.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Akt_06 | CON.3.A12            |
| BK_03_Anf_13 | Datenträger sollten räumlich getrennt von den gesicherten IT-Systemen aufbewahrt werden. Der Aufbewahrungsort sollte so klimatisiert sein, dass die Datenträger entsprechend der zeitlichen Vorgaben des Datensicherungskonzepts aufbewahrt werden können.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Akt_06 | CON.3.A12            |

**A\_ 10: Anforderungen reguläres Backup: CON.3 Datensicherungskonzept**

## Anlagen, Kapitel 3: Forensischer Wert

| ID   | Anforderungen elementar geclustert                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Begründung d. Konsolidierung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Formulierte Last                                                                                                                                                                                                                                                                                                |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| L_01 | <p>BK_02_Anf_03</p> <p>Systemdaten sollten regelmäßig backuped werden</p> <p>#####</p> <p>BK_02_Anf_04</p> <p>Frequenz der Backups sollte nach Kritikalität und Änderungsfrequenz der Daten festgelegt sein</p> <p>#####</p> <p>BK_01_Anf_01</p> <p>Durchführen von Backups in abgestimmter Häufigkeit</p> <p>#####</p> <p>BK_01_Anf_01</p> <p>Durchführen von Backups von festgelegter Systemkomponenten</p> <p>#####</p> <p>BK_03_Anf_08</p> <p>Der IT-Betrieb muss regelmäßige Datensicherungen gemäß dem (Minimal-)Datensicherungskonzept erstellen</p> | <p>Gemein der Anforderung ist, dass Backups überhaupt und in einer festgelegten, regelmäßigen Periodizität durchgeführt werden sollen. Parameter dieser sind Frequenz und Zeitpunkt, daraus ableitbar die Häufigkeit.</p> <p>Wertzuweisung der Parameter wird als Teil der Festlegung des Standard-Verfahrens über das Datensicherungskonzept verstanden und dort aufgenommen. Hier geht es darum dass ein Backup durchgeführt wird und dass es standardisiert durchgeführt wird. Nicht um die Standardisierung selbst</p> | <p>Das Backup soll in regelmäßiger Frequenz und zu festgelegten Zeitpunkten nach dem Datensicherungskonzept durchgeführt werden.</p>                                                                                                                                                                            |
| L_02 | <p>BK_02_Anf_04</p> <p>Scope der Backups sollte nach Kritikalität und Änderungsfrequenz der Daten festgelegt sein</p> <p>#####</p> <p>BK_03_Anf_02</p> <p>Der IT-Betrieb muss für jedes IT-System ein Verfahren festlegen, das definiert, welche Daten des IT-Systems wie gesichert werden</p> <p>#####</p> <p>BK_03_Anf_04</p> <p>Für die Datensicherungsverfahren müssen Art der Datensicherungen auf Basis der Einflussfaktoren bestimmt werden</p>                                                                                                      | <p>es wird ein Verfahren zur Identifizierung von Datenquellen gefordert. Änderungsfrequenz ist bereits Teil der Einflussfaktoren.</p>                                                                                                                                                                                                                                                                                                                                                                                      | <p>Es soll ein Verfahren geben, das für jedes IT-System bestimmt, welche Daten wie gesichert werden. Es soll mindestens Kritikalität der Daten und Einflussfaktoren [Speichervolumen, Änderungsvolumen, Änderungszeitpunkte, Verfügbarkeitsanforderungen, integritätsbedarf, rechtl. Anf.] berücksichtigen.</p> |

|      |                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                     |                                                                                                                                                                                                                 |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | <p>#####</p> <p>BK_03_Anf_01</p> <p>Einflussfaktoren für die Datensicherung müssen erhoben und dokumentiert werden.</p> <ul style="list-style-type: none"> <li>• Speichervolumen,</li> <li>• Änderungsvolumen,</li> <li>• Änderungszeitpunkte,</li> <li>• Verfügbarkeitsanforderungen,</li> <li>• Integritätsbedarf sowie</li> <li>• rechtliche Anforderungen</li> </ul> |                                                                                                                                                                                     |                                                                                                                                                                                                                 |
| L_03 | <p>BK_03_Anf_03</p> <p>In virtuellen Umgebungen sollte geprüft werden, ob das System durch Snapshot-Mechanismen der Virtualisierungsumgebung gesichert werden kann</p>                                                                                                                                                                                                   | übernommen                                                                                                                                                                          | In virtuellen Umgebungen soll geprüft werden, ob das System durch Snapshot-Mechanismen der Virtualisierungsumgebung gesichert werden kann                                                                       |
| L_04 | <p>BK_02_Anf_05</p> <p>Es sollte festgelegte Location, Namensschema, Medienretention und Transportmethode geben.</p> <p>#####</p> <p>BK_03_Anf_05</p> <p>Es muss definiert sein, welche Speichermedien benutzt werden und wie der Transport ausgestaltet wird</p>                                                                                                        | Spezifiziert, um was es sich handelt, auf das die Anforderung anzuwenden ist.                                                                                                       | Es soll für Backupmedien und Backupdateien die physische Verortung, ein Namensschema, Retention und Transportmethode festgelegt sein.                                                                           |
| L_05 | <p>BK_01_Anf_03</p> <p>Kopien der Backups sollten an nicht colocated Standort mit Produktiv-Systemen gespeichert werden</p> <p>#####</p> <p>BK_02_Anf_07</p> <p>Datenbackups sollten in einer Offsite-Location liegen</p> <p>#####</p> <p>BK_03_Anf_13</p> <p>Datenträger sollten räumlich getrennt von den gesicherten IT-Systemen aufbewahrt werden.</p>               | Ziel dieser Anforderung ist die räumliche Trennung der gehaltenen Backups. Dies ist weitreichender als die Trennung von Prod-Systemen und Backup-Daten.                             | Eine Kopie der Backupdaten soll an einer Offsite-Location gehalten werden                                                                                                                                       |
| L_06 | <p>BK_01_Anf_05</p> <p>Implementierung kryptografischer Mechanismen zur Verhinderung der unbefugten Offenlegung oder Änderung.</p> <p>#####</p> <p>BK_03_Anf_09</p> <p>Die erstellten Datensicherungen müssen in geeigneter Weise vor dem Zugriff Dritter</p>                                                                                                            | Zusammengefasst wird hier die sichere Verwahrung der Backups durch logischen Zugriffsschutz, physikalische Zugangsschutz und Umweltkontrolle gefordert. Damit beschreiben die kumu- | Sicherungsdateien sollen kryptografisch gesichert vor Manipulation, unbefugter Offenlegung, geschützt vor unberechtigtem Zugriff auf Medien in einer zugangsgeschützten, umweltkontrollierten Umgebung gehalten |

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | <p>geschützt werden</p> <p>#####</p> <p>BK_03_Anf_12</p> <p>Der IT-Betrieb sollte die Datenträger von Datensicherungen geeignet aufbewahren, sodass diese vor unbefugtem Zugriff geschützt werden.</p> <p>#####</p> <p>BK_03_Anf_13</p> <p>Der Aufbewahrungsort sollte so klimatisiert sein, dass die Datenträger entsprechend der zeitlichen Vorgaben des Datensicherungskonzepts aufbewahrt werden können.</p> <p>#####</p> <p>BK_03_Anf_05</p> <p>Es muss definiert sein, welche Speichermedien benutzt werden und wie Aufbewahrungsmodalitäten ausgestaltet sein müssen.</p>                                                                                                                                                                                                                                                   | <p>lierten Anforderungen bereits einen der Aufbewahrungsmodalitäten aus BK_03_Anf_05</p>                                                                                                                  | <p>werden.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| L_07 | <p>BK_01_Anf_04</p> <p>Bei Löschung von Backups sollte ein Vieraugenprinzip herrschen.</p> <p>#####</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <p>Übernommen. In der Integrität wird auch das Vorhandensein angenommen.</p>                                                                                                                              | <p>Bei Löschung von Backups soll ein Vieraugenprinzip herrschen.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|      | <p>BK_01_Anf_09</p> <p>Komponenten, benutzt für die Wiederherstellung müssen geschützt sein</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <p>Entfällt, kein Spezifikum von Backup-Systemen. Jedes System muss geschützt sein.</p>                                                                                                                   | <p>- entfällt -</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| L_08 | <p>BK_03_Anf_06</p> <p>Der IT-Betrieb muss ein Datensicherungskonzept auf Basis der festgelegten Verfahrensweise für die Datensicherung erstellen.</p> <ul style="list-style-type: none"> <li>• welche IT-Systeme und welche darauf befindlichen Daten durch welche Datensicherung gesichert werden,</li> <li>• wie die Datensicherungen erstellt und wiederhergestellt werden können,</li> <li>• welche Parameter zu wählen sind, sowie</li> <li>• welche Hard- und Software eingesetzt wird.</li> <li>• Definitionen zu wesentlichen Aspekten der Datensicherung (z. B. zu differenzierende Datenarten), • Gefährdungslage,</li> <li>• Einflussfaktoren je IT-Systeme,</li> <li>• Datensicherungsplan je IT-Systeme sowie</li> <li>• relevante Ergebnisse des Notfallmanagements/BCM, insbesondere die Recovery Point</li> </ul> | <p>Es werden zusammengefasst die Eigenschaften eines Datensicherungskonzepts in der Synthese der untersuchten Dokumente abzubilden hat. Dafür wird BK_03_Anf_06 als Grundlage übernommen und ergänzt.</p> | <p>Es soll ein Datensicherungskonzept erstellt werden, das mindestens beinhaltet:</p> <ul style="list-style-type: none"> <li>• welche IT-Systeme und welche darauf befindlichen Daten durch welche Datensicherung gesichert werden,</li> <li>• in welcher Frequenz Backups durchgeführt werden</li> <li>• wie die Datensicherungen erstellt und wiederhergestellt werden können,</li> <li>• welche Parameter zu wählen sind, sowie</li> <li>• welche Hard- und Software eingesetzt wird.</li> <li>• Definitionen zu wesentlichen Aspekten der Datensicherung</li> </ul> |

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                              |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | <p>Objective (RPO) je IT-System</p> <p>#####</p> <p>BK_03_Anf_07</p> <p>Das Minimaldatensicherungskonzept muss festlegen, welche Anforderungen für die Datensicherung mindestens vom IT-Betrieb einzuhalten sind.</p> <p>#####</p> <p>BK_02_Anf_04</p> <p>Frequenz der Backups sollte nach Kritikalität und Änderungsfrequenz der Daten festgelegt sein</p> <p>#####</p> <p>BK_02_Anf_02</p> <p>In der Planung sollten verschiedene Arten des Backups und Restores betrachtet werden und nach Anforderung der Umgebung gewählt.</p> <p>#####</p> <p>BK_02_Anf_06</p> <p>Spezifische Methoden sollten gewählt werden nach Datenverfügbarkeit und Integritätsanforderungen</p> <p>#####</p> <p>BK_01_Anf_01</p> <p>Durchführen von Backups auf</p> <p>Nutzerebene</p> <p>Systemebene</p> <p>Systemdokumentation</p> <p>von festgelegten Systemkomponenten in abgestimmter Häufigkeit</p> <p>#####</p> <p>Transaktionsbasierte Systeme sollten auch transaktionsbasiert gesichert werden</p> <p>#####</p> |                                                                                                                                                                                                                             | <p>cherung (z. B. zu differenzierende Datenarten),</p> <ul style="list-style-type: none"> <li>• Gefährdungslage,</li> <li>• Einflussfaktoren je IT-Systeme,</li> <li>• Datensicherungsplan je IT-Systeme</li> <li>• relevante Ergebnisse des Notfallmanagements/BCM, insbesondere die Recovery Point Objective (RPO) je IT-System</li> </ul> |
| L_09 | <p>BK_01_Anf_02</p> <p>Verwendung einer Stichprobe von Sicherungsdaten bei der Wiederherstellung ausgewählter Systemfunktionen als Teil der Notfallplanprüfung.</p> <p>####</p> <p>BK_03_Anf_10</p> <p>Es muss regelmäßig getestet werden, ob die Datensicherungen wie gewünscht funktionieren</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <p>Der weitreichenste Test einer Datensicherung ist die Wiederherstellung, daher werden die beiden inhaltlich unterschiedlichen Anforderungen hier zusammengefasst. Bei diesen Tests lässt sich die Zeit ermitteln. Die</p> | <p>In regelmäßigen Tests soll die Funktionalität der Sicherung und der Wiederherstellung in angemessener Zeit getestet werden.</p>                                                                                                                                                                                                           |

|      |                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                              |                                                                                                                                                            |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | #####<br>BK_03_Anf_11<br>Es muss regelmäßig getestet werden, ob gesicherte Daten problemlos und in angemessener Zeit zurückgespielt werden können                                                                                                                                                                                                                                      | Zeitvorgaben, sind Teil des Datensicherungskonzept im BCM.                                                                                                                                                   |                                                                                                                                                            |
|      | BK_01_Anf_06<br>Systeme sollen innerhalb einer zuvor definierten Zeit wiederhergestellt werden können<br>#####<br>BK_01_Anf_08<br>Ein sicherer Zustand muss innerhalb einer definierten Zeit wiederhergestellt werden,<br>#####<br>BK_02_Anf_01<br>Wiederherstellungszeiten sollen sich am BCM orientieren                                                                             | Für diese Arbeit ist nicht Zeit, sondern die Möglichkeit der Wiederherstellung relevant. Im Kontext der Arbeit ist mit Wiederherstellung die Bereitstellung des Systems für die forensische Analyse gemeint. | - entfällt -                                                                                                                                               |
| L_10 | BK_01_Anf_06<br>Systeme sollen in einen bekannten Zustand wiederhergestellt werden können<br>#####<br>BK_01_Anf_08<br>Ein sicherer Zustand muss wiederhergestellt werden<br>#####<br>BK_01_Anf_08<br>System sollten in einen sicheren Zustand wiederherstellbar sein. ein sicherer Zustand definiert sich über konfigurationskontrollierten und integritätsgeprüften Wiederherstellung | Diese Anforderungen eint die Forderung nach Wiederherstellbarkeit in einen bekannten Zustand.                                                                                                                | Die Wiederherstellung soll in einen nachvollziehbaren Zustand geschehen. Dieser definiert sich über eine Integritätsprüfung und einen Konfigurationsstand. |

#### A\_11: Konsolidierte Anforderungen reguläres Backup

| ID   | Anforderungen elementar geclustert                                                                                                                                                                          | Begründung d. Konsolidierung                                                                                                                                                          | Formulierte Last                                                                                                                                           |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| L_11 | FR_01_Anf_01<br>Analyseauslösendes Event muss dokumentiert sein                                                                                                                                             | übernommen                                                                                                                                                                            | Analyseauslösendes Event muss dokumentiert sein                                                                                                            |
| L_12 | FR_01_Anf_03<br>Vorbereitung: forens. Werkzeuge müssen identifiziert und bereitgestellt sein<br>####<br>FR_01_Anf_24<br>Aus Katalog der forensischen Werkzeuge wird geeignetes Werkzeug ausgewählt<br>##### | Hier werden Eigenschaften der Werkzeuge und der Werkzeugauswahl beschreiben. Annahme, existiert ein Katalog impliziert dies eine Vorauswahl. CFTT Testing wird ausgenommen, da spezi- | Forensische Werkzeuge sollen in einem Katalog begründet ausgewählt und verfügbar sein. Sie sollen eine Fehlererkennung implementiert haben, die Ungenauig- |

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                              |                                                                                                                                  |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
|      | <p>FR_01_Anf_04</p> <p>Vorbereitung: Kriterien, nach denen forensische Werkzeuge ausgewählt wurden sollten dokumentiert sein</p> <p>#####</p> <p>FR_02_Anf_03</p> <p>Eingesetzte forensische Werkzeuge sollten geeignet sein</p> <p>#####</p> <p>FR_03_Anf_10</p> <p>Tool für Imaging sollte CFTT Testing durchlaufen haben</p> <p>#####</p> <p>FR_04_Anf_13</p> <p>Forensik-Tools sollten Fehlererkennung implementiert haben [Ungenauigkeit, Unvollständigkeit, Missinterpretation]</p> <p>#####</p> <p>FR_01_Anf_23</p> <p>Prozessbegleitende Dokumentation protokolliert Parameter der Datensammlung. Parameter können sein:</p> <ul style="list-style-type: none"> <li>- Motivation zur Auswahl dieses Werkzeugs</li> </ul> | fisch US-Amerikanisch.                                                                                                                                                                       | keit, Unvollständigkeit oder Missinterpretation sichtbar macht.                                                                  |
| L_13 | <p>FR_02_Anf_04</p> <p>Bei Werkzeugen muss sichergestellt sein, dass diese nicht manipuliert wurden</p> <p>#####</p> <p>FR_01_Anf_23</p> <p>Prozessbegleitende Dokumentation protokolliert Parameter der Datensammlung. Parameter können sein:</p> <ul style="list-style-type: none"> <li>- Forensische Absicherung dieses Werkzeugs, notfalls durch externe Schutzmechanismen wie Prüfsummen, Verschlüsselung, Signierung, Hardware-Schreibblocker oder andere Maßnahmen, die geeignet sind, Authentizität, Integrität oder Vertraulichkeit sicherzustellen</li> </ul>                                                                                                                                                          | Anf. kann bei Imaging als auch bei der Analyse angebracht werden                                                                                                                             | Bei Werkzeugen muss sichergestellt sein, dass diese nicht manipuliert wurden                                                     |
| L_14 | <p>FR_01_Anf_05</p> <p>Datensammlung: findet auf potenziell betroffenen Komponenten statt</p> <p>#####</p> <p>FR_01_Anf_10</p> <p>Datensammlung: Ein forens. Dublikat sollte von allen betroffenen Massenspeichern gewonnen werden</p> <p>#####</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Es soll ein forensisches Duplikat bzw eine Sicherung angelegt wird, daher der Rückgriff auf unspezifischen Term "Datensammlung" und "Komponente" welche IT-Systeme und IT-Infrastruktur ein- | Die Datensammlung soll auf allen potenziell betroffenen Komponenten durchgeführt werden, ggf. auch außerhalb des phys. Zugriffs. |

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                     |                                                                                                                                                        |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | FR_03_Anf_01<br>Analysten sollen auch Speicherorte außerhalb des phys. Zugriffs bedenken (zb Cloudspeicher, Mail-Server)                                                                                                                                                                                                                                                                                                                                                                                     | schließt.                                                                                                                                                                                                           |                                                                                                                                                        |
| L_15 | FR_01_Anf_07<br>Datensammlung:(idealerweise) Übereinstimmung mit forens. Prinzipien keine Verfälschung der Daten durch Sicherung<br>#####<br>FR_01_Anf_08<br>werden Daten verändert bzw. nur unvollständig gesichert, muss dies dokumentiert und gerechtfertigt werden, sowie der Verfälschungsgrad und dessen Bedeutung bewertet werden<br>#####<br>FR_01_Anf_15<br>Fehlerbehandlung - Lesefehler müssen eindeutig erkannt und protokolliert werden und durch vorher festgelegte Füllmuster ersetzt werden; | Veränderungen der Daten während der Sicherung, auf der Sicherung müssen erkennbar sein.<br>Aus der Erkennbarkeit muss sich die Bedeutung ableiten lassen, was ein Analyseschritt ist und hier nicht berücksichtigt. | Abänderungen der forensischen Sicherung gegenüber der Datenquelle sollen konkret nachvollziehbar sein.                                                 |
| L_16 | FR_01_Anf_09<br>Datensammlung: Prinzipiell Daten in Reihenfolge ihrer Flüchtigkeit sammeln<br>#####<br>FR_01_Anf_42<br>Ggf Sicherung flüchtiger Daten planen<br>#####<br>FR_03_Anf_03<br>Sicherung priorisieren nach [Wert; Flüchtigkeit; Aufwand]                                                                                                                                                                                                                                                           | Hier wird vorgegeben in welcher Reihenfolge Daten gesichert werden sollen. Weitreichend ist FR_03_Anf_03 das inhaltlich übernommen wird.                                                                            | forensische Sicherungen sollen priorisiert nach Wert, Flüchtigkeit und Aufwand erfolgen                                                                |
|      | FR_01_Anf_02<br>Forensische Analyse unterteilt in:<br>• strategische Vorbereitung; • operationale Vorbereitung; • Datensammlung; • Untersuchung; • Datenanalyse; • Dokumentation                                                                                                                                                                                                                                                                                                                             | Allgemeine Gliederung, entfällt.                                                                                                                                                                                    | - entfällt -                                                                                                                                           |
| L_17 | FR_01_Anf_06<br>Datensammlung: prinzipiell ist die Durchführung der Datensammlung zu dokumentieren<br>#####<br>FR_01_Anf_11<br>Datensammlung: Der Ablauf der Datengewinnung muss angemessen dokumentiert werden<br>#####<br>FR_02_Anf_12<br>Bei Beweissicherung sollten alle Schritte dokumentiert                                                                                                                                                                                                           | Grundsätzlich ist eine prozessbegleitende Dokumentation anzufertigen. Kumulierter Inhalt aus den Anforderungen:<br>- Ablauf der Datengewinnung<br>- eingesetzte Methoden/Datei<br>- einzelne Schritte zur           | Es sollen die eingesetzte Methode und die einzelnen Schritte zur Datengewinnung dokumentiert werden, ebenso wie Eigenschaften des gesicherten Systems. |

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                       |                                                                                                                                 |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
|      | <p>werden:</p> <ul style="list-style-type: none"> <li>- welche Methoden wurden eingesetzt und warum</li> </ul> <p>#####</p> <p>FR_03_Anf_05</p> <p>Jeder Schritt zur Datenakquise sollte geloggt werden</p> <p>FR_01_Anf_22</p> <p>Prozessbegleitende Dokumentation zeichnet auf, welche Daten beim Durchführen der einzelnen Methoden gewonnen wurden</p> <p>#####</p> <p>FR_01_Anf_34</p> <p>Während der Durchführung ist prozessbegleitend zu dokumentieren</p> <p>#####</p> <p>FR_01_Anf_41</p> <p>Hardwareverzeichnis für alle Datenträger erstellen</p> <p>#####</p> <p>FR_03_Anf_09</p> <p>Eigenschaften des zu sichernden Systems sollten Dokumentiert werden</p> <p>#####</p> <p>FR_02_Anf_02</p> <p>Im Leitfaden sollte beschrieben sein, wie Beweise gesichert werden</p> | Datenakquise                                                                                                                                                                                          |                                                                                                                                 |
| L_18 | <p>FR_01_Anf_23</p> <p>Prozessbegleitende Dokumentation protokolliert Parameter der Datensammlung. Parameter können sein:</p> <ul style="list-style-type: none"> <li>- Name und Versionsnummer des verwendeten Programms</li> <li>- Kommandozeilenparameter des Aufrufs</li> <li>- Erfahrung des Untersuchenden mit diesem Werkzeug</li> </ul> <p>#####</p> <p>FR_01_Anf_27</p> <p>Über die Ausgabe der eingesetzten forensischen Werkzeuge sollte eine geeignete kryptographische Hashsumme erzeugt werden</p>                                                                                                                                                                                                                                                                      | <p>Nachvollziehbarkeit bei der Verwendung des Werkzeugs.</p> <p>Eigenschaften des Analysen werden nicht in Anforderungen der Sicherung aufgenommen, sie liegen Außerhalb der Reconnaissance Phase</p> | <p>Aufrufparameter und Rückgaben der verwendeten Tools sollten integritäts- und authentizitätsgeschützt gespeichert werden.</p> |
| L_19 | <p>FR_01_Anf_13</p> <p>Unverändertheit des Dateninhalts eines Datenträgers ist eine absolute Notwendigkeit, wenn dieser ein Beweisstück eines jurist. Prozesses ist.</p> <p>#####</p> <p>FR_01_Anf_35</p> <p>Zur Gewinnung des Datenträgerabbildes muss es an</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <p>Nachweis über die Unverändertheit der Datenquelle fordern die versch. Quellen recht einheitlich</p>                                                                                                | <p>Die originale Datenquelle soll durch den Prozess der forensischen Sicherung nachweisbar nicht geändert worden sein.</p>      |

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                   |                                                                                                                                                            |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | <p>einer forensischen Workstation angeschlossen sein oder an einem System betrieben werden das nachweislich während der Erstellung des Abbildes keine Änderungen vorgenommen hat.</p> <p>#####</p> <p>FR_01_Anf_36</p> <p>Keine Änderung am Originaldatenträger während der Sicherung</p> <p>####</p> <p>FR_01_Anf_37</p> <p>Keine Änderung am Originaldatenträger durch die Sicherungen</p> <p>#####</p> <p>FR_03_Anf_11</p> <p>Integrität der Original-Datenquelle muss gewährt bleiben, dafür werden Schreibblocker eingesetzt</p>                                                                                                                                                                                                                             |                                                                                                                                                                                                   |                                                                                                                                                            |
| L_20 | <p>FR_01_Anf_18</p> <p>Es sollte ein HW-Writeblocker eingesetzt werden</p> <p>#####</p> <p>FR_01_Anf_40</p> <p>Einsatz eines Writeblockers wird empfohlen</p> <p>####</p> <p>FR_01_Anf_43</p> <p>Schreibschutz überprüfen</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <p>Um das Originalbeweismittel zu schützen wird der Einsatz von Schreibblockern gefordert.</p>                                                                                                    | <p>Es sollen Schreibblocker eingesetzt werden, um die Integrität der originalen Datenquelle zu schützen</p>                                                |
| L_21 | <p>FR_01_Anf_14</p> <p>Anforderung forens. Dublikation:</p> <p>Physische Kopie - Von dem Datenträger muss eine physische Kopie hergestellt werden, d. h. der gesamte Sektorinhalt aller Sektoren des Datenträgers wird in die Datei hineingeschrieben</p> <p>#####</p> <p>FR_01_Anf_12</p> <p>Forensische Dublikation sollte bis auf begründete Ausnahmen im Rahmen der forens. Untersuchung angefertigt werden</p> <p>#####</p> <p>FR_01_Anf_16</p> <p>Anforderung forens. Dublikation:</p> <p>Vollständigkeit des Abbildes - Reservierte Bereiche von Massenspeichern (bspw. HPA und DCO, siehe Kapitel ) müssen sicher erkannt werden und für den Zeitpunkt der Abbilderstellung deaktiviert werden, um ein vollständiges Abbild zu erhalten;</p> <p>#####</p> | <p>Allen Anfordereungen ist gemein, dass Abbilder vollständig, möglichst auf bit, physikalischer Ebene durchgeführt werden sollen. Auf dieser Ebene bleibt automatisch FR_03_Anf_15 erhalten.</p> | <p>Eine forensische Sicherung soll als physische Kopie des Datenträgers erstellt werden und diesen vollständig, inkl. reservierter Bereiche, abbilden.</p> |

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                     |                                                                                                                                                  |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
|      | <p>FR_01_Anf_38</p> <p>Gesamter, erfassbarer Inhalt des Datenträgers wird gesichert</p> <p>#####</p> <p>FR_02_Anf_06</p> <p>Datenträger sollten möglichst komplett dupliziert werden</p> <p>#####</p> <p>FR_03_Anf_06</p> <p>Bit Stream Imaging ist dem logical Backup vorzuziehen</p> <p>#####</p> <p>FR_03_Anf_07</p> <p>Analysen sollten auf der Kopie durchgeführt werden</p> <p>#####</p> <p>FR_03_Anf_15</p> <p>File Modification, Access &amp; creation Time sollen erhalten bleiben</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                     |                                                                                                                                                  |
| L_22 | <p>FR_01_Anf_17</p> <p>Die Erstellung des Abbildes muss mit der Berechnung einer kryptographischen Checksumme abgeschlossen werden, um die Unverändertheit des Abbildes nachweisen zu können</p> <p>#####</p> <p>FR_01_Anf_19</p> <p>Nachdem das Abbild erstellt wurde, muss eine kryptographische Hashsumme sowohl über dem Originaldatenträger als auch über dem Image berechnet werden. Die Übereinstimmung ist die beweissichere Basis</p> <p>#####</p> <p>FR_02_Anf_08</p> <p>Es sollten schriftlich dokumentierte kryptografische Prüfsummen von den Datenträgern angelegt werden</p> <p>#####</p> <p>FR_01_Anf_39</p> <p>Das Original und die Kopie haben denselben Inhalt, sichergestellt durch kryptographische Verfahren</p> <p>#####</p> <p>FR_02_Anf_07</p> <p>Das Duplikat sollte bestenfalls nicht verändert werden, falls nicht möglich, dann möglichst wenig</p> <p>#####</p> <p>FR_03_Anf_12</p> <p>Nach Abschluss der Sicherung sollte das exakte Dup-</p> | <p>Alle Anforderungen laufen zusammen, dass es nach der Sicherung einen Nachweis über die Exaktheit der Kopie gegenüber dem Original geben soll. Dies soll über Hashsummen nachgewiesen werden.</p> | <p>Über ein kryptographisches Verfahren soll nach der forensischen Sicherung das exakte Duplikat gegenüber dem Original nachgewiesen werden.</p> |

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                         |                                                                                           |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
|      | <p>likat über eine Checksumme nachgewiesen werden.<br/>(message digist)</p> <p>#####</p> <p>FR_03_Anf_13</p> <p>Es sollte SHA-1 genutzt werden als Hashing-Algo</p> <p>#####</p> <p>FR_04_Anf_02</p> <p>Hashes und digitale Signaturen müssen entweder durch entsprechende Softwaresysteme übernommen werden oder manipulationssicher vor dem Analysten abgelegt werden.</p> <p>#####</p> <p>FR_04_Anf_11</p> <p>Hashes müssen an einem sichrern Ort gespeichert werden.</p> <p>#####</p> <p>FR_03_Anf_14</p> <p>Der Hashwert soll über Quell-Datenträger vor der Backup-Erzeugung generiert werden und vergleichend über Sicherung danach</p> |                                                                                                                                                         |                                                                                           |
| L_23 | <p>FR_01_Anf_20</p> <p>Datenträger für Aufnahme forensischer Daten müssen in einen gelöschten Zustand vor Aufnahme neuer Daten gesetzt werden, um Fehlinterpretationen zu verhindern</p> <p>#####</p> <p>FR_04_Anf_05</p> <p>Beweise müssen auf zuvor zuverlässig gelöschten Medien liegen</p>                                                                                                                                                                                                                                                                                                                                                 | Recht identische Anforderungen, zusammengefasst darauf, dass die Medien einen gelöschten Zustand haben sollen, welche die forensischen Sicherung tragen | Forensische Sicherungen sollen auf zuverlässig gelöschten Medien gespeichert werden.      |
| L_24 | <p>FR_01_Anf_21</p> <p>Sicheres Löschen stellt den Datenschutz sicher</p> <p>#####</p> <p>FR_01_Anf_33</p> <p>Es ist festzulegen wann die Daten durch sicheres Löschen wieder entfernt werden</p> <p>#####</p> <p>FR_02_Anf_05</p> <p>Haltedauer von forensisch relevanten Daten sollte im Vorfeld festgelegt werden</p>                                                                                                                                                                                                                                                                                                                       | recht identische Anforderungen.                                                                                                                         | Forensische Sicherungen sollen nach einer zuvor festgelegten Zeit sicher gelöscht werden. |
|      | <p>FR_01_Anf_25</p> <p>Erfassung der Systemzeit, ggf. Abweichungen zur Referenzzeit müssen dokumentiert werden</p> <p>#####</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Irrelevant bei post Mortem Analyse                                                                                                                      | - entfällt -                                                                              |

|      |                                                                                                                                                                                                                                                                                                                                                 |                                                                                              |                                                                                                               |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
|      | FR_01_Anf_26<br>Eingestellte Zeitzone muss dokumentiert sein                                                                                                                                                                                                                                                                                    |                                                                                              |                                                                                                               |
|      | FR_01_Anf_28<br>Liste der laufenden Prozesse sollte erstellt werden durch statisch kompilierte Programme von schreibgeschützten Datenträgern<br>#####<br>FR_01_Anf_29<br>Alle am System offenen Netzwerkverbindungen sind zu erfassen<br>#####<br>FR_01_Anf_30<br>Am System angemeldete Nutzer sollten erfasst werden                           | Irrelevant bei post Mortem Analyse                                                           | - entfällt -                                                                                                  |
| L_25 | .FR_04_Anf_06<br>Eine Kopie aller Beweise sollte an anderem Ort, der unwahrscheinlich gleichzeitig betroffen sein wird, gespeichert werden#<br>#####<br>FR_02_Anf_09<br>Forens. Sicherungen sollten getrennt und in mehreren Kopien aufbewahrt werden<br>#####<br>FR_04_Anf_07<br>Für Cloudspeicher beachte Security, Encryption und Transition | Verwahrung der forensischen Sicherung. Sicherung in Cloudsystemen wird hier nicht betrachtet | Forensischen Sicherungen sollen in mehreren Kopien an unterschiedlichen Orten vorgehalten werden.             |
| L_26 | FR_01_Anf_32<br>Vertraulichkeit der Daten muss gewährleistet sein<br>#####<br>FR_04_Anf_08<br>Daten sollten on Rest verschlüsselt sein                                                                                                                                                                                                          | Recht identische Anforderungen                                                               | Ruhende forensischen Sicherungen sollen verschlüsselt werden.                                                 |
| L_27 | FR_02_Anf_01<br>Prüfung rechtlicher und regulatorischer Rahmenbedingungen zur Erfassung und Auswertbarkeit                                                                                                                                                                                                                                      | Übernommen, Auswertung nicht Betrachtungsgegenstand                                          | Foren. Sicherungen sollen im rechtlich/regulatorischen Rahmen erstellt werden                                 |
| L_28 | FR_02_Anf_10<br>Es sollte sichergestellt sein, dass die so [schriftlich] dokumentierten Prüfsummen nicht verändert werden können                                                                                                                                                                                                                | übernommen                                                                                   | Es sollte sichergestellt sein, dass die [schriftlich] dokumentierten Prüfsummen nicht verändert werden können |
| L_29 | FR_02_Anf_11<br>Damit die Daten gerichtlich verwertbar sind, sollte ein Zeuge bestätigen, wie dabei vorgegangen wurde und die erstellten Prüfsummen beglaubigen.                                                                                                                                                                                | FR_02_Anf_11 inhaltlich übernommen                                                           | Es soll ein Zeuge bestätigen, wie bei der forensischen Sicherung vorgegangen wurde                            |

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                           |                                                                                                                                                       |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | #####<br>FR_03_Anf_06<br>Wenn möglich, sollte ein “designated the evidence custodian” hinzugezogen werden                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                           | und, die Prüfsummen beglaubigen                                                                                                                       |
|      | FR_03_Anf_02<br>Proactive “measures” und Auditrecords können angelegt werden, um Untersuchungen ggf. zu vereinfachen. Diese zentral zu speichern ist hilfreich<br>Userverhalten tracken wird ebenso erwähnt                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Irrelevant bei post Mortem Analyse                                                                                                                        | - entfällt -                                                                                                                                          |
| L_30 | FR_01_Anf_31<br>Daten der forens. Duplikation müssen in ihrem Verbleib und deren Einsichtnahme lückenlos dokumentiert werden<br>#####<br>FR_03_Anf_04<br>Eine chain of custody sollte definiert und befolgt werden<br>#####<br>FR_04_Anf_01<br>Chain of Custody: Dokumentation der Original-Quelle & wie das Image erstellt wurde<br>#####<br>FR_02_Anf_12<br>Bei Beweissicherung sollten alle Schritte dokumentiert werden:<br>- lückenlose Nachvollziehbarkeit des Umgangs mit Originalbeweismitteln<br>#####<br>FR_02_Anf_13<br>Sichere Verwahrung von Originaldatenträgern und Beweismitteln<br>FR_04_Anf_04<br>Fileabsicherung: [Daten] sollten gehalten werden in einem System, dass nicht mit dem Internet verbunden ist mit strengen Zutritts und Authorisierungskontrollen und Logging | Diese Anforderungen zielen auf die lückenlose Nachvollziehbarkeit des Umgangs mit dem originalen Beweismittel. Dieser soll lückenlos dokumentiert werden. | Im Umgang mit den Beweismitteln soll eine Chain of Custody gewahrt bleiben. Diese umfasst im Besonderen Verwahrung, Einsichtnahme, Quelle und Umgang. |
|      | FR_04_Anf_03<br>Fehlgeschlagener Hashvergleich:<br>Mehrere Kopien ablegen, sodass defekte Kopie verworfen werden kann<br>Blockhashes verwenden um Fehler einzugrenzen<br>Bei fehlendem Backup muss herausgefunden werden, ob Änderung versehentlich oder absichtlich erzeugt                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Analysetätigkeit. Anforderung, dass es nachvollziehbar sein muss ist aufgenommen.                                                                         | - entfällt -                                                                                                                                          |

### A\_12: : Konsolidierte Anforderungen forensische Sicherung

| Anforderung: | Thema                                                          |
|--------------|----------------------------------------------------------------|
| L_11         | Ohne Untersuchung                                              |
| L_12         | Untersucht in Thema 2 Eigenschaften des Werkzeugs              |
| L_0a         | Untersucht in Thema 2 Eigenschaften des Werkzeugs              |
| L_13         | Untersucht in Thema 3 Eigenschaften des Systems                |
| L_14         | Untersucht in Thema 4 Vollständigkeit der Datensicherung       |
| L_15         | Untersucht in Thema 2 Eigenschaften des Werkzeugs              |
| L_16         | Untersucht in Thema 4 Vollständigkeit der Datensicherung       |
| L_17         | Untersucht in Thema 5 Dokumentation                            |
| L_18         | Untersucht in Thema 6 Nachvollziehbarkeit                      |
| L_19         | Untersucht in Thema 7 Schutz der Datenquelle                   |
| L_20         | Untersucht in Thema 7 Schutz der Datenquelle                   |
| L_21         | Untersucht in Thema 8 Datenhaltung                             |
| L_22         | Untersucht in Thema 1 Integritätsnachweis gegenüber der Quelle |
| L_23         | Ohne Untersuchung                                              |
| L_24         | Untersucht in Thema 8 Datenhaltung                             |
| L_25         | Untersucht in Thema 8 Datenhaltung                             |
| L_26         | Untersucht in Thema 8 Datenhaltung                             |
| L_27         | Ohne Untersuchung                                              |
| L_28         | Untersucht in Thema 6 Nachvollziehbarkeit                      |
| L_29         | Untersucht in Thema 6 Nachvollziehbarkeit                      |
| L_30         | Untersucht in Thema 9 Chain of Custody                         |

### A\_13: Zuordnung Anforderung forensische Sicherung zum Thema

| ID                                                                                       | Forens. Dim.        | Last                                                                                                                                                   | Gewicht |
|------------------------------------------------------------------------------------------|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| Relevanz, Authentizität, Integrität, Nachvollziehbarkeit und gerichtliche Verwertbarkeit |                     |                                                                                                                                                        |         |
| L_12                                                                                     | Nachvollziehbarkeit | Forensische Werkzeuge sollen in einem Katalog begründet vorausgewählt und verfügbar sein.                                                              | 4       |
| L_30                                                                                     | Nachvollziehbarkeit | Im Umgang mit den Beweismitteln soll eine Chain of Custody gewahrt bleiben. Diese umfasst im Besonderen Verwahrung, Einsichtnahme, Quelle und Umgang   | 4       |
| L_17                                                                                     | Nachvollziehbarkeit | Es sollen die eingesetzte Methode und die einzelnen Schritte zur Datengewinnung dokumentiert werden, ebenso wie Eigenschaften des gesicherten Systems. | 3       |
| L_24                                                                                     | Nachvollziehbarkeit | Forensische Sicherungen sollen nach einer zuvor festgelegten Zeit sicher gelöscht werden.                                                              | 2       |
| L_15                                                                                     | Nachvollziehbarkeit | Abänderungen der forensischen Sicherung gegenüber der Datenquelle sollen konkret nachvollziehbar sein.                                                 | 1       |
| L_18                                                                                     | Nachvollziehbarkeit | Aufrufparameter und Rückgaben der verwendeten Tools sollten integritäts- und authentizitätsgeschützt gespeichert werden.                               | 1       |
| L_28                                                                                     | Nachvollziehbarkeit | Es sollte sichergestellt sein, dass die [schriftlich] dokumentierten                                                                                   | 1       |

|               |                             |                                                                                                                                                     |           |
|---------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
|               |                             | Prüfsummen nicht verändert werden können                                                                                                            |           |
| L_22          | Authentizität               | Über ein kryptographisches Verfahren soll nach der forensischen Sicherung das exakte Duplikat gegenüber dem Original nachgewiesen werden.           | 4         |
| L_13          | Integrität                  | Bei Werkzeugen muss sichergestellt sein, dass diese nicht manipuliert wurden                                                                        | 3         |
| L_21          | Integrität                  | Eine forensische Sicherung soll als physische Kopie des Datenträgers erstellt werden und diesen vollständig, inkl. reservierter Bereiche, abbilden  | 3         |
| L_16          | Integrität                  | Forensische Sicherungen sollen priorisiert nach Wert, Flüchtigkeit und Aufwand erfolgen                                                             | 2         |
| L_19          | Integrität                  | Die originale Datenquelle soll durch den Prozess der forensischen Sicherung nachweisbar nicht geändert worden sein.                                 | 2         |
| L_23          | Integrität                  | Forensische Sicherungen sollen auf zuverlässig gelöschten Medien gespeichert werden.                                                                | 2         |
| L_25          | Integrität                  | Forensische Sicherungen sollen in mehreren Kopien an unterschiedlichen Orten vorgehalten werden.                                                    | 2         |
| L_26          | Integrität                  | Ruhende forensische Sicherungen sollen verschlüsselt werden.                                                                                        | 2         |
| L_0a          | Integrität                  | Forensische Werkzeuge sollen eine Fehlererkennung implementiert haben, die Ungenauigkeit, Unvollständigkeit oder Missinterpretation sichtbar macht. | 4         |
| L_20          | Integrität                  | Es sollen Schreibblocker eingesetzt werden, um die Integrität der originalen Datenquelle zu schützen                                                | 1         |
| L_14          | gerichtliche Verwertbarkeit | Die Datensammlung soll auf allen potenziell betroffenen Komponenten durchgeführt werden, ggf. auch außerhalb des phys. Zugriffs                     | 2         |
| L_29          | gerichtliche Verwertbarkeit | Es soll ein Zeuge bestätigen, wie bei der forensischen Sicherung vorgegangen wurde, und die Prüfsummen beglaubigen                                  | 2         |
| L_27          | gerichtliche Verwertbarkeit | Foren. Sicherungen sollen im rechtlich/regulatorischen Rahmen erstellt werden                                                                       | 1         |
| L_11          | -ohne-                      | Analyseauslösendes Event muss dokumentiert sein                                                                                                     | 1         |
| <b>Summe:</b> |                             |                                                                                                                                                     | <b>47</b> |

#### A\_ 14: Metrik zur Beurteilung der forensischen Güte

| ID   | Last                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| L_01 | Das Backup soll in regelmäßiger Frequenz und zu festgelegten Zeitpunkten nach dem Datensicherungskonzept durchgeführt werden.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| L_02 | Es soll ein Verfahren geben, das für jedes IT-System bestimmt, welche Daten wie gesichert werden. Es soll mindestens Kritikalität der Daten und Einflussfaktoren [Speichervolumen, Änderungsvolumen, Änderungszeitpunkte, Verfügbarkeitsanforderungen, integritätsbedarf, rechtl. Anf.] berücksichtigen.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| L_03 | In virtuellen Umgebungen soll geprüft werden, ob das System durch Snapshot-Mechanismen der Virtualisierungsumgebung gesichert werden kann                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| L_04 | Es soll für Backupmedien und Backupdateien die physische Verortung, ein Namensschema, Retention und Transportmethode festgelegt sein.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| L_05 | Eine Kopie der Backupdaten soll an einer Offsite-Location gehalten werden                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| L_06 | Sicherungsdateien sollen kryptografisch gesichert vor Manipulation, unbefugter Offenlegung, geschützt vor unberechtigtem Zugriff auf Medien in einer zugangsgeschützten, umweltskontrollierten Umgebung gehalten werden.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| L_07 | Bei Löschung von Backups soll ein Vieraugenprinzip herrschen.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| L_08 | Es soll ein Datensicherungskonzept erstellt werden, das mindestens beinhaltet: <ul style="list-style-type: none"> <li>• welche IT-Systeme und welche darauf befindlichen Daten durch welche Datensicherung gesichert werden,</li> <li>• in welcher Frequenz Backups durchgeführt werden</li> <li>• wie die Datensicherungen erstellt und wiederhergestellt werden können,</li> <li>• welche Parameter zu wählen sind, sowie</li> <li>• welche Hard- und Software eingesetzt wird.</li> <li>• Definitionen zu wesentlichen Aspekten der Datensicherung (z. B. zu differenzierende Datenarten),</li> <li>• Gefährdungslage,</li> <li>• Einflussfaktoren je IT-Systeme,</li> <li>• Datensicherungsplan je IT-System</li> <li>• relevante Ergebnisse des Notfallmanagements/BCM, insbesondere die Recovery Point Objective (RPO) je IT-System</li> </ul> |
| L_09 | In regelmäßigen Tests soll die Funktionalität der Sicherung und der Wiederherstellung in angemessener Zeit getestet werden.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| L_10 | Die Wiederherstellung soll in einen nachvollziehbaren Zustand geschehen. Dieser definiert sich über eine Integritätsprüfung und einen Konfigurationsstand.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

### A\_ 15: Zusammenfassende Übersicht der Backup-Anforderungen



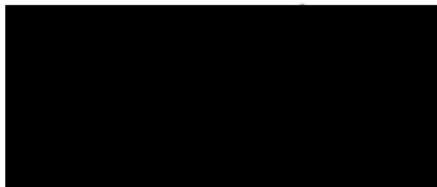
## Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Rathenow, den 18.07.2024



Thomas Willnat