Hochschule Luzern | Bachelor in Information and Cybersecurity | Projektarbeit

Implementierung von Chain of Custody in Incident Response Situationen

vorgelegt von:

Böller Jonas, Eser Kiymet, Isenring Alenka, Özsoy Derya, Schär Michelle, Sustic Andrea Megan

Betreuer der Arbeit: Spichiger Hannes
07.12.2023

Titelbild generiert mit OpenAI GPT-4

Implementierung von Chain of Custody in Incidence Response Situationen

Hochschule Luzern | Bachelor in Information and Cybersecurity | Projektarbeit

Böller Jonas
jonas.boeller@stud.hslu.ch

Eser Kiymet
kiymet.eser@stud.hslu.ch

Isenring Alenka
alenka.isenring@stud.hslu.ch

Özsoy Derya
derya.oezsoy@stud.hslu.ch

Schär Michelle
michelle.schaer@stud.hslu.ch

Sustic Andrea Megan
andrea.sustic@stud.hslu.ch

Dozent: Wiese Hanno
Betreuer: Spichiger Hannes

Hochschule Luzern, 07.12.2023

Management Summary

Das Buch «Implementierung von Chain of Custody in Incident Response Situationen» gibt umfassenden Einblick in die Bedeutung, Herausforderungen und Anwendungen der Chain of Custody (CoC) im Bereich der Incident Response (IR) innerhalb der Cybersicherheit. Es verbindet theoretische Grundlagen mit praktischen Anwendungen und unterstreicht die Relevanz einer korrekten Beweiskettenführung in der digitalen Forensik.

Die Zielgruppe dieses Buches besteht aus Fachleuten und Studierenden des Bereichs Informationssicherheit. Es soll ein umfassendes Verständnis der Bedeutung und Komplexität, eine Chain of Custody zu implementieren, vermitteln. Das Buch bietet wertvolle Erkenntnisse durch eine Kombination aus theoretischen Überlegungen und praktischen Erfahrungen und dient als umfassender Leitfaden zur Optimierung der Sicherheitspraktiken in Organisationen. Ziel ist es, das Bewusstsein dafür zu schärfen, wie wichtig es ist, einen durchdachten Chain of Custody Prozess zu implementieren und diesen in der Praxis effektiv umzusetzen, um die technischen und rechtlichen Anforderungen der Cybersicherheit zu erfüllen.

Kapitel 1 («Bedeutung der Chain of Custody in der IT-Forensik») beschäftigt sich zusammenfassend mit der grundlegenden Bedeutung und Struktur der Chain of Custody in der Forensik. Es wird betont, wie wichtig es ist, die Integrität und Authentizität digitaler Beweise durch detaillierte Dokumentationsprozesse und forensische Techniken zu sichern. Dieses Wissen hilft in der Praxis bei der Sicherstellung der Zulassung digitaler Beweise in rechtlichen Auseinandersetzungen und stärkt die Beweiskraft in IT-Forensik-Ermittlungen.

Im **Kapitel 2 («Möglichkeiten und Herausforderungen zur Einhaltung der Chain of Custody»)** werden die technischen Massnahmen zur Sicherung der Chain of Custody behandelt und Herausforderungen wie moderne IT-Umgebungen und Cloud-Systeme beleuchtet. Write-Blocker, Hashing und Memory Capture sind hierbei die Schlüsseltechniken, die verwendet werden. Die Anwendbarkeit dieser Techniken ist für Unternehmen und Organisationen von grosser Bedeutung, um die Integrität von Beweisen zu wahren und rechtlichen Anforderungen zu genügen.

Kapitel 3 («Incident Response in der IT-Forensik») beschäftigt sich mit dem Incident-Response-Prozess mit dem Schwerpunkt auf der Rolle der Incident-Response-Prozess in der IT-Forensik und Cybersicherheit. Es betont die Wichtigkeit von vorbereiteten Reaktionsstrategien und forensischen Praktiken für die Analyse und Bewältigung von Sicherheitsvorfällen. Dieses Kapitel ist von besonderer Relevanz für das IT-Sicherheitsmanagement in Unternehmen, um auf Cyberangriffe effektiv reagieren und Risiken minimieren zu können.

Kapitel 4 («Operationelle Einschränkungen und Entscheidungskriterien im Incident-Response») behandelt die operationellen Einschränkungen und Entscheidungskriterien im Incident-Response-Prozess. Dabei wird die Wichtigkeit von Fachwissen, technologischer Ausstattung und rechtlicher Einhaltung hervorgehoben, um Krisensituationen effektiv zu bewältigen und eine rechtskonforme Vorgehensweise sicherzustellen.

Im **Kapitel 5 («Herausforderungen der Chain of Custody in der Incident Response»)** werden die gegenwärtigen Herausforderungen und zukünftigen Entwicklungen der Chain of Custody, einschliesslich der Rolle von KI und Blockchain, erörtert. Dieses Kapitel ist von besonderer Relevanz für die technologischen Fortschritte und Innovationen in der IT-Forensik und trägt dazu bei, dass Organisationen sich auf künftige Bedrohungen und technologische Veränderungen besser vorbereiten können.

Zusammenfassung der wichtigsten Erkenntnisse:

- Die Chain of Custody ist ein entscheidender Faktor für die Beweisführung und das Management von Sicherheitsvorfällen.
- Technologische Entwicklungen wie künstliche Intelligenz und Blockchain bieten neue Möglichkeiten, die Effizienz der Chain of Custody zu verbessern.
- Die Anpassung an gesetzliche Änderungen und internationale Standards bleibt eine ständige Herausforderung.
- Menschliches Verhalten und Bewusstsein spielen eine zentrale Rolle bei der erfolgreichen Umsetzung der Chain of Custody.

Das Konzept, das sich aus allen Kapiteln ergibt, ist ein umfassendes Rahmenwerk für das Management von Incident Response und die Umsetzung der Chain of Custody in Incident Response. Durch die effektive Kombination dieser Erkenntnisse können Organisationen ein starkes Sicherheitssystem aufbauen, das sowohl vorbeugende als auch reaktive Massnahmen beinhaltet.

Schlussfolgerungen und Handlungsempfehlungen:

- Für eine effektive Implementierung und Verwaltung der Chain of Custody ist ein interdisziplinärer Ansatz erforderlich.
- Eine Integration von forensischen Prinzipien in die Incident-Response-Prozesse ist von grosser Bedeutung.
- Auch sollten Teams gebildet werden, die sowohl technisches als auch juristisches Verständnis mitbringen.
- Zudem sollten technologische Innovationen für zukünftige Herausforderungen in der IT-Forensik berücksichtigt werden.

Organisationen sollten sich darauf konzentrieren, ein interdisziplinäres Team aufzubauen, das sowohl technisches als auch rechtliches Verständnis besitzt, um die Chain of Custody in verschiedenen Situationen zu implementieren und zu verwalten. Die Integration von forensischen Prinzipien in die Incident-Response-Prozesse ermöglicht es, fundierte Entscheidungen zu treffen, die sowohl rechtlich abgesichert als auch technisch durchführbar sind.

Vorwort

Dieses Buch entstand im Rahmen des Moduls «Secure Project und Teamarbeit» an der Hochschule Luzern. Leiterin des Projekts war Andrea Megan Sustic. Die Autoren sind Jonas Böller, Kiymet Eser, Alenka Isenring, Derya Özsoy, und Michelle Schär. Das Modul wurde geleitet von Hanno Wiese und der Coach für diese Arbeit war Hannes Spichiger.

Das Buch befasst sich mit der Umsetzung der Chain of Custody in Incident Response Situationen. Die ersten beiden Kapitel geben einen Überblick über das Thema Chain of Custody. Die zwei Kapitel danach befassen sich mit dem Incident Response Prozess und das letzte Kapitel mit der Umsetzung der Chain of Custody in den verschiedenen Phasen des Incident Response Prozesses.

Danksagung

Unser Dank gilt allen, die uns bei der Entstehung dieser Arbeit unterstützt haben.

Insbesondere möchten wir unserem Coach, Hannes Spichiger, für seine fortwährende Unterstützung und wertvolle Anleitung danken, die zur Verbesserung dieser Arbeit beigetragen hat.

Gleichzeitig möchten wir Hanno Wiese, unserem Dozenten, für seine hilfreichen Anregungen und konstruktive Kritik danken, die zur inhaltlichen und methodischen Optimierung beigetragen haben.

Ein herzliches Dankeschön an unsere Kommilitonen, die durch ihre Peer-Reviews und konstruktiven Dialog dazu beigetragen haben, die Qualität dieser Arbeit zu verbessern. Wir schätzen die engagierte Unterstützung aller Beteiligten während des Entstehungsprozesses dieser Arbeit.

Gender Disclaimer

In diesem Text konnten geschlechtsneutrale Formulierungen aus Gründen der Lesbarkeit und des Textflusses nicht überall verwendet werden.

Die Verwendung maskuliner oder femininer Pronomen und Begriffe sollte als inklusiv für alle Geschlechter verstanden werden, und es wird keine Voreingenommenheit oder Diskriminierung beabsichtigt. Es ist wichtig zu beachten, dass diese Formulierungen beabsichtigen, alle Geschlechter einzubeziehen und keinesfalls diskriminierend sind.

Wir schätzen und respektieren Vielfalt und Inklusivität, und dieses Werk soll für alle Leser*innen zugänglich sein.

KI-Disclaimer

Einige Abschnitte dieser wissenschaftlichen Arbeit wurden mithilfe von künstlicher Intelligenz (KI) erstellt. Die KI basiert auf den fortschrittlichen Textgeneratoren Deepl-WriteAI, OpenAI GPT-4 und -3.5, die darauf trainiert wurden, menschenähnliche Texte zu generieren. Daher wurden die erstellten Texte von einem Menschen überprüft und ggf. angepasst.

Die KI ist in der Lage, konsistente und relevante Inhalte zu erzeugen, jedoch kann die Richtigkeit und Vollständigkeit nicht garantiert werden. Die von KI generierten Abschnitte wurden sorgfältig von den Autoren der Arbeit überprüft und gegebenenfalls korrigiert oder angepasst, um sicherzustellen, dass sie den wissenschaftlichen Standards entsprechen und zum Gesamtkontext der Arbeit passen.

Die Autoren übernehmen die Verantwortung für mögliche Fehler oder Mängel, die auf die Verwendung von KI in dieser Arbeit zurückzuführen sind.

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

CERT	.....	*Computer Emergency Response Team*
CIO	.....	*Chief Information Officer*
CMT	.....	*Crisis Management Team*
CSIRT	.....	*Computer Security Incident Response Team*
IDS	.....	*Intrusion-Detection-System*
IoC	.....	*Indicators of Compromise*
IoT	.....	*Internet of Things*
IR	.....	*Incident Response*
NIST	.....	*National Institute of Standards and Technology*

Einleitung

«Chain of Custody» und «Incident Response» sind Begriffe, die jedem aus dem täglichen Leben bekannt sind. Sie werden in verschiedenen Formen und Bereichen verwendet, wie z.B. die Beweiskette bei der polizeilichen Beweisführung oder die Notfallreaktion in Krankenhäusern. Im Buch «Implementierung der Chain of Custody in Incident Response Situationen» untersuchen wir, wie diese beiden Konzepte in Bezug auf die Cybersicherheit zusammenhängen.

Das Buch ist in fünf umfassende Kapitel unterteilt, die die verschiedenen Facetten der Chain of Custody in Incident-Response-Szenarien beleuchten. Das erste Kapitel bietet einen Einblick in die Grundprinzipien und die Relevanz der Chain of Custody. Im zweiten Kapitel werden die Herausforderungen und Methoden bei der Implementierung eines Chain of Custody besprochen. Das dritte Kapitel beschäftigt sich mit dem Incident-Response-Prozess mit dem Schwerpunkt auf der Rolle der Incident-Response-Prozess in der IT-Forensik. Im vierten Kapitel werden die operationellen Einschränkungen und Entscheidungskriterien im Incident-Response-Prozess behandelt. Schliesslich gibt das fünfte Kapitel eine Perspektive auf zukünftige Entwicklungen und potenzielle Verbesserungen im Bereich der Chain of Custody in Incident Response.

Das Werk «Implementierung von Chain of Custody in Incident Response Situationen» vermittelt ein tiefes Verständnis für die Chain of Custody und ihre kritische Rolle in der Incident Response. Durch die ausgewogene Kombination aus theoretischen Grundlagen und praxisbezogenen Anleitungen bieten sich wertvolle Erkenntnisse und es dient als umfassender Leitfaden zur Verbesserung der Sicherheitspraktiken in Organisationen. Es betont die Bedeutung einer robusten Chain of Custody, um nicht nur Sicherheitsvorfälle effektiv abzuwehren, sondern auch forensisch nachvollziehbar zu untersuchen und darauf zu reagieren.

Insgesamt erfordert die effektive Anwendung des in diesem Buch vermittelten Wissens eine kontinuierliche Anpassung und Weiterbildung in den Bereichen IT-Sicherheit, rechtliche Rahmenbedingungen und forensische Technologien. Dadurch können Organisationen nicht nur auf aktuelle Bedrohungen reagieren, sondern sich auch auf zukünftige Entwicklungen vorbereiten und ihre Resilienz in einer sich ständig wandelnden digitalen Welt stärken.

Implementation von Chain of Custody in Incident-Response-Situationen

1. Bedeutung der Chain of Custody in der IT-Forensik

Vorgelegt von: Özsoy Derya

Abstract

Dieses Kapitel befasst sich eingehend mit der grundlegenden Bedeutung der Chain of Custody in der IT-Forensik. Es erläutert nicht nur die Struktur und den Aufbau digitaler Beweismittel, sondern geht auch ausführlich auf das Verfahren ein, mit dem sichergestellt wird, dass diese Beweismittel vor Gericht als zulässig angesehen werden. Dieses Kapitel verdeutlicht die Notwendigkeit, eine sorgfältige Beweissicherung durchzuführen und beschreibt die erforderlichen Schritte. Die gründliche Untersuchung von Cyber-Angriffen erfolgt mit Hilfe spezialisierter forensischer Analysewerkzeuge und -techniken. Durch die genaue Dokumentation und die Einhaltung der Chain of Custody wird nicht nur die lückenlose Nachvollziehbarkeit der Beweiskette gewährleistet, sondern auch die rechtliche Zulässigkeit vor Gericht sichergestellt.

1.1. Einleitung

In unserer Zeit der zunehmenden Digitalisierung gewinnt das Konzept der «Chain of Custody» in der IT-Forensik immer mehr an Bedeutung. Der Schwerpunkt liegt dabei auf der lückenlosen Beweissicherung digitaler Spuren. Dies ist in einer Welt, in der elektronische Beweismittel oft der Schlüssel zu erfolgreichen kriminalistischen Ermittlungen sind, von entscheidender Bedeutung. Dabei geht es nicht nur um die Überwachung aller Aspekte digitaler Spuren, sondern auch um die Sicherstellung, dass jeder Schritt von der Entdeckung bis zur Übergabe genau verfolgt und detailliert dokumentiert wird. In diesem Zusammenhang ist die Gewährleistung der Integrität, Authentizität und Unveränderbarkeit der Daten von entscheidender Bedeutung.

Dieses Kapitel gibt einen Überblick über die grundlegende Bedeutung der Beweismittelkette in der IT-Forensik. In der Einführung wird gezeigt, welche zentrale Rolle dieses Konzept spielt, um die Verlässlichkeit von digitalem Beweismaterial in verschiedenen rechtlichen und forensischen Kontexten zu gewährleisten.

Ziel ist es, ein vertieftes Verständnis der komplexen und kritischen Beweissicherungsprozesse im digitalen Zeitalter zu erlangen. Vor allem die Sicherstellung der Integrität digitaler Beweismittel stellt eine Herausforderung in der IT-Forensik dar. Dies gilt insbesondere in einem Umfeld vielfältiger Akteure und Systeme. Die zunehmende Vernetzung und die Vielfalt der Datenquellen erschweren eine lückenlose Nachverfolgung. Einheitliche Standards und Protokollierungsmethoden sind daher für die Sicherung und den Transfer von Beweismitteln von entscheidender Bedeutung.

Angesichts der raschen technologischen Entwicklung ist es notwendig, die Effizienz der Chain of Custody durch ständige Anpassung an neue Technologien, Zusammenarbeit zwischen den verschiedenen Akteuren und strikte Einhaltung der Standards zu gewährleisten.

1.2. Chain of Custody

Die Chain of Custody oder Beweismittelkette, Überwachungskette ist in der Forensik und in Ermittlungsverfahren von entscheidender Bedeutung. Dabei handelt es sich um eine detaillierte Dokumentation, die die gesamte Abfolge der Aufbewahrung, Kontrolle, Übertragung, Analyse und Verfügbarkeit von physischen oder elektronischen Beweismitteln im rechtlichen Kontext umfasst (Badiye et al., 2023).

Diese Kette stellt die Integrität, Authentizität und Glaubwürdigkeit vor Gericht sicher. Jeder Schritt wird genau dokumentiert, um Manipulationen oder Veränderungen des Beweismaterials zu verhindern (Badiye et al., 2023).

Der Dokumentationsprozess erstreckt sich über den gesamten Zeitraum bis zur Wiederherstellung der Daten. Die Aufbewahrung der Beweismittel folgt strengen Richtlinien, um ihre Integrität zu gewährleisten. Ein benannter Verwahrer trägt die Verantwortung und dokumentiert die ordnungsgemässe Aufbewahrung durch die Unterschriften aller Beteiligten (Badiye et al., 2023).

Die Überprüfung der Beweismittel ist von entscheidender Bedeutung, um ihre Richtigkeit zu gewährleisten. Es werden genaue Methoden angewandt, um Fälschungen zu verhindern und sicherzustellen, dass die Beweismittel die Tatsachen wiedergeben (Badiye et al., 2023).

Die Übergabe der Beweismittel erfolgt unter genauer Protokollierung und erfordert die Unterschriften aller Beteiligten. Diese sorgfältige Handhabung reduziert das Risiko von Fehlern oder Manipulationen durch Polizei, Labore oder Gerichtsbeamte (Badiye et al., 2023).

1.3. Ablauf einer Chain of Custody

Die Sicherstellung eines digitalen Beweismittels und vollständigen Rückverfolgbarkeit ist ein grundlegender Bestandteil in einem Ermittlungsprozess. Die Ermittler oder Personen, welche für die digitalen Beweismittel verantwortlich sind, sind verpflichtet, die Beweise und die dazugehörigen Formulare der Überwachungskette vollständig auszufüllen. Diese Dokumentation stellt die Zuverlässigkeit der gesammelten Beweismittel dar.

Jede Probe wird beschriftet und mit einem Etikett versehen. Es enthält den Identifizierungscode, die Ortsangabe, das genaue Datum und die Uhrzeit der Probenahme sowie die Namen und Unterschriften der Personen, die die Probenahme durchgeführt haben, und die Unterschriften der Zeugen. Diese genaue Dokumentation trägt dazu bei, die Transparenz und die Verlässlichkeit der gesammelten Beweise zu erhöhen (Badiye et al., 2023).

1.3.1. Verpackung

Es ist wichtig, Beweismittel im Ermittlungsverfahren angemessen zu verpacken, um jeglicher Art der Beschädigung zu verhindern. Dies erfolgt durch manipulationssichere Beutel, Bänder oder digitale Versiegelungstechnologien (Badiye et al., 2023):

- Die Daten dürfen nicht auf einem Computer oder einem anderen Datenträger hinzugefügt, geändert oder gelöscht werden.

- Hohe Temperaturen, Feuchtigkeit, Erschütterungen, elektrische Entladungen und magnetische Quellen sind zu vermeiden.
- Es sollte sichergestellt werden, dass die Beweismittelkette für elektronische Beweise lückenlos ist und dass die Dokumentation über Verpackung, Transport und Lagerung ordnungsgemäss geführt wird.

1.3.2. Transport

Um die Unversehrtheit der Beweismittel während des Transports zu gewährleisten, müssen bestimmte Verfahren und Vorsichtsmassnahmen eingehalten werden. Bei magnetischen Einflüssen und elektronischen Beweismitteln ist besondere Vorsicht geboten. (Jansen & Ayers, 2004) Diese Anforderungen werden im Folgenden näher erläutert:

- Magnetische Einflüsse, wie z. B. Funkübertragungen, Lautsprecher vermeiden.
- Extrem hohe oder niedrige Temperaturen sowie hoher Luftdruck beim Transport vermeiden.
- Stösse und Vibrationen auf ein Minimum reduzieren.

1.3.3. Lagerung

Die korrekte Aufbewahrung von Beweisen ist entscheidend für deren Integrität und Beweiskraft. Nachfolgend sind einige zusätzliche Verfahren zur Beweissicherung aufgeführt (Jansen & Ayers, 2004):

- Das Beweismaterial muss den entsprechenden Richtlinien entsprechen.
- Das Beweismaterial ist an einem sicheren Ort, fern von extremen Temperaturen und Feuchtigkeit zu lagern.
- Das Beweismaterial muss vor magnetischen Quellen, Feuchtigkeit, Staub und anderen schädlichen Partikeln oder Verunreinigungen geschützt werden.

1.3.4. Formular

Für jedes Beweismittel ist ein separates Formular erforderlich, das mindestens diese Informationen enthalten muss, damit das Beweismittel akzeptiert werden kann (Badiye et al., 2023):

- Eindeutige Kennung
- Name und Unterschrift des Probenehmers
- Offizielle Adresse und Kontaktnummer
- Name des Empfängers
- Anschrift des Labors
- Einzelheiten zu jeder Probe, einschliesslich:
    - Eindeutige Kennung und Matrix
    - Datum und Uhrzeit der Entnahme
    - Art der gewünschten Analyse
- Unterschriften aller an der Besitzkette Beteiligten mit Datum und Uhrzeit
- Datum und Art der Lieferung
- Autorisierung für die Analyse der Probe
- Sonstige Informationen über die Probe

Änderungen am Beweismittel müssen sorgfältig auf dem Überwachungsketten-Formular dokumentiert werden. Das Formular ist mit rechtsverbindlicher Unterschrift, Datum und genauer Uhrzeit der Änderung zu versehen. Die formelle Inverwahrungnahme erfolgt erst durch die zuständige Person nach sicherer und ordnungsgemässer Lagerung. Dieser entscheidende Vorgang gewährleistet den geschützten Zustand der Beweismittel, um mögliche Beeinträchtigungen zu verhindern und ihre Verwendbarkeit vor Gericht zu sichern (Badiye et al., 2023).

1.3.5. Beweismittel in physischer oder digitaler Form

Die ordnungsgemässe Behandlung von Computerbeweisen, ob in physischer oder digitaler Form, ist für die Erhaltung ihrer Beweiskraft von entscheidender Bedeutung. Dazu gehört auch die Wiederherstellung von nicht elektronischen Beweismitteln, die von unschätzbarem Wert sein können. Beispiele hierfür sind schriftliche Passwörter, handschriftliche Notizen, leere Papierblöcke mit eingerücktem Text, Hardware- und Software-Handbücher, Kalender, Literatur, Computerausdrucke in Textform oder als Grafik sowie Fotos (Jansen & Ayers, 2004).

Die Erhaltung der Beweiskraft erfordert einen sorgfältigen Umgang mit physischen Beweismitteln. Bei schriftlichen Passwörtern und handschriftlichen Notizen ist es von entscheidender Bedeutung, dass sie in unverändertem Zustand gesichert werden. Die Erhaltung der Unversehrtheit von leeren Papierblöcken mit eingerückter Schrift erfordert eine sorgfältige Handhabung, um Abdrücke oder Zusätze zu vermeiden (Jansen & Ayers, 2004).

Hardware- und Softwarehandbücher können wichtige Informationen über die Funktionsweise von Systemen enthalten und sollten daher an einem sicheren Ort aufbewahrt werden. Kalender können zeitliche Zusammenhänge liefern, während Literatur und Computerausdrucke in textlicher oder grafischer Form zusätzliche Unterstützung bieten (Jansen & Ayers, 2004).

Die Erstellung klarer und detaillierter Protokolle während des Wiederherstellungsprozesses ist unerlässlich. Dazu gehören genaue Angaben über Ort, Zeit und beteiligte Personen, um die Nachvollziehbarkeit und Glaubwürdigkeit der Beweise zu gewährleisten (Jansen & Ayers, 2004).

Insgesamt ist die professionelle Handhabung und Wiederherstellung von nicht elektronischen Beweismitteln von entscheidender Bedeutung, um sicherzustellen, dass sie vor Gericht als zuverlässige und unverfälschte Beweismittel verwendet werden können (Jansen & Ayers, 2004).

1.4. Wie wird die Chain of Custody für digitale Beweismittel gewährleistet?

Grundvoraussetzung für eine erfolgreiche forensische Analyse ist die sichere Aufbewahrung von digitalen Beweismitteln. Dabei ist es entscheidend, die Unversehrtheit (Integrität) und Echtheit (Authentizität) der digitalen Beweismittel sicherzustellen. Zunächst werden die digitalen Beweismittel auf ihre Integrität und Authentizität überprüft. Der nächste Schritt besteht darin, das gesamte Speichermedium physisch auszulesen. Dabei kann es sich um eine

exakte Kopie des Datenträgers oder um einen Klon logischer Dateien wie Dokumente, E-Mails vom Mailserver, Auszüge aus bestimmten Programmen, Datenbanken oder Netzlaufwerken handeln.

Nach dem Auslesen der Daten ist die Berechnung und Speicherung eines Hash-Wertes der gesicherten Daten erforderlich. Hierzu werden gängige Hash-Algorithmen wie MD5, SHA1 oder SHA256 verwendet. Es ist jedoch zu beachten, dass die Verwendung von MD5 und SHA1 vermieden werden sollte. Diese gelten als nicht mehr kollisionsresistent. Den Hash-Wert zu berechnen und zu speichern, dient der weiteren Sicherstellung der Integrität und Unveränderbarkeit des ursprünglich gesicherten Nachweises.

Um zu gewährleisten, dass die forensische Analyse der Daten ohne jegliche Beeinträchtigung durchgeführt werden kann, wird die forensische Analyse ausschliesslich auf dem erstellten Klon durchgeführt. Dieser Schritt ist von entscheidender Bedeutung für die Vermeidung von möglichen Veränderungen oder Manipulationen, die bei einer direkten Analyse des Originals auftreten könnten und somit eine Erschwerung der Ermittlungen zur Folge hätten.

Die Verwendung dieses Klonansatzes stellt sicher, dass die Ergebnisse der forensischen Analyse zuverlässig sind und als Beweismittel vor Gericht verwendet werden können. Gleichzeitig bleibt das ursprüngliche Beweismittel unverändert und intakt, sodass die Authentizität und Integrität des Beweismittels nach wie vor gewährleistet ist. Diese sorgfältigen Schritte sind unerlässlich, um eine rechtsgültige forensische Untersuchung zu ermöglichen und gleichzeitig sicherzustellen, dass die Originaldaten intakt bleiben (Trebo & Meier, 2023).

1.5. Arten der Techniken zur Unterstützung der Chain of Custody

Die Metadatenanalyse bezieht sich auf die in einer Datei enthaltenen Informationen wie Erstellungsdatum und Standort des Geräts. In der forensischen Bild-/Dokumentenanalyse werden Techniken wie Pixelanalyse und Wasserzeichenerkennung eingesetzt, um die Authentizität zu überprüfen und Manipulationen aufzudecken. Gesichtserkennung wird zur Aufklärung von Verbrechen eingesetzt, indem Gesichter auf Bildern mit Datenbanken abgeglichen werden. Deep-Learning-Technologien wie künstliche neuronale Netze erleichtern die Mustererkennung, insbesondere bei der Gesichtserkennung, durch Training mit unterschiedlichen Datensätzen. Kontinuierliche Verbesserungen werden durch die Erweiterung der Datensätze oder die Anpassung der Netzwerkarchitektur erreicht (Trebo & Meier, 2023).

1.5.1. Sicherung der Chain of Custody durch technisches Mitteln

Ein wichtiger Aspekt der forensischen Untersuchung ist die sorgfältige Beweisanalyse. Zur Erhaltung der Unversehrtheit der Beweise und zur Gewährleistung einer zuverlässigen Rückverfolgbarkeit der Chain of Custody ist eine Vielzahl von technischen Hilfsmitteln im Einsatz. Die Sicherung einer Chain of Custody wird in Kapitel 2 näher erläutert.

1.5.2. Datensicherheit

Die Datensicherheit umfasst Massnahmen zum Schutz vor unbefugtem Zugriff, unbefugter Veränderung oder Vernichtung digitaler Daten. Dazu werden Methoden wie Zugangskontrolle, Verschlüsselung, Authentifizierung, Firewalls und Schulungen eingesetzt.

Die Einhaltung von Datenschutzbestimmungen ist notwendig, um Cyberangriffe und Datenverluste zu verhindern. Ausserdem muss die Verlässlichkeit von Beweismitteln in der Forensik gewahrt und Datenschutzverletzungen vermieden werden (IBM, 2023).

1.5.3. Datenintegrität

Die Datenintegrität gewährleistet die Genauigkeit, die Konsistenz und die Sicherheit der Daten. Massnahmen wie Validierung, Sicherung und Redundanz von Daten sind für die Einhaltung vordefinierter Regeln unerlässlich. Techniken wie Hashing, Prüfsummen und Audit Trails werden verwendet, um Datenverfälschungen zu erkennen und zu verhindern. Dies ermöglicht fundierte Entscheidungen und schützt vor Datenproblemen wie Korruption und Betrug (Buckbee, 2023).

1.5.4. Fotografien / Screenshots

Fotografien, Screenshots, Write-Blocker, Imaging und Datenkopien sichern die Chain of Custody (Obbayi, 2019). Memory Capture erfasst flüchtige Informationen. Dabei werden Risiken und Nutzen abgewogen (Michael, 2020). Hashing, z.B. mit SHA-256, sichert die Authentizität von Daten. Es ermöglicht die Überprüfung von Beweisen in der Forensik (Bouam et al., 2021). Fuzzy Hashing identifiziert nahezu identische Dateien durch syntaktische Ähnlichkeiten und ist besonders nützlich bei sich verändernder Malware (Sarantinos et al., 2016).

1.6. Welche Gesetze gibt es in der Schweiz für die Chain of Custody?

Im Gegensatz zu den Vereinigten Staaten von Amerika (USA) ist die Verwendung oder Einführung von Beweismitteln in der Schweiz kaum gesetzlich geregelt. Nach Art. 139 Abs. 1 der Schweizer Strafprozessordnung müssen die vor Gericht vorgebrachten Beweise den gesetzlichen Anforderungen entsprechen und sich auf Wissenschaft und Erfahrung stützen. Dabei gilt der Grundsatz der freien Beweiswürdigung nach Artikel 10 Abs. 2. Nur wenn die Beweismittel ordnungsgemäss versiegelt und aufbewahrt wurden und keine Anzeichen einer Manipulation erkennbar sind, ist die Zulässigkeit der Beweise vor Gericht gewährleistet.

Eine Einschränkung dieses Grundsatzes ist jedoch durch die Bestimmungen über die Beweissicherung nach Art. 196 lit. a StPO möglich, die dem Schutz öffentlicher und privater Interessen dienen. Sollte die Anordnung der Beweissicherung (Art. 196 lit. a StPO) den Strafverfolgungsbehörden Schwierigkeiten bereiten, sind sie berechtigt, Zwangsmassnahmen gemäss den Bestimmungen der Art. 196-298 StPO zu ergreifen. Es ist daher von entscheidender Bedeutung, dass die Beweissicherung in Übereinstimmung mit den gesetzlichen Bestimmungen erfolgt, um die Rechtmässigkeit und Zulässigkeit der Beweismittel vor Gericht zu gewährleisten (Meier, 2020).

Unter Zwangsmassnahmen sind verfahrensleitende Massnahmen der Strafbehörden zu verstehen, die in die Grundrechte der Betroffenen eingreifen und in erster Linie dem Zweck der Strafverfolgung dienen. Ziel dieser Massnahmen ist die Aufklärung von Straftaten nach Massgabe der gesetzlichen Bestimmungen und die Wahrung der Integrität des gerichtlichen Verfahrens. Es handelt sich dabei um gesetzlich sanktionierte Eingriffe, die in besonderen Situationen zur Gewährleistung einer effektiven Strafverfolgung vorgenommen werden.

Dabei ist darauf zu achten, dass ein Ausgleich zwischen dem öffentlichen Interesse an der Strafverfolgung und den Grundrechten des Einzelnen gewahrt bleibt.

Es ist wichtig zu betonen, dass Zwangsmassnahmen innerhalb eines klaren rechtlichen Rahmens angewendet werden sollten. Dabei ist der Grundsatz der Verhältnismässigkeit zu beachten. Auf diese Weise wird sichergestellt, dass die Eingriffe gerechtfertigt und notwendig sind, um die strafrechtlichen Ermittlungen voranzubringen, ohne dass es zu einem unverhältnismässigen Eingriff in die Grundrechte und -freiheiten des Einzelnen kommt (Meier, 2020).

Zweck der Strafverfolgung:

- Beweise zu sichern
- die Anwesenheit von Personen im Verfahren sicherzustellen
- die Vollstreckung der Entscheidung zu gewährleisten

Für die IT-Forensiker ist es bedeutsam, die Beweissicherung nach den geltenden Regeln der Technik zu handeln. Die internationalen Standards wurden durch die Normen ISO/ IEC 27037: 2012 festgelegt (Meier, 2020).

1.7. Herausforderungen bei der Umsetzung der präventiven Methoden / Techniken

Aufgrund unterschiedlicher Rahmenbedingungen und Geschäftsmodelle stehen Ermittler und Experten im Bereich der digitalen Forensik vor vielfältigen Herausforderungen. Besonders deutlich werden diese Unterschiede bei der Unterscheidung zwischen Strafverfolgungsbehörden und privaten Akteuren (Prayudi & SN, 2015).

Die Rahmenbedingungen für digitale forensische Untersuchungen variieren stark und beeinflussen die Vorgehensweise bei Sicherung, Handhabung und Analyse von Beweismitteln. Insbesondere die Kriterien zur Aufbewahrung differenzieren sich erheblich, wobei Strafverfolgungsbehörden oft spezifische Vorschriften haben, die von privaten Forensik Standards abweichen können. Effizienz, Sicherheit und die Einhaltung gesetzlicher Vorschriften stehen dabei im Mittelpunkt. Die Speicherung und Klassifizierung von Produkten verschiedener Hersteller stellt zusätzlich eine Herausforderung dar (Prayudi & SN, 2015).

In der privaten Forensik werden unterschiedliche Technologien und Produkte verschiedener Hersteller eingesetzt, wobei individuelle Präferenzen oder Unternehmensrichtlinien eine Rolle spielen können. Strafverfolgungsbehörden müssen möglicherweise spezielle Produkte einsetzen, die den Standards der Behörden entsprechen. Die Einführung von Speichermodellen wie NAS und SAN stellt eine zusätzliche Herausforderung dar. Die Art und Weise, wie digitale Beweismittel gespeichert und verwaltet werden, wirkt sich direkt auf die Effizienz forensischer Untersuchungen aus. Private Akteure sind bei der Auswahl und Implementierung solcher Modelle flexibler, während Strafverfolgungsbehörden durch staatliche Vorgaben oder Budgetbeschränkungen auf bestimmte Modelle beschränkt sein können (Prayudi & SN, 2015).

Die Vielfalt der Rahmenbedingungen und Geschäftsmodelle in der digitalen Forensik unterstreicht die Notwendigkeit einer umfassenden Anpassung an die spezifischen Anforderungen der einzelnen Institutionen. Dies ist entscheidend, um die Integrität und Effizienz forensischer Untersuchungen zu gewährleisten (Prayudi & SN, 2015).

1.7.1. Network Attached Storage (NAS):

Ermöglicht mehreren Benutzern die Speicherung und gemeinsame Nutzung von Dateien in einem TCP/IP-Netzwerk über WiFi oder Ethernet-Kabel. Es bietet eine strukturierte Plattform für die Verwaltung von Dateien und fördert die Zusammenarbeit zwischen den Benutzern. Die Benutzer können von verschiedenen Geräten aus auf ihre Daten zugreifen (IBM, 2023).

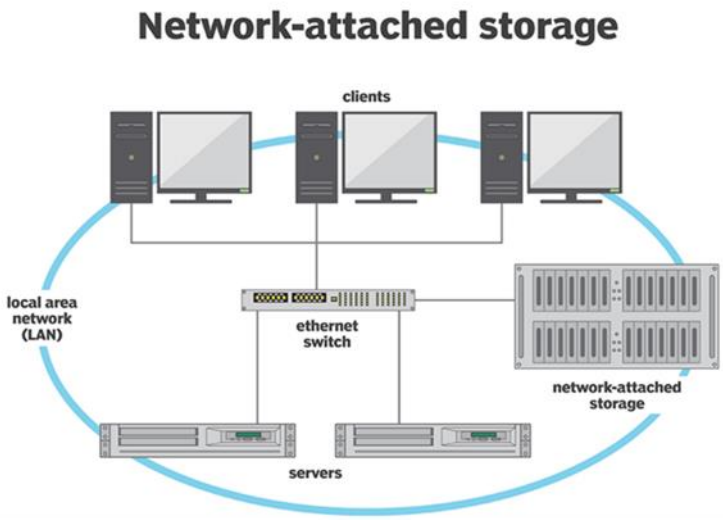

Abbildung 1 – NAS (TechTarget, 2023)

1.7.2. Storage Area Network (SAN):

Ist eine massgeschneiderte Infrastruktur, die für eine bestimmte Umgebung entwickelt wurde. Sie bietet eine Optimierung für die spezifischen Anforderungen mit integrierten Servern, Speichersystemen, Netzwerk-Switches, Software und Dienste (IBM, 2023).

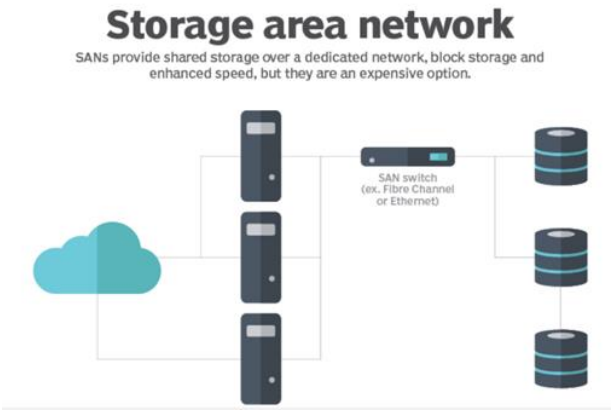

Abbildung 2 – SAN (TechTarget, 2023)

1.7.3. Eine sichere Infrastruktur:

Digitale Forensik und eine sichere Beweiskette erfordern eine robuste Infrastruktur, insbesondere im Hinblick auf die Mobilität der Ermittler. Ein Secure Sockets Layer (SSL) Virtual Private Networks (VPNs) Konzept mit Trusted Computing und Access Control gewährleistet den sicheren Zugriff auf Server und Speicher. Die nahtlose Integration von SSL-VPN und Trusted Computing ist aufgrund ihrer Komplexität eine aktuelle Herausforderung (Prayudi & SN, 2015).

Entscheidend ist ein umfassendes Framework für das Management der digitalen Langzeitarchivierung. Dieses bietet Lösungen von der Speicherung bis zur Archivierung digitaler Beweismittel und regelt das Zusammenspiel in einer Beweiskette. Besonderes Augenmerk liegt auf der Sicherstellung der Integrität, Authentizität und Unveränderbarkeit digitaler Beweismittel (Prayudi & SN, 2015).

SSL-VPN, Trusted Computing und ein effizientes Langzeitarchivierungs-Framework zu kombinieren, bietet eine stabile Grundlage für forensische Untersuchungen. Dieser Ansatz gewährleistet einen sicheren Zugriff auf digitale Beweismittel und eine vertrauenswürdige Verwaltung über den gesamten Lebenszyklus (Prayudi & SN, 2015).

1.8. Schlussfolgerung

Die «Chain of Custody» ist entscheidend in forensischer Wissenschaft und Ermittlungen, da sie Integrität, Authentizität und Glaubwürdigkeit der Beweise sicherstellt. Die detaillierte Dokumentation umfasst Aufbewahrung, Kontrolle, Übertragung, Analyse und Verfügbarkeit von Beweismaterial, um Manipulation zu verhindern.

Strikte Einhaltung von Aufbewahrungsvorschriften und die Benennung eines Verwahrers, der von allen Beteiligten durch Unterschrift bestätigt wird, sind essenziell. Die gerichtliche Verwertbarkeit erfordert präzise Überprüfungsmethoden. Protokollierung und Unterschrift bei Übergabe reduzieren Risiken von Fehlern oder Manipulationen.

Dieser umfassende Dokumentationsprozess gewährleistet Zuverlässigkeit und Unwiderlegbarkeit der Beweise. Die schweizerische Strafprozessordnung betont die Bedeutung ordnungsgemäßer Beweissicherung. Innovative Technologien wie Metadatenanalyse, forensische Bild- und Dokumentenanalyse sowie Gesichtserkennung und Deep Learning erhöhen die Sicherheit und Authentizität von Beweisen.

Eine sichere Infrastruktur und Einhaltung internationaler Standards wie ISO/IEC 27037:2012 sind in der digitalen Forensik entscheidend. Präzise Protokollierung und professioneller Umgang mit Beweismitteln in der «Chain of Custody» gewährleisten einen rechtskonformen Beitrag zur Aufklärung von Straftaten.

1.9. Literaturverzeichnis

Badiye, A., Kapoor, N., & G. Menezes, R. (2023, February 13). *Chain of Custody.* Europe PMC. https://europepmc.org/article/nbk/nbk551677

Bouam, M., Bouillaguet, C., Delaplace, C., & Noûs, C. (2021). *Computational Records with aging hardware: Controlling half the output of SHA-256.* Parallel Computing, 106, 102804. https://doi.org/10.1016/j.parco.2021.102804

Buckbee, M. (n.d.). *Datenintegrität : Was ist das und wie ist sie aufrecht zu erhalten?.* Varonis. https://www.varonis.com/de/blog/datenintegritat-was-ist-das-und-wie-ist-sie-aufrecht-zu-erhalten, Aufgerufen am 19.11.2023.

IBM. (n.d.). *Was ist datensicherheit? definition von Datensicherheit und übersicht.* https://www.ibm.com/de-de/topics/data-security, Aufgerufen am 19.11.2023.

IBM. (n.d.). *Was ist ein storage area network (SAN)?* San-definiert. IBM. https://www.ibm.com/de-de/topics/storage-area-network

IBM. (n.d.). *Was IST network attached storage (NAS)?* https://www.ibm.com/de-de/topics/network-attached-storage

Jansen, W., & Ayers, R. (2004). 34-38. In *Guidelines on PDA forensics: Recommendations of the National Institute of Standards and Technology* (pp. 1–67). essay, Computer Security Division, Information Technology Laboratory.

Meier, D. (2020, June 29). *Vorgehen eines it-forensikers und Deren Ethischen Grundsätze sowie die beweisverwertbarkeit der Erstellten Analysen in der Schweiz und EU.* Wirtschaftsinformatik reloaded. https://www.fhnw.ch/plattformen/iwi/2020/06/24/homeoffice-und-onlinekonferenzen-4-9-2-3-2-12/%C2%A0

Michael J., H. (2020). *The importance of volatile computer memory evidence, the tradeoffs between acquiring potential evidence from volatile memory on a running computer, and the defense perspective.* Computer and Internet Lawyer. https://www.proquest.com/docview/2523185919/fulltextPDF/56625A661CBF453FPQ/1?accountid=169375

Obbayi, L. (2019, July 6). *Computer forensics: Chain of custody* [updated 2019]. Infosec. https://resources.infosecinstitute.com/topics/digital-forensics/computer-forensics-chain-custody/, Aufgerufen am 19.11.2023.

Prayudi, Y., & SN, A. (2015). International Journal of Computer Applications. *Digital Chain of Custody: State of the Art, 1–10.* https://doi.org/10.5120/19971-1856

Sarantinos, N., Benzaid, C., Arabiat, O., & Al-Nemrat, A. (2016). *Forensic malware analysis: The value of fuzzy hashing algorithms in identifying similarities.* 2016 IEEE Trustcom/BigDataSE/ISPA. https://doi.org/10.1109/trustcom.2016.0274

Strafprozessordnung (stpo). Schweizerische Strafprozessordnung. (2007, October 5). https://www.rhf.admin.ch/rhf/de/home/strafrecht/rechtsgrundlagen/national/sr-312-0.html

Trebo, M., & Meier, R. (2023, June 15). *Aufdecken digitaler Beweise Durch Dokumentenanalyse*. Analyse von Bildern und Dokumenten. https://www.scip.ch/?labs.20230615

Implementation von Chain of Custody in Incident-Response-Situationen

2. Technische Möglichkeiten und Herausforderungen zur Einhaltung der Chain of Custody

Vorgelegt von: Böller Jonas

Abstract

In Kapitel 2 werden die technischen Massnahmen und Herausforderungen erörtert, die für die Aufrechterhaltung der Chain of Custody essenziell sind. Dabei liegt der Fokus auf der Sicherstellung, dass Daten weder versehentlich noch böswillig verändert werden. Dies umfasst die Diskussion verschiedener Technologien und Methoden, wie Write-Blocker und Hashing-Techniken, die zur Beweissicherung eingesetzt werden. Zudem werden die Herausforderungen in Bezug auf moderne IT-Umgebungen und Cloud-Systeme beleuchtet.

2.1. Einleitung

Digitale Beweismittel, die im Zusammenhang mit einem Vorfall von Bedeutung sein könnten, müssen gesichert werden. Wenn Beweismittel auf falsche Weise gesichert oder überhaupt nicht gesichert werden, wird die Integrität und Authentizität dieser Beweismittel infrage gestellt. Vor Gericht können diese Beweismittel dann nicht mehr verwendet werden. Daher ist es wichtig, die richtigen technischen Werkzeuge anzuwenden, die es dem Experten ermöglichen, zu beweisen, dass nichts an den Beweismitteln verfälscht oder gelöscht wurde. In der heutigen Zeit wird es immer schwieriger, technische Prozesse einzuhalten, da sich die Technik ständig verändert oder sogar neu erfunden wird. Dies birgt Herausforderungen und erfordert eventuell Kompromisse. Ziel dieses Kapitels ist es aufzuzeigen, welche Technologien zur Einhaltung der Chain of Custody eingesetzt werden und welche Herausforderungen damit verbunden sind.

Im ersten Teil des Kapitels werden technische Mittel zur Einhaltung der Chain of Custody vorgestellt.

Im zweiten Teil werden technische Möglichkeiten zur Dokumentation der Chain of Custody gezeigt. Es genügt nämlich nicht nur, die Daten zu sichern und richtig zu behandeln. Es muss dokumentiert werden, wie sie gesichert wurden, wer darauf Zugriff hatte und vieles mehr.

Im dritten Abschnitt werden Beispiele aufgeführt, die eine Herausforderung darstellen und die Komplexität der Chain of Custody aufzeigen.

Im vierten und letzten Abschnitt wird ein kurzer Blick in die Zukunft geworfen. Es wird ein mögliches Beispiel genannt, das in Zukunft interessant werden könnte, um die Chain of Custody technisch zu realisieren.

2.2. Technische Möglichkeiten die Chain of Custody zu sichern

Welche technischen Mittel und Bedingungen gibt es, die es Forensiker erlauben Beweismittel zu untersuchen und in der Chain of Custody helfen, die Integrität der Beweismittel zu behalten.

2.2.1. Datensicherheit

Datensicherheit umfasst Massnahmen zur Gewährleistung des Schutzes digitaler Daten vor unautorisiertem Zugriff, Änderung oder Zerstörung. Dazu gehören passende Methoden zur Zugangskontrolle, Verschlüsselung, Authentifizierung, Implementierung von Firewalls und Intrusion-Detection-Systemen sowie Sicherheitsrichtlinien, Datensicherungen und Schulungen für Mitarbeiterinnen und Mitarbeiter (IBM, 2023). Die Einhaltung von Datenschutzvorschriften und die Vermeidung von Datenschutzverletzungen sind entscheidende Aspekte, die in der Forensik und so auch in der Chain of Custody eine Rolle spielen. Sie schützt vor Gefahren wie Cyberangriffen und Datenverlusten und tragen dazu bei, das Vertrauen und die Integrität der Beweismittel zu bewahren.

2.2.2. Datenintegrität

Bei der Datenintegrität geht es darum, die Genauigkeit, Konsistenz und Sicherheit von Daten während ihres gesamten Lebenszyklus zu gewährleisten. Hierzu gehört die einwandfreie Pflege der Daten, welche vordefinierten Regeln entsprechen. Zu den wichtigsten Massnahmen für die Datenintegrität gehören Datenvalidierung, Sicherheit und Redundanz (Buckbee, 2023). Die Erkennung und Verhinderung von Datenverfälschungen oder unbefugten Änderungen ist von entscheidender Bedeutung. Techniken wie Hashing, Prüfsummen und Audit Trails werden häufig zur Wahrung der Datenintegrität eingesetzt. Die Datenintegrität hilft begründete Entscheidungen treffen zu können, die Zuverlässigkeit des Systems zu gewährleisten und sich vor datenbezogenen Problemen wie Korruption und Betrug zu schützen.

2.2.3. Fotografie / Screenshots

Ein erster Schritt, der einfach klingt, aber die Chain of Custody auf technischer Ebene absichern kann, sind einfache Fotografien oder Screenshots der Beweismittel (Obbayi, 2019). So können mögliche Verstösse bildlich nachgewiesen werden, ohne dass die Originaldaten verändert werden müssen. Dies kann vor allem bei laufenden Systemen sinnvoll sein.

2.2.4. Write-Blocker

Wo immer es möglich ist, wird davon abgeraten, mit den Originaldaten zu arbeiten, da dies unvermeidlich zu einer Veränderung der Daten führt. Damit ist nicht nur das externe Auslesen eines Datenträgers gemeint. Gemeint sind auch ganze Systeme. Beispielsweise das Benutzen eines für den Vorfall relevanten Rechners, um dort den Browserverlauf einzusehen. Weniger schwerwiegend wäre der Einsatz eines «Schreibblockers». Es wird hauptsächlich zwischen zwei verschiedenen Typen von Write-Blockern unterschieden:

- Software-Write-Blocker
- Hardware-Write-Blocker

Der Unterschied ist, wie der Name schon sagt, dass ein Software Write-Blocker das Schreiben auf die Originaldaten mit einer Software oder einem Betriebssystem (OS) verhindert, während ein Hardware-Write-Blocker dies mit einem physischen Port macht (CRU, 2023).

Hardware-Write-Blocker werden bevorzugt, obwohl sie meist teurer sind als Software-Write-Blocker. Die Verwendung von Software ist in den meisten Fällen ein zu grosses Risiko, da diese fehleranfälliger sind. Grund dafür ist, dass Softwarefehler oder Bugs auftreten können und somit unabsichtlich die Daten verfälschen. Deshalb sind Hardware-Write-Blocker zuverlässiger und einfacher zu gebrauchen (030 Datenrettung Berlin, 2023).

2.2.5. Imaging und Datenkopien

Der Industriestandard ist die Replikation der Daten mit einer Datenträgerkopie oder einem Geräteabbild (Belkasoft, 2023). Während des Kopiervorgangs wird das Gerät über einen Hardware-Write-Blocker geschützt, um zu vermeiden, dass Schreibvorgänge stattfinden. Nach dem Kopiervorgang wird mit der replizierten Version weitergearbeitet. Beim Übertragen auf den neuen Datenträger ist darauf zu achten, dass dieser vollständig formatiert und steril ist.

2.2.6. Memory Capture

Es wurde bis jetzt nur erwähnt, wie wichtig es ist, ein Geräteabbild oder Datenträgerkopie zu erstellen, um Originaldaten nicht abzuändern. Es gibt jedoch Situationen, in denen Forensiker eine «Live-Analyse» oder ein «Memory-Capture» (auch Memory-Dump genannt) durchführen sollten. Der Grund dafür ist, dass Netzwerkinformationen, Artefakte oder andere Informationen, die im RAM gespeichert sind, erfasst werden können (Michael, 2020). Diese Informationen verschwinden, sobald das Gerät ausgeschaltet wird. Damit wären viele möglicherweise relevante Beweise gelöscht und nicht mehr wiederherstellbar.

Es muss also ein Kompromiss gefunden werden, bei dem man das Risiko eingeht, mögliche Veränderungen an den Originaldaten zuzulassen und dafür ein Memory-Capture durchführen zu können, oder der gesamte «flüchtige Speicher» geht verloren.

In folgenden Fällen ist es sinnvoll, ein Memory Capture durchzuführen und das System nicht herunterzufahren (Michael, 2020):

- offensichtlich beweiskräftige Daten sind auf dem Bildschirm gut sichtbar.
- Chat-Räume
- offene Textdokumente
- Remote-Speicherung von Daten
- Instant-Messaging-Fenster
- Kinderpornografie
- Schmuggelware
- finanzielle Dokumente
- Datenverschlüsselung
- scheinbar illegale Aktivitäten

Ein weiterer Trend ist, dass Malware immer häufiger keine Spuren auf nichtflüchtigen Speichern hinterlässt (Michael, 2020). Aus diesem Grund wird die Methode des Memory-Capture immer wichtiger.

Ein Memory Capture verändert die Beweise immer bis zu einem gewissen Grad. Dies liegt daran, dass die Software auf dem Zielobjekt installiert und ausgeführt werden muss.
Ein mögliches Risiko eines Memory Capture ist auch, dass das System abstürzt. Ein Systemabsturz tritt auf, wenn das Memory Capture Tool zum falschen Zeitpunkt auf einen reservierten Datenbereich oder auf eine systemkritische Funktion zugreift (Michael, 2020).

2.2.7. Hashing

Ein wichtiger Teil der Chain of Custody ist auch, dass die Daten, welche bearbeitet werden, auch wirklich die richtigen Daten sind, die gesammelt wurden. Eine bekannte Methode in der digitalen Welt dafür ist die Verwendung einer sogenannten «Hash»-Berechnung (Zola, 2021).

Hashing ist der Akt der Umwandlung eines Schlüssels oder einer Zeichenfolge in einen neuen Wert. Der neue Wert ist in der Regel kürzer und fast unmöglich zurückzutransformieren. Dieser Transformationsprozess kann mit verschiedenen Algorithmen durchgeführt werden, die alle ein wenig anders funktionieren. SHA-256 ist ein solcher Hash-Algorithmus, der weit verbreitet ist und als sicher gilt (Bouam et al., 2021).

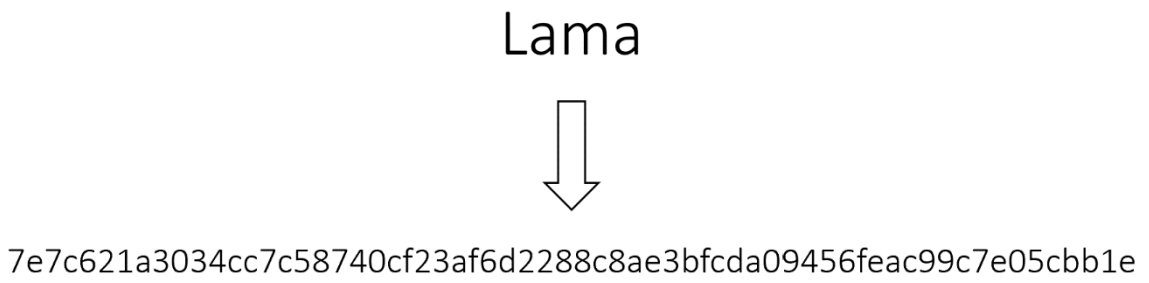

Abbildung 3 - SHA-256 Hash von «Lama» (Böller, 2023)

Anhand des SHA-256-Algorithmus wird im obigen Bild ein Hash von dem Wort Lama gemacht. Der Ausgangswert wird in Hexadezimal ausgegeben. Wenn jetzt nur etwas an dem Wort geändert oder hinzugefügt wird. Kommt ein komplett neuer Wert heraus.

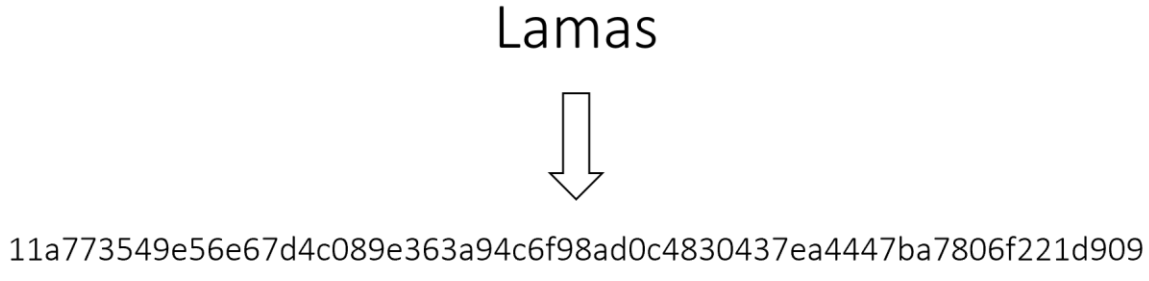

Abbildung 4 - SHA-256 Hash von «Lamas» (Böller, 2023)

Der Ausgangswert hat immer die gleiche Hexadezimal Länge, egal wie lange der Eingang ist. Mit folgendem Beispiel wird dies klar ersichtlich:

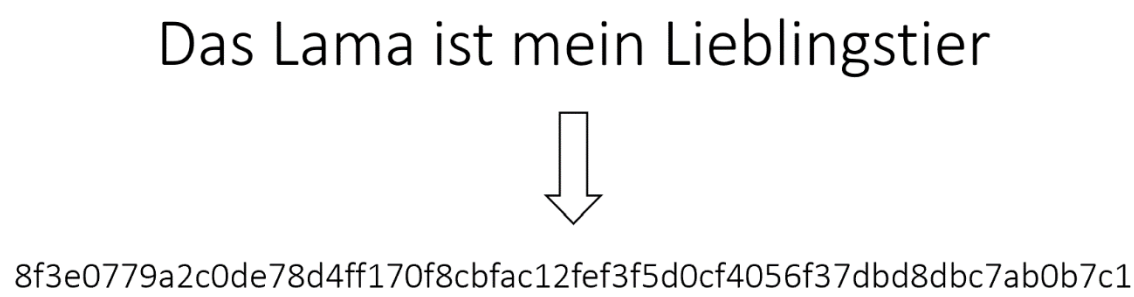

Abbildung 5 - SHA-256 Hash von «Das Lama ist mein Lieblingstier» (Böller, 2023)

Hashing hilft bei der Authentifizierung von Daten durch Hash-Signaturen. Diese kann verwendet werden, um sicherzustellen, dass Daten nicht verändert wurden und sie tatsächlich Bit für Bit mit den Originaldaten übereinstimmen.

Hashing kann in diesem Fall als Kontrolle in der Forensik eingesetzt werden. So kann ein Beweismittel verifiziert werden, dass z.B. der kopierte Datenträger exakt mit dem Original übereinstimmt und während des Kopiervorgangs nichts verändert wurde.

Der Speicherinhalt eines laufenden Systems ändert sich immer, sodass ein Hash hier nichts bringen würde, da ein Speicherabzug sich von einem einige Minuten später ausgeführten Abzug unterscheiden wird. Die Hash-Signatur wird sich daher immer vollständig von einer Aufnahme des Gesamten unterscheiden. Wird jedoch eine Aufnahme einer einzelnen aktiven Datei gemacht, so kann diese später mit dem Hash auf Veränderungen überprüft werden (Michael, 2020).

2.2.8. Fuzzy Hash

Fuzzy Hashing ist eine hybride Hashing-Technik. Sie kombiniert Elemente von Kryptografischen Hashes, Rolling Hashes und Piecewise Hashes. Im Gegensatz zu herkömmlichen Hashes wird bei Fuzzy Hashing ein «grauer» Hash-Ansatz verfolgt (Sarantinos et al., 2016). Er identifiziert Dateien, die nahezu identisch sind, auf der Grundlage der Syntaxähnlichkeit. Der Dateienvergleich erzeugt einen prozentualen Wert zwischen 0 und 100 (Sarantinos et al., 2016).

Ursprünglich als Tool zur Suche nach Datei-Updates entwickelt, wurde es später für die Identifizierung von Ähnlichkeiten und die Filterung von Spam-E-Mails eingesetzt. Später wurde es modifiziert, um Ähnlichkeiten von Segmenten oder Abschnitten einer Datei effizienter zu identifizieren (Sarantinos et al., 2016).

Fuzzy-Hashing überwindet die Begrenzungen kryptografischer Hashes, indem es die Identifizierung von eingebetteten Beweisen oder Spuren, Code-Versionen, verwandten Dokumenten und Korrelationen zwischen Speicher - und Netzwerkquellen ermöglicht. Es ist effektiv für den Gebrauch, wo es immer wieder Veränderungen gibt. Beispielsweise Malware, die sich immer wieder ein wenig in der Struktur ändert (Sarantinos et al., 2016),

wird so entdeckt, was auch in der Forensik nützlich ist und somit auch in der Chain of Custody gebraucht wird, um zu sehen, wie sich Beweismittel unterscheiden.

2.3. Aufwand und Herausforderungen bei der Einhaltung der Chain of Custody

Es wurden einige technische Möglichkeiten aufgezeigt, um die Daten unverändert zu halten und sicherzustellen, dass mit den richtigen Daten gearbeitet wird. In diesem Kapitel werden mögliche Komplikationen erläutert, die bei der Einhaltung der Chain of Custody auftreten können, und wie diese technisch umgesetzt werden können.

2.3.1. Speicher Medium

Daten werden auf verschiedenen Arten von Datenträgern gespeichert. Einige Beispiele sind:

- Hard Disk Drive (HDD)
- Solid State Drive (SSD)
- M.2 SSD
- Secure Digital (SD)
- Mikro-SD
- USB-Sticks

Datenträger ändern sich und werden ständig weiterentwickelt. Aus diesem Grund müssen Forensiker die von ihnen verwendete Software oder Hardware stets überprüfen, ob sie fehlerfrei und für das verwendete System geeignet ist. Denn ein defektes Gerät oder eine fehlerhafte Software kann das einzige Beweismittel zerstören oder verändern.

Noch nicht erwähnt wurde, dass bei einer SSD die Veränderung der Daten nicht versichert werden kann (Kumar, 2021). Der Grund dafür liegt in der Funktionsweise und im Aufbau einer SSD. Die SSD löscht nicht mehr benötigte Daten als Hintergrundprozess, was der Host nicht sieht. Ein Image einer SSD ist in den meisten Fällen nicht identisch mit dem Original, da im Hintergrund eine Schreibaktion von der SSD selbst durchgeführt wird.

2.3.2. Internet of Things

Alle genannten Beispiele gehen davon aus, dass alle relevanten Daten auf einem herkömmlichen Datenträger eines bekannten Betriebssystems liegen und somit leicht kopiert werden können. Dies ist in der heutigen Zeit jedoch leider nicht mehr der Fall. Das Internet of Things (IoT) besteht aus Tausenden von Geräten, die ihre eigenen Strukturen haben und alle ebenso relevante Daten enthalten können. Hierzu gehören auch Smartphones, die unteranderem ein eigenes Betriebssystem haben können, sowie intelligente Haushaltsgeräte und Sensoren, die Daten generieren und somit auch als potenzielle Beweismittel gelten können.

IoT-Geräte produzieren enorme Mengen an Daten, die sich im Format unterscheiden. Es gibt auch oft proprietärer Protokolle und Kommunikationsmethoden (Stoyanova et al., 2020). Es erfordert deshalb einen höheren Aufwand, da immer eine Evaluierung notwendig ist und die Daten in ein angemessenes Format verarbeitet werden müssen, um die Daten analysieren zu können (Stoyanova et al., 2020).

Der Zugriff auf die Daten dieser Geräte kann sich als schwierig erweisen, vor allem, wenn sie nicht leicht zu erreichen sind oder sich in den Händen von Dritten befinden wie zum Beispiel von Cloud-Anbietern.

Dazu kommt, dass IoT Geräte meist einfach manipuliert werden können und es auch schwierig ist festzustellen, dass die Daten in ihrem ursprünglichen Zustand erhalten bleiben (Stoyanova et al., 2020). Deshalb macht das IoT den ganzen Prozess komplizierter. Der Forensiker hat mehr Arbeit und muss darüber hinaus beim Umgang mit IoT-Beweisen rechtliche und ethische Überlegungen sorgfältig berücksichtigen, um die Rechte und die Privatsphäre der an digitalforensischen Untersuchungen beteiligten Personen zu schützen.

2.3.3. Cloud

Die Technologiekomponenten der Cloud machen sie anfällig für zahlreiche Sicherheitsprobleme. Diese Schwachstellen beeinträchtigen die Sicherheit der gespeicherten Daten in der Cloud und reduzieren deren forensischen Wert, da sie von böswilligen Nutzern ausgenutzt werden können.

Das «forensische Cloud-Problem» stellt eine bedeutende Herausforderung dar, da böswillige Täter in der Lage sind, Daten zu manipulieren oder zu löschen, sobald sie Zugang erlangen (Stoyanova et al., 2020). Die verteilte Natur der Cloud kann es jedoch Kriminellen erschweren, Spuren zu verwischen, da digitale Beweise oft an mehreren Orten gesichert und indiziert sind.

Datenschutz und mangelnde Transparenz bei Cloud-Diensten stellen bei Ermittlungen eine Herausforderung dar. Die intransparente interne Infrastruktur der Cloud-Service-Provider (CSP) erschwert Ermittlern den Zugang. Aufgrund der Gesetze des Gastlandes kann der Standort von Datenzentren den Datenzugang beeinflussen (Stoyanova et al., 2020).
Dienstanbieter legen die Dauer der Datenspeicherung fest, welche je nach Land und Region variiert. Rechtsvorschriften wie die Datenschutz-Grundverordnung (DSGVO) haben das Ziel, die Datenspeicherfristen zu verkürzen.

2.3.4. Verschlüsselung

Verschlüsselungen stellen in der Digitalen Forensik eine Herausforderung und vor allem im Einhalten der Chain of Custody. Eine klare Herausforderung ist, dass gewisse Daten gar nicht zugänglich sind, da sie verschlüsselt wurden und niemand einen Zugang geben kann oder darf. Das führt zu einer beeinträchtigten Beweismittel Sammlung und unvollständigen Daten (Ilbiz & Kaunert, 2021).

Der Untersucher der Daten muss sich somit Zugriff auf die verschlüsselten Daten schaffen. Eine erfolgreiche Entschlüsselung erfordert in der Regel den Zugriff auf die Zugangsdaten oder Schlüssel des Eigentümers oder Verdächtigen. Die Weitergabe oder Nutzung dieser Zugangsdaten könnte als Manipulation von Beweismitteln angesehen werden und somit gegen die Chain of Custody verstossen. Die Entschlüsselung von Daten für forensische Analysen wirft Bedenken hinsichtlich der Datenintegrität auf (Ilbiz & Kaunert, 2021). Das Entschlüsseln und der Zugriff auf Informationen können schwer nachzuvollziehen sein, insbesondere in sensiblen oder vertraulichen Szenarien. Die Aufzeichnung, der während des

Entschlüsselungsvorgangs durchgeführten Schritte, ist von grosser Bedeutung. So wird sichergestellt, dass die verschlüsselten Originaldaten unverändert bleiben.

2.4. Technische Möglichkeiten Chain of Custody zu dokumentieren

Es wurden viele Techniken erwähnt, wie die Daten vor Veränderungen gesichert werden und die Integrität deren versichert wird. Ein grosser Teil der Chain of Custody ist aber auch, wer auf die Daten zugreift, wann das passiert und wie und wann die Daten transferiert werden. Das ganze Vorgehen muss dokumentiert und nachvollziehbar sein, sodass die Chain of Custody eingehalten wird.

Diese ganze Dokumentation muss auch abgesichert werden. Denn wenn das nicht der Fall wäre, könnten die Daten manipuliert werden und dann einfach die Dokumentation abgeändert werden, um die Veränderungen zu vertuschen.

2.4.1. Timestamps

Zeitstempel (Timestamps) sind kryptografische Aufzeichnungen des genauen Zeitpunkts, zu dem Daten oder ein digitales Ereignis erstellt, geändert oder aufgerufen wird (Pietro, 2022). Timestamps spielen eine entscheidende Rolle in der digitalen Forensik und sichern die Integrität sowie die chronologische Reihenfolge digitaler Beweise. Die Verwendung von Zeitstempeln gewährleistet die Verkettung von Beweismitteln und somit auch die Nachvollziehbarkeit von Veränderungen und Zugriffen auf digitale Daten. Zeitstempel werden von vertrauten «timestamp authorities» erstellt, sind kryptografisch signiert und können unabhängig verifiziert werden, um die Authentizität von Beweisen und deren chronologische Reihenfolge zu beweisen (Hathaway, 2020). Dadurch wird die rechtliche Zulässigkeit verbessert und es wird ein Prüfpfad für digitale Beweismittel erstellt.

2.4.2. Logs

Wer was gemacht hat, kann mit «Logs» realisiert werden. Logs dokumentieren jede Aktion, die ein Benutzer macht. Es kann nachvollzogen werden, was ein bestimmter Benutzer gemacht hat. Es kann bewiesen werden, dass die Daten nicht anders manipuliert wurden als angegeben.

Mit Logs kann komplett nachvollzogen werden, wer eine Aktion wann ausgeführt hat und wieso es gemacht worden ist. Die Logs, die für einen Fall erstellt werden, können in der Chain of Custody als Audit Trail oder auch als Evidence Log bezeichnet werden (Ali et al., 2022).

2.5. Blockchain als zukunftsorientierte Möglichkeiten

Blockchain wurde vor allem durch Kryptowährungen bekannt. Allerdings kann die Technologie auch anderweitig sehr nützlich sein. Blockchain kann als ein unveränderliches «Hauptbuch» betrachtet werden, das die Dokumentation von Ereignissen im Falle von digitaler Forensik und die Verfolgung von Aktionen erleichtert. Unveränderlich bedeutet, dass jeder Eintrag in dieses Hauptbuch von niemandem mehr bearbeitet oder gelöscht werden

kann (Ali et al., 2022). Dies garantiert, dass alle Massnahmen, die an den Beweismitteln vorgenommen werden, nachgewiesen und nicht verändert werden können.

Jede Handlung wird als «Block» in der Blockchain aufgezeichnet. Was aufgezeichnet wird, kann selbst definiert werden (Ali et al., 2022). Mögliche Informationen für die forensische Analyse könnten ähnliche Kategorien aufweisen wie ein normales Chain of Custody Formular:

- Datum und Uhrzeit
- Zugriffsort
- Name des Untersuchers
- Art des Datenträgers und Seriennummer des Datenträgers.
- Marke und Modell des Datenträgers
- Methode der Erfassung (verwendete Werkzeuge)
- Physikalische Beschreibung des Computers einschliesslich Betriebszustand
- Name der erfassten Abbilddatei oder Ergebnisdateien
- Hash-Werte

Jeder Block ist mit den vor- und nachgeschalteten Blöcken verbunden, wodurch eine Datenkette entsteht. Die Blöcke bestätigen objektiv den exakten Zeitpunkt und die Reihenfolge der Aktionen. Sie sind sicher miteinander verbunden, um jegliche Veränderung oder das Einfügen eines Blocks zwischen zwei bestehenden Blöcken zu verhindern. Jeder zusätzliche Block stärkt die Überprüfung des vorherigen Blocks und auch der gesamten Blockchain. Die Blockchain wird durch diese Massnahmen fälschungssicher und gewährleistet somit die Unveränderlichkeit der aufgezeichneten Daten. Manipulationen durch böswillige Akteure sind ausgeschlossen und es entsteht ein vertrauenswürdiges Buch der Ereignisse (Gopalan et al., 2019).

2.6. Schlussfolgerung

Es gibt zahlreiche technische Massnahmen und Vorarbeiten, die für die Umsetzung der Chain of Custody notwendig sind. In diesem Kapitel wurden verschiedene Möglichkeiten und Herausforderungen benannt, darunter Write-Blocker, Geräteabbilder, Memory-Captures und Hashes, die es ermöglichen, forensische Untersuchungen an Beweismitteln, ohne jegliche Verfälschung durchzuführen.

Aufgrund der Komplexität ist es wichtig, dass alle Schritte sorgfältig dokumentiert werden. Durch die Verwendung von Evidence-Logs und Zeitstempeln kann eine Dokumentation nachvollziehbar erstellt werden. Es existieren jedoch weitere Technologien, die bei diesen Arbeiten unterstützen, jedoch nicht erwähnt wurden.

In der heutigen digitalen Welt werden immer mehr Daten erzeugt und somit auch immer mehr verschiedene Beweismittel verwendet. Es entstehen zunehmend Schwierigkeiten, wodurch mehr Kompromisse notwendig werden. Je wichtiger die Chain of Custody im Laufe der Zeit wird, desto schwieriger wird es, sie technisch einzuhalten. Folglich ist es von grosser Bedeutung, technische Möglichkeiten zu erfinden oder weiterzuentwickeln, um sie aufrechtzuerhalten.

Hier bieten sich zukunftsorientierte Technologien an. Ein Beispiel dafür ist die Blockchain, die immer interessanter wird und eine mögliche Lösung darstellt, um viele Teile der Chain of Custody miteinander zu verbinden und technisch umzusetzen. Es ist jedoch möglich, dass sich herausstellt, dass dies nicht der richtige Weg dafür ist und ein anderer Weg eingeschlagen werden muss. Ob dies der Fall ist, kann nur mit der Zeit beurteilt werden.

2.7. Literaturverzeichnis

030 Datenrettung Berlin. (2023, June 23). *Write-blocker in der it-forensik und Datenrettung.* 030 Datenrettung Berlin: Datenrettung und Datenwiederherstellung Festplatte RAID NAS Server SSD und Flash. https://www.030-datenrettung.de/datenrettung-lexikon/write-blocker, Aufgerufen am 19.11.2023.

Ali, M., Ismail, A., Elgohary, H., Darwish, S., & Mesbah, S. (2022). A procedure for tracing chain of custody in digital image forensics: A paradigm based on grey hash and Blockchain. *Symmetry*, 14(2). https://doi.org/10.3390/sym14020334

Belkasoft. (n.d.). Preserving chain of custody in digital forensics. https://belkasoft.com/preserving_chain_of_custody, Aufgerufen am 19.11.2023.

Bouam, M., Bouillaguet, C., Delaplace, C., & Noûs, C. (2021). Computational Records with aging hardware: Controlling half the output of SHA-256. *Parallel Computing, 106,* 102804. https://doi.org/10.1016/j.parco.2021.102804

Buckbee, M. (n.d.). *Datenintegrität : Was ist das und wie ist sie aufrecht zu erhalten?*. Varonis. https://www.varonis.com/de/blog/datenintegritat-was-ist-das-und-wie-ist-sie-aufrecht-zu-erhalten, Aufgerufen am 19.11.2023.

CRU. (2020, December 2). *Write blockers*. https://www.cru-inc.com/data-protection-topics/write-blockers/, Aufgerufen am 19.11.2023.

Gopalan, Dr. S. H., Suba, S. A., Ashmithashree, C., Gayathri, A., & Andrews, V. J. (2019). Digital forensics using blockchain. *International Journal of Recent Technology and Engineering*. https://doi.org/10.35940/ijrte.b1030.0982s1119

Hathaway, M. (2020). What is a timestamping authority? *ascertia*. November 19, 2023, https://blog.ascertia.com/what-is-a-timestamping-authority

IBM. (n.d.). *Was ist Datensicherheit? Definition von Datensicherheit und Übersicht.* https://www.ibm.com/de-de/topics/data-security, Aufgerufen am 19.11.2023.

Ilbiz, E., & Kaunert, C. (2021). Europol and cybercrime: Europol's sharing decryption platform. *Journal of Contemporary European Studies*, 30(2), 270–283. https://doi.org/10.1080/14782804.2021.1995707

Kumar, M. (2021). Solid state drive forensics analysis—challenges and recommendations. *Concurrency and Computation: Practice and Experience*, 33(24). https://doi.org/10.1002/cpe.6442

Michael J., H. (2020). *The importance of volatile computer memory evidence, the tradeoffs between acquiring potential evidence from volatile memory on a running computer,*

and the defense perspective. Computer and Internet Lawyer. https://www.proquest.com/docview/2523185919/fulltextPDF/56625A661CBF453FPQ/1?accountid=169375

Obbayi, L. (2019, July 6). *Computer forensics: Chain of custody [updated 2019]*. Infosec. https://resources.infosecinstitute.com/topics/digital-forensics/computer-forensics-chain-custody/, Aufgerufen am 19.11.2023.

Pietro. (2022, June 9). *What is a timestamp and how does it work?.* Namirial Magazine. https://focus.namirial.global/what-is-a-timestamp/, Aufgerufen am 19.11.2023.

Sarantinos, N., Benzaid, C., Arabiat, O., & Al-Nemrat, A. (2016). Forensic malware analysis: The value of fuzzy hashing algorithms in identifying similarities. *2016 IEEE Trustcom/BigDataSE/ISPA*. https://doi.org/10.1109/trustcom.2016.0274

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A survey on the internet of things (IOT) forensics: Challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials,* 22(2), 1191–1221. https://doi.org/10.1109/comst.2019.2962586

Zola, A. (2021, June 3). *What is hashing and how does it work?*. Data Management. https://www.techtarget.com/searchdatamanagement/definition/hashing, Aufgerufen am 19.11.2023.

Implementation von Chain of Custody in Incident-Response-Situationen

3. Incidence Response in der IT-Forensik

Vorgelegt von: Eser Kiymet

Abstract

In diesem Kapitel wird ein Überblick über zwei zentrale Bereiche der Informationssicherheit geboten: Die Reaktion auf Vorfälle, auch bekannt als Incident Response, und die IT-Forensik. Diese Bereiche spielen eine entscheidende Rolle bei der Bewältigung von Sicherheitsvorfällen in den modernen digitalen Umgebungen.

Das Hauptziel dieses Kapitels besteht darin, ein fundiertes Grundlagenwissen zu versehen und mit den wichtigen Konzepten sowie den entscheidenden Funktionen in den genannten Fachgebieten vertraut zu machen. Der Schwerpunkt liegt auf der präzisen Erläuterung, wie die IT-Forensik als effektives Werkzeug zur Analyse von Sicherheitsvorfällen eingesetzt wird. Dabei wird besonderer Wert auf eine klare und leicht verständliche Darstellungsweise gelegt.

Schrittweise werden in den kommenden Abschnitten die grundlegenden Prinzipien erläutert, um das Verständnis für die IT-Forensik bei der erfolgreichen Bewältigung von Sicherheitsvorfällen zu fördern. Dabei kann es hilfreich sein, die aktuellen Entwicklungen und Technologien in diesem dynamischen Bereich zu berücksichtigen, um ein praxisnahes Verständnis zu ermöglichen.

3.1. Einleitung

Dieses Kapitel widmet sich den wesentlichen Themen der Incident Response und IT-Forensik in der heutigen digitalen Welt. Der Schwerpunkt liegt auf der sachgerechten Handhabung von Beweismitteln bei Incident Response Vorfällen. Die zentralen Aspekte von Incident Response und IT-Forensik werden dabei vorgestellt und die Schlüsselrolle dieser Disziplinen für die Sicherheit von Organisationen hervorgehoben. Es wird erläutert, wie die Rahmenbedingungen den gesamten Prozess der Reaktion auf Vorfälle leiten oder anders ausgedrückt, den gesamten Ablauf der Incident Response steuern. Eine Illustration erfolgt darüber, wie die IT-Forensik als unverzichtbares Werkzeug zur Untersuchung von Sicherheitsvorfällen eingesetzt wird.

Die operationellen Einschränkungen und technischen sowie rechtlichen Herausforderungen werden im Kapitel 4 artikuliert. Das Ziel dieses Kapitels besteht hauptsächlich darin, eine leicht verständliche Einführung in die wichtigsten Sicherheitsdisziplinen zu geben und die wesentlichen Konzepte und Funktionen dieser Bereiche verständlich zu machen. Somit wird eine solide Grundlage für das Verständnis der nachfolgenden Themenbereiche gelegt.

3.2. Incident Response Prozess

In den kommenden Abschnitten erhalten Sie einen weitreichenden Einblick in die Incident Response. Dieses Kapitel konzentriert sich auf die geordnete Reihenfolge von Massnahmen, beginnend bei der Vorbereitung über die Früherkennung bis hin zur abschliessenden Analyse von Sicherheitsvorfällen. Besondere Aufmerksamkeit gilt dabei den Cyber Defense Teams, der Entwicklung von Notfallplänen, der effektiven Isolation von Sicherheitsvorfällen, der Wiederherstellung von Systemen und der kontinuierlichen Optimierung der gesamten Sicherheitsinfrastruktur. Betreten Sie mit uns das Gebiet der professionellen Bewältigung von Sicherheitsvorfällen

3.2.1. Was ist ein Incident Response?

Ein Incident Response beinhaltet Massnahmen zur schnellen Reaktion auf Sicherheitsvorfälle, wie gezielte Cyberangriffe, unbeabsichtigte Datenlecks oder technische Ausfälle. Eine entscheidende Rolle spielt dabei die Integration in die Sicherheitsarchitektur, um Risiken zu minimieren und geschäftskritische Operationen aufrechtzuerhalten.

Der Incident Response ist ein strukturierter Prozess, der darauf abzielt, potenzielle Bedrohungen, Angriffe oder Verletzungen der Informationssicherheit zu erkennen und darauf zu reagieren. Das Hauptziel besteht darin, die Integrität, Vertraulichkeit und Verfügbarkeit von Daten und Systemen zu schützen. Dieser systematische Ansatz gewährleistet eine effektive Reaktion und den umfassenden Schutz von sensiblen Informationen und Systemen.

Schnelle Reaktion auf einen Vorfall: Incident Response ermöglicht eine zügige, koordinierte Reaktion, um Auswirkungen zu minimieren und Schäden zu begrenzen.

Schutz von Daten und Systemen: Effektive Incident Response gewährleistet die Sicherheit von Daten und Systemen, verhindert unberechtigten Zugriff auf vertrauliche Informationen.

Einhalten von Vorschriften: Incident Response unterstützt die Erfüllung spezifischer Anforderungen an das Melden und Untersuchen von Sicherheitsvorfällen in verschiedenen Branchen und Regionen.

Reputationsschutz: Schnelle, professionelle Reaktionen bewahren das Vertrauen von Kunden und Partnern, schützen den Ruf der Organisation.

Lernen aus Vorfällen: Incident Response ermöglicht Organisationen, aus Sicherheitsvorfällen zu lernen, Massnahmen zu ergreifen und zukünftige Vorfälle zu verhindern.

Rechtliche Aspekte: Sorgfältige Durchführung der Incident Response sichert Beweismittel für rechtliche Verfahren.

3.2.2. Der Incident Response Prozess

Wenn Cyberkriminelle erfolgreich in ein Netzwerk eingedrungen sind, ist eine gut organisierte Cyberabwehr unerlässlich. Dabei ist es wichtig, ruhig zu bleiben und die geplanten Notfallmassnahmen einzuleiten. Auch das Einhalten der vorgesehenen Meldewege ist entscheidend. In diesem Kapitel werden daher die notwendigen Schritte zur Abwehr

vorgestellt, die zu einem funktionierenden Prozess zur Reaktion auf Zwischenfälle gehören. Nach erfolgreicher Abwehr eines Cyberangriffs müssen die gewonnenen Erkenntnisse umgesetzt werden, um zukünftige Angriffe zu verhindern. Denn nach dem Angriff ist vor dem nächsten Angriff, den es abzuwehren gilt.

Wenn sich Angreifer erst einmal im Netzwerk des Opfers eingenistet haben, ist eine funktionierende Abwehr notwendig. Hier kommt der Notfallplan und das Cyber Defence Team, auch CERT (Computer Emergency Response Team) oder CSIRT (Computer Security Incident Response Team) genannt, zum Einsatz. Ein CERT besteht aus Sicherheitsexperten, die bei der Lösung konkreter Sicherheitsvorfälle helfen. Solche Vorfälle können das Bekanntwerden neuer Sicherheitslücken in bestimmten Anwendungen oder Betriebssystemen, neue Virenverbreitungen, Spamwellen durch infizierte PCs oder gezielte Angriffe auf die IT-Infrastruktur umfassen (Kebschull, 2023).

Wenn sich Angreifer erst einmal im Netzwerk des Opfers eingenistet haben, ist eine funktionierende Abwehr notwendig. Hier kommt der Notfallplan und das Cyber Defence Team, auch CERT (Computer Emergency Response Team) oder CSIRT (Computer Security Incident Response Team) genannt, zum Einsatz. Ein CERT besteht aus Sicherheitsexperten, die bei der Lösung konkreter Sicherheitsvorfälle helfen. Solche Vorfälle können das Bekanntwerden neuer Sicherheitslücken in bestimmten Anwendungen oder Betriebssystemen, neue Virenverbreitungen, Spamwellen durch infizierte PCs oder gezielte Angriffe auf die IT-Infrastruktur umfassen (Kebschull, 2023).

3.2.3. Cyber Security Incident Response Team (CSIRT)

Ein Cyber Security Incident Response Team (CSIRT) ist eine feste Abteilung in einem Unternehmen. Der Leiter, häufig der IT-Leiter oder CIO (Chief Information Officer), trifft die technischen Entscheidungen im Notfall. Das Team besteht aus IT-Mitarbeitern, DFIR-Beratern (DFIR: Digital Forensics & Incident Response) und einem Protokollführer. Sie geben regelmässig Updates. Das Cyber Security Incident Response Team (CSIRT) trifft sich zweimal täglich zur Planung und Statusbesprechung. Es gibt klare Kommunikationswege zu den Mitarbeitern über das CMT (Crisis Management Team) (Oelmaier et al., 2023).

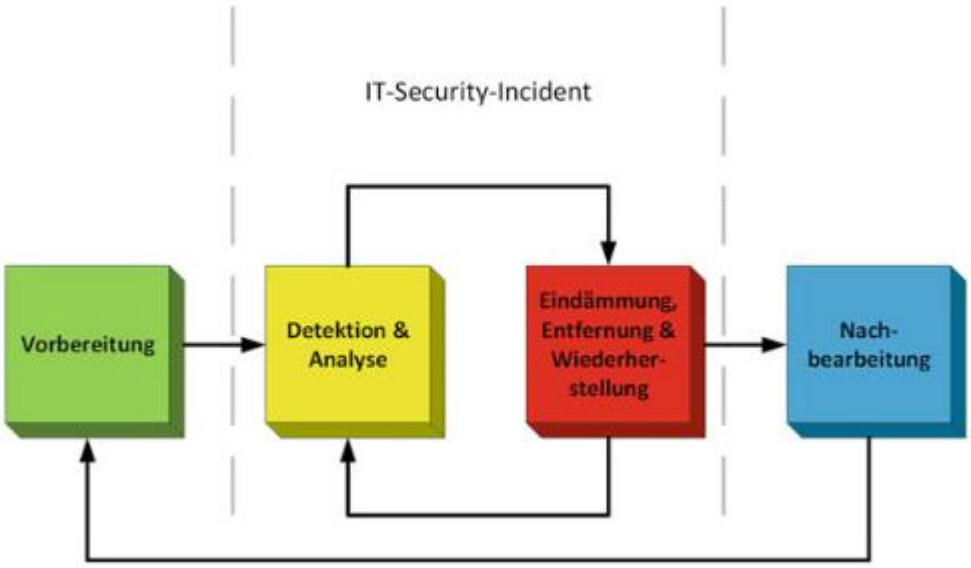

Abbildung 6 - Zweck einen Incident-Response-Zyklus (Kebschull, 2023)

Das amerikanische National Institute of Standards and Technology (NIST), eine Bundesbehörde für Normen und Technologie, hat den in Abbildung 6 dargestellten Incident-Response-Zyklus vorgeschlagen, um Organisationen bei der Bewältigung von Sicherheitsvorfällen zu unterstützen. (Kebschull, 2023)

3.2.4. Vorbereitung

Die Motivation zur Vorbereitung auf unbekannte oder noch nicht erkannte Angriffe fehlt oft. Dennoch ist es entscheidend, angemessene Massnahmen zu ergreifen, um im Ernstfall gerüstet zu sein. Dazu gehört die Aktualisierung und Bereitstellung von Kontaktdaten, die Beschaffung geeigneter Kommunikationsmittel sowie die Bereitstellung von Räumlichkeiten mit notwendiger Ausstattung, einschliesslich Computern und Kommunikationsgeräten. Im Notfall müssen relevante Personen und Stellen, darunter interne Teammitglieder, externe Geschäftspartner, Sicherheitsdienstleister und möglicherweise juristische oder regulative Stellen, schnell erreichbar sein. Zuverlässige Kommunikationsmittel sind entscheidend, um Informationen zum Vorfall schnell und effektiv auszutauschen, sowohl intern als auch extern. Eine vorbereitete Umgebung für das Incident Response Team, mit der notwendigen Ausstattung wie Computern und Kommunikationsgeräten, ist wichtig, um effektiv arbeiten zu können. Die Vorbereitung ist entscheidend für eine schnelle und effektive Reaktion auf Sicherheitsvorfälle. Es ist besser, sich vorzubereiten und möglicherweise keinen Vorfall zu erleben, als unvorbereitet zu sein, wenn es tatsächlich zu einem Vorfall kommt (Kebschull, 2023).

3.2.5. Detektion & Analyse

Im Fall eines Angriffs ist es entscheidend, die Art der Bedrohung und ihr Ausmass zu ermitteln. Die Sicherung von Beweismitteln ermöglicht spätere forensische Untersuchungen. Ein gut konfiguriertes Intrusion-Detection-System (IDS) kann Angriffe frühzeitig erkennen, bevor Schäden entstehen. In dieser Phase werden Schwachstellen analysiert, Abwehrprioritäten festgelegt, der Zwischenfall aufgezeichnet und alle Beteiligten benachrichtigt. Die sachliche Bewertung der Untersuchungsergebnisse und die Übermittlung der notwendigen Berichte an zuständige Behörden wie Strafverfolgung, CERT (Computer Emergency Response Team), Datenschutzbeauftragte etc. sind unerlässlich.

Art der Bedrohung und Ausmass feststellen: Wichtig, um geeignete Massnahmen zur Begrenzung und Behebung des Vorfalls zu ergreifen.

Beweise sichern für forensische Untersuchungen: Die Beweissicherung ist entscheidend für spätere forensische Untersuchungen, um die Herkunft des Angriffs zu identifizieren und weitere Sicherheitsmassnahmen zu ergreifen.

Intrusion-Detection-System (IDS): Ein gut eingestelltes IDS kann frühzeitig auf Angriffe hinweisen, bevor Schaden entsteht.

P**rotokollierung des Vorfalls und Benachrichtigung Betroffener:** Wichtig, um eine umfassende Nachbereitung zu ermöglichen, und die betroffenen Personen und Stellen schnellstmöglich zu informieren.

Melden bei zuständigen Behörden: Je nach Art des Vorfalls und den betroffenen Daten können rechtliche Verpflichtungen bestehen. Die entsprechenden Behörden wie Polizei,

Cyber-Sicherheitsteams und Datenschutzbeauftragte sollten informiert werden. (IDS: Intrusion-Detection-System; CERT: Computer Emergency Response Team) (Kebschull, 2023).

3.2.6. Eindämmung, Entfernung & Wiederherstellung

In dieser Phase ist es entscheidend, den Angriff zu isolieren und angemessene Massnahmen zu ergreifen, um weitere Verbreitung und zusätzlichen Schaden zu verhindern. Konkrete Eingrenzungspläne können dabei helfen, abhängig von der Angriffsart die richtigen Massnahmen zu treffen. Zu den Massnahmen wird im Kapitel 4 spezifisch auf die Eindämmung eingegangen.

Es ist von elementarer Bedeutung, Beweismaterial für mögliche rechtliche Schritte oder forensische Untersuchungen zu sichern. In einigen Fällen kann es sinnvoll sein, den Angriff unter kontrollierten Bedingungen fortzuführen, um mehr Erkenntnisse über die Angreifer zu erlangen. Die Beseitigung von Schadsoftware und die Wiederherstellung von kompromittierten Konten sind entscheidende Massnahmen zur Säuberung der betroffenen Systeme. Die Wiederherstellung der Systemintegrität erfordert verschiedene Massnahmen wie die Installation von Updates, die Verbesserung der Firewall-Regeln, die Neuinstallation von Malware-Schutzsoftware sowie das Zurücksetzen auf saubere Backups.

Besondere Bedeutung kommt auch dem Zurücksetzen von Passwörtern zu, um sicherzustellen, dass keine kompromittierten Zugangsdaten weiterhin Zugriff ermöglichen.
Eingrenzungspläne legen spezifische Massnahmen zur Begrenzung von Angriffen je nach Art im Voraus fest. Forensische Untersuchungen beinhalten die Analyse von Beweismitteln, um die Ursache eines Angriffs zu identifizieren und mögliche rechtliche Schritte einzuleiten. Saubere Backups sind Sicherungskopien von Systemen oder Daten, die nicht von Schadsoftware beeinträchtigt wurden (Kebschull, 2023).

3.2.7. Nachbearbeitung

Nach erfolgreicher Abwehr eines Angriffs kommt es zur Phase der Diskussion und Analyse des Vorfalls. Hierbei bewertet das Team, was gut funktioniert hat und identifiziert Bereiche, die verbessert werden müssen. Die gesammelten Beweise werden sorgfältig archiviert, um mögliche rechtliche Schritte oder forensische Untersuchungen zu unterstützen. Ein detaillierter Bericht über alle Aspekte des Vorfalls wird erstellt und kann mit anderen Organisationen geteilt werden, um sie auf ähnliche Angriffe vorzubereiten.

Die gewonnenen Erkenntnisse fliessen zurück in die Vorbereitungsphase des Incident-Response-Prozesses, um die Reaktion auf zukünftige Vorfälle zu verbessern. Dieser kontinuierliche Prozess betont, dass die Reaktion auf Zwischenfälle nicht als einmaliges Ereignis betrachtet wird, sondern als wiederkehrender Ablauf. Jeder erfolgreiche Abwehrversuch liefert wertvolle Erkenntnisse, die die Sicherheitsmassnahmen verbessern und an sich verändernde Bedrohungen anpassen (Kebschull, 2023).

3.2.8. IT-Security-Incidents

Der Text behandelt verschiedene Aspekte von IT-Sicherheitsvorfällen und hebt die Bedeutung von präventiven Massnahmen und einer strukturierten Reaktionsplanung hervor. Ein IT-Security-Zwischenfall kann durch verschiedene Auslöser entstehen, wie

beispielsweise Hinweise von Intrusion-Detection-Systemen (IDS), Warnungen externer Einrichtungen, das Erkennen von Indicators of Compromise (IoC) oder ungewöhnliches Verhalten der IT-Systeme (IoA). Die Reaktion auf Zwischenfälle erfordert präzise definierte Prozesse, um Fehler zu vermeiden. Mögliche Fehler, wenn vorbereitende Massnahmen fehlen, wurden ebenfalls erläutert, darunter das Übersehen von Hinweisen, falsche Einschätzung des Vorfallumfangs und mangelhafte Kommunikation.

Ein Beispiel aus dem Buch «Computer Hacking» veranschaulicht einen Vorfall in einem Krankenhaus, bei dem ein vermeintlicher Ransomware-Angriff zur Abschaltung des gesamten Dateidienstes führte. Die forensische Analyse zeigte später, dass der Angriff von einem einzelnen kompromittierten Client ausging, und ein gezieltes Abschalten dieses Rechners hätte genügt. (Kebschull, 2023).

Verschiedene Komponenten können Sicherheitsvorfälle auslösen, darunter Schadprogramme, nicht autorisierte Zugriffe, Phishing, und Anomalien in Logdateien oder Firewall-Verbindungen. Ein Computer Emergency Response Team (CERT) kann durch verschiedene Indikatoren aktiviert werden, wie entdeckte Spionageaktivitäten oder Meldungen über Spam- oder Phishing-Attacken von externen Einrichtungen. Der Text betont die kontinuierliche Verbesserung des Incident-Response-Prozesses durch Analyse von Vorfällen und Integration gewonnener Erkenntnisse in die Vorbereitungsphase (Kebschull, 2023).

3.3. Incident-Response-Prozess und seine Phasen

Der Prozess der Incident Response, der nach dem NIST Computer Security Incident Handling Guide strukturiert ist, setzt sich aus verschiedenen Phasen zusammen. Diese Phasen sind in Abbildung 2 dargestellt (Kebschull, 2023).

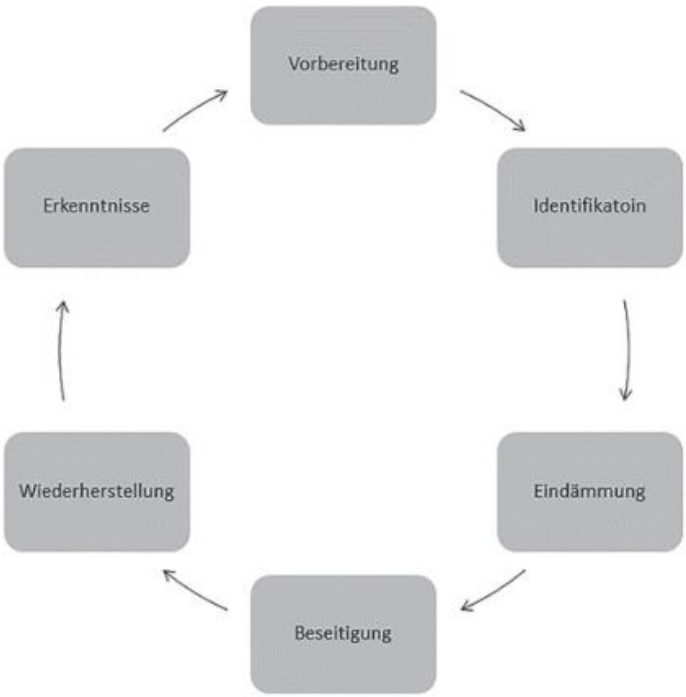

Abbildung 7 - Schritten der Incident-Response-Prozess (Kebschull, 2023)

Der Incident Response Prozess, wie in Abbildung 7 dargestellt, besteht aus mehreren wichtigen Schritten, die auf dem NIST Computer Security Incident Handling Guide basieren. Diese werden in den folgenden Schritten beschrieben.

Während der Vorbereitungsphase wird darauf geachtet, dass genügend Personal und Ressourcen vorhanden sind, um effektiv auf Cyberangriffe zu reagieren. Schulungen und regelmässige Übungen dienen dazu, die Reaktionsstrategie zu optimieren und sicherzustellen, dass die Sicherheitsmassnahmen wirksam sind.

Im Falle eines Angriffs werden in der Identifikationsphase die betroffenen Komponenten genau identifiziert, wichtige Daten gesichert und die Nutzer zeitnah informiert. Die anschliessende Eindämmungsphase hat zum Ziel, weiteren Schaden zu verhindern, wobei schnelle Reaktion und Vertraulichkeit gegenüber dem Angreifer im Vordergrund stehen.

In der Beseitigungsphase werden schädliche Dateien gelöscht, betroffene Systeme neu installiert und die Sicherheitsmassnahmen werden verstärkt. Sobald die Beseitigung erfolgreich abgeschlossen wurde, folgt die Wiederherstellung des Normalbetriebs, die durch Überwachungsmethoden begleitet wird, um sicherzustellen, dass alle Prozesse den geltenden Standards entsprechen.

Die Gewinnung von Erkenntnissen aus dem Vorfall ist entscheidend und wird in einer Analysephase durchgeführt. Hier werden mögliche Verbesserungen evaluiert, um ähnliche Vorfälle in Zukunft zu vermeiden.

Die Wichtigkeit eines strukturierten Incident Response Prozesses zeigt sich in der Risikominderung, effizienten Ressourcennutzung, effektiven Behandlung und Wiederherstellung sowie das Lernen aus Erfahrungen. Unklare Strukturen könnten zu Verzögerungen, Geschäftsunterbrechungen und rechtlichen Konsequenzen führen, während ein durchdachter Prozess schnelle Erkennung, effiziente Ressourcennutzung und minimale Ausfallzeiten ermöglicht.

Insgesamt fördert ein strukturierter Incident-Response-Prozess eine proaktive, effiziente und lernorientierte Herangehensweise an Sicherheitsvorfälle, was zu einer Stärkung der Gesamtsicherheit einer Organisation führt (Kebschull, 2023).

3.4. Forensik im Incident Response

In den kommenden Abschnitten wird der massgebliche Zusammenhang der forensischen Informatik für die Analyse vergangener Sicherheitsvorfälle im Incident Response ausgeleuchtet. Dabei liegt der Fokus auf der Effektivität, Vorbereitung und den Zielen, wobei sowohl kriminalistische als auch technische Forensik entscheidend sind. Das Ziel ist die Identifizierung von Angreifern sowie die Klärung von Auswirkungen und zeitlichen Abläufen von Angriffen.

3.4.1. Was ist die IT-Forensik?

IT-Forensik, ein Sammelbegriff für Datenanalysetechniken, zielt darauf ab, Erkenntnisse über vergangene Ereignisse zu gewinnen, insbesondere bei Sicherheitsvorfällen wie Ransomware-Angriffen. Die Aussagekraft hängt von verfügbaren Daten ab, die durch

Systemkonfigurationen beeinflusst werden. Eine umfassende Vorbereitung auf forensische Untersuchungen fehlt oft, was die Aufklärungschancen reduziert.

Nach einem abgewehrten Angriff ist es sinnvoll, die Eintrittspunkte, betroffene Systeme und Dauer des Zugriffs zu analysieren. Ziel ist es, Angreifer zu identifizieren und Spuren zu untersuchen. Die Untersuchung von Computersystemen, auch Computerforensik genannt, spielt eine entscheidende Rolle. Während eines Angriffs müssen Daten und Logfiles gesichert werden. Spuren hinterlassen immer Hinweise, die untersucht werden können. Diese Untersuchung dient zwei Zielen: kriminalistische und technische Forensik.

Kriminalistische Forensik sammelt gerichtsverwertbare Beweise für strafbares Verhalten, während technische Forensik Angriffe analysiert, um Art, Ursprung und Ausmass zu bestimmen. Letztere beinhaltet das Sammeln von Informationen über betroffene Systeme und entwendete oder manipulierte Daten. (Kebschull, 2023)

Die Untersuchung von IT-Vorfällen ist bei der Behebung von Schäden und der Vermeidung von Betriebsunterbrechungen von grosser Bedeutung. Die Kosten für solche Untersuchungen hängen stark von den gesteckten Zielen und der Komplexität des Vorfalls ab. Auch wichtig sind die komplexen IT-Systeme des Unternehmens, die Dauer des unbemerkten Netzwerkzugriffs der Angreifer und die Verfügbarkeit von wichtigen Logdaten. Zu Beginn der Untersuchung ist meistens unklar, wie gross der Angriff war und deshalb kann der Untersuchungsaufwand erst nach der ersten Überprüfung abgeschätzt werden. Die Höhe des Schadens variiert von niedrigen vierstelligen bis zu hohen sechsstelligen Beträgen (Oelmaier et al., 2023).

3.4.2. Ziele der IT-Forensik

Die Ziele der technischen Forensik und Klärung der folgenden Fragestellungen (Kebschull, 2023):

- Wurde ein bestimmtes System erfolgreich angegriffen?
- Welche Auswirkungen hatte der Angriff?
- Wie war der zeitliche Ablauf?
- Wurden Daten entwendet oder manipuliert?
- Sind weitere Systeme betroffen und müssen diese untersucht werden?

Ein Hacker verwendet in der Regel Programme, um Schwachstellen in einem Computer oder Netzwerk auszunutzen und seine Ziele zu erreichen. In der Sicherungsphase werden wichtige Daten identifiziert und geschützt, Entscheidungen über tolerierbare Änderungen getroffen, die gesicherten Daten mit verschiedenen Programmen analysiert und die Ergebnisse in der Verarbeitungsphase übersichtlich dargestellt (Kebschull, 2023).

3.5. Schlussfolgerung

Die Analyse von Incident Response und IT-Forensik unterstreicht die Bedeutung von gut organisierten Prozessen in der heutigen IT-Infrastruktur. Eine rasche Bedrohungserkennung und eine effiziente Reaktion sind entscheidend, um Daten und Systeme zu schützen.

Die Integration forensischer Methoden in Reaktionsprozesse markiert einen bedeutenden Fortschritt. Unternehmen können nicht nur auf akute Vorfälle reagieren, sondern auch wertvolle Erkenntnisse gewinnen. Diese Erkenntnisse ermöglichen nicht nur die Behandlung von Symptomen, sondern auch das Verstehen der Ursachen von Sicherheitsvorfällen und die Implementierung langfristiger Lösungen.

Insgesamt unterstreicht die Schlussfolgerung die Bedeutung eines ganzheitlichen Sicherheitsansatzes, der nicht nur auf Reaktion, sondern auch auf Prävention und kontinuierliche Verbesserung abzielt. Das ist von grosser Bedeutung, um den Herausforderungen der IT-Welt zu begegnen und die Sicherheitsintegrität von Unternehmen nachhaltig zu gewährleisten.

3.6. Literaturverzeichnis

Eran Salfati Michael Pease (2022). *Digital Forensics and Incident Response (DFIR)* Framework for Operational Technology (OT). https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8428.pdf, Aufgerufen am 15.10.2023

George Grispos, Tim Storer, William Bradley Glisson (2023). *Security incident response criteria: A practitioner's perspective.* (2023). https://arxiv.org/pdf/1508.02526, Aufgerufen am 15.10.2023

Johansen, G. (2022). *Digital Forensics and Incident Response - third edition*. O'Reilly Online Learning. https://www.oreilly.com/library/view/digital-forensics-and/9781803238678/B18571_FM.xhtml, Aufgerufen am 10.10.2023

Kebschull, U. (2023). *Computer hacking*. SpringerLink. Kebschull, U. (2023). *Computer hacking*. SpringerLink. https://link.springer.com/book/10.1007/978-3-662-67030-9#about-this-book, Aufgerufen am 10.10.2023

Kebschull, U. (2023). IT-Forensik. In *Computer Hacking: Eine Einführung zur Verbesserung der Computersicherheit in komplexen IT-Infrastrukturen* (S. 237–249). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-67030-9_13, Aufgerufen am 11.10.2023

Oelmaier, F., Knebelsberger, U., & Naefe, A. (2023). *Krisenfall ransomware*. SpringerLink. https://link.springer.com/book/10.1007/978-3-658-41614-0, Aufgerufen am 11.10.2023

Implementation von Chain of Custody in Incident-Response-Situationen

4. Operationelle Einschränkungen und Entscheidungskriterien im Incident Response

Vorgelegt von: Isenring Alenka

Abstract

Der Incident-Response-Prozess beschreibt die Vorgehensweise im Falle eines Cyber-Sicherheits-Angriffs. Der Ablauf und die Funktionsweise dieses Prozesses wurden bereits im Kapitel 3 erläutert. Dieses Kapitel fokussiert sich auf die operationellen Einschränkungen, die während eines Incident-Response-Prozesses beachtet werden sollten. Dabei werden die personellen, technischen und rechtlichen Herausforderungen analysiert. Zusätzlich werden die verschiedenen Entscheidungskriterien beleuchtet, die während dieses Prozesses festgelegt werden müssen. Dazu gehört die Einstufung des Vorfalls, die Kommunikation, sowie die rechtlichen Anforderungen und die Eindämmungsstrategie.

4.1. Einleitung

Die Gewährleistung der Cybersicherheit stellt für Unternehmen eine stetige Herausforderung dar. Im Falle eines Sicherheitsvorfalls muss dieser mit Hilfe des Incident-Response-Prozesses bewältigt werden. Dieser Prozess hilft der Organisation, ihre Daten zu schützen und potenzielle Schäden zu minimieren. Die erfolgreiche Umsetzung dieses Prozesses kann jedoch durch eine Reihe von operationellen Einschränkungen beeinträchtigt werden. Des Weiteren müssen Sicherheitsteams, während diesem Prozess schnelle Entscheidungen treffen, die sich auf das gesamte Unternehmen auswirken können. Ziel dieses Kapitels ist es, diese beiden Bereiche zu veranschaulichen.

Im ersten Teil des Kapitels werden die operationellen Einschränkungen eines Incident-Response-Prozesses angeschaut. Zunächst werden die personellen Herausforderungen, dann die technischen und schliesslich die rechtlichen Herausforderungen analysiert und mögliche Konsequenzen aufgezeigt.

Im zweiten Teil des Kapitels wird näher auf die Entscheidungskriterien eingegangen, die im Laufe des Incident Response berücksichtigt werden müssen. Dabei wird der Vorfall zuerst nach seinem Schweregrad eingestuft und priorisiert. Anschliessend werden die rechtlichen Konsequenzen eingeleitet, sowie die nötige Kommunikation und Eindämmungsstrategie festgelegt.

4.2. Operationelle Einschränkungen im Incident Response

Bei der Bearbeitung von Sicherheitsvorfällen mit Hilfe des Incident-Response-Prozesses können viele verschiedene Herausforderungen auftreten, mit denen sich Unternehmen auseinandersetzen müssen. Diese können die Effizienz und Wirksamkeit des Prozesses beeinflussen. Die Herausforderungen umfassen eine Vielzahl von Aspekten, von personellen, über technische, bis hin zu rechtlichen Schwierigkeiten.

4.3. Personelle Einschränkungen

Im folgenden Teil wird auf personellen Einschränkungen des Incident Response, wie Fachkräftemangel und mangelhafte Schulungen eingegangen.

4.3.1. Fachkräftemangel

Eine Schwierigkeit bei der Reaktion auf Sicherheitsvorfälle ist der Mangel an qualifizierten Fachkräften im Bereich der Cybersicherheit. Dies beeinträchtigt die Fähigkeit vieler Organisationen, sich gegen die ständig weiterentwickelnden Cyber-Bedrohungen zu verteidigen.

In einer von (ISC)² im Jahr 2021 durchgeführten Umfrage, die weltweit an Fachkräfte im Bereich der Cybersicherheit und IT gerichtet war, wurde der Zustand der Branche ermittelt. Trotz eines Anstiegs der Zahl der Cybersicherheitsexperten, hat die Studie aufgedeckt, dass rund 2,72 Millionen Fachkräfte fehlen, die notwendig sind, um kritische Infrastrukturen angemessen zu schützen ((ISC)², 2021).

60% der Teilnehmer der Studie berichteten, dass der Personalmangel im Bereich der Cybersicherheit ein Risiko für ihre Unternehmung darstellt ((ISC)², 2021).

Zu den Konsequenzen des Personalmangels gehören beispielsweise:

Erhöhte Sicherheitsrisiken und langsamere Reaktionszeiten: Ein unterbesetztes Team ist nicht in der Lage, eine Überwachung von System und Netzwerk vollumfänglich zu gewährleisten. Es besteht die Gefahr, dass trotz der Verwendung von Tools, Sicherheitslücken übersehen werden, da nicht jedes einzelne System detailliert geprüft werden kann. Um Sicherheitsvorfälle ausreichend zu bearbeiten und Sicherheitsrisiken zu minimieren, ist daher ein grösserer Zeitaufwand notwendig. Folglich ist eine schnelle Reaktion auf Vorfälle nicht möglich, da zu wenig Personal vorhanden ist.

Erhöhter Stress und Burnout: Es besteht ein erhöhtes Risiko für Stress und Burnout bei Mitarbeitern im Sicherheitsbereich, da diese oft unter hohem Druck stehen. Wenn nicht genügend Personal vorhanden ist, erhöht dies den Druck zusätzlich und kann die Ausfallwahrscheinlichkeit der Mitarbeiter aufgrund eines Burnouts erhöhen (Almanza, 2023). Das wiederum verringert die Zahl der Sicherheitsfachleute und führt zu weiterem Druck auf die restlichen Teammitglieder.

Höhere Kosten: Durch die erhöhte Nachfrage an Cyber-Sicherheitsspezialisten können Unternehmen sich gezwungen fühlen, höhere Gehälter zu zahlen, um qualifiziertes Personal zu gewinnen oder im Unternehmen zu halten, was höhere Kosten verursacht.

Es gibt verschiedene Ansätze, um den Personalmangel im Bereich der Cybersicherheit zu reduzieren. Eine Möglichkeit besteht darin, neues Personal auszubilden und vorhandenes in den entsprechenden Bereichen zu schulen. Dabei kann das National Initiative for Cybersicherheit Education (NICE) Framework von NIST (National Institute of Standards and Technology) einer Organisation bei der Planung, Umsetzung und Überwachung eines strategischen Cybersicherheitsprogramms helfen (Newhouse et al., 2017).

4.3.2. Mangelndes Sicherheitsbewusstsein und unzureichende Schulung

Ein weiteres Problem ist ein mangelndes Sicherheitsbewusstsein der Mitarbeiter und unzureichende oder fehlende Schulungen für das Incident-Response-Team. Auch wenn in einer Unternehmung genügend Personal vorhanden ist, um ein spezialisiertes Team für die Bearbeitung von Sicherheitsvorfällen zu bilden, kann ihre Effizienz beeinträchtigt werden, wenn regelmässige Schulungen und Trainings vernachlässigt werden.

Angesichts der schnellen Entwicklung von Cyberangriffen, insbesondere durch Zero-Day-Exploits, welche bislang unbekannte Sicherheitslücken von Organisationen ausnützen (Kebschull, 2023), ist es unerlässlich, dass Sicherheitsteams regelmässig auf den neuesten Stand gebracht und bezüglich der neuesten Abwehrmethoden und -techniken geschult werden (Johansen, 2022).

Doch nicht nur das spezialisierte Sicherheitspersonal sollte regelmässig geschult werden. Jeder Mitarbeiter sollte eine Grundausbildung in Sicherheitsfragen erhalten, um verdächtige Aktivitäten schneller erkennen und melden zu können. Dadurch kann die Reaktionszeit auf einen Vorfall reduziert werden.

Ein wirksames Instrument, um das Bewusstsein der Mitarbeiter für Bedrohungen wie Phishing, Malware und Social Engineering zu schärfen sind Schulungen und Workshops zu aktuellen Bedrohungen und Trends im Sicherheitsbereich (Bättig et al., 2023).

Das National Institute of Standards and Technology (NIST) hat zu diesem Thema das Dokument NIST Special Publication 800-50 mit dem Titel „Building an Information Technology Security Awareness and Training Program“ veröffentlicht. Es bietet Unternehmen konkrete Richtlinien und Best Practices für die Entwicklung eines effektiven, vierstufigen Schulungs- und Sensibilisierungsprogramms für IT-Sicherheit. Insbesondere betont es die Notwendigkeit regelmässiger Schulungen, um auf aktuelle Bedrohungen und Herausforderungen reagieren zu können (Wilson & Hash, 2003).

Die verschiedenen Stufen des Programms reichen von der Sensibilisierung bis hin zur professionellen Entwicklung, die den Unternehmen helfen, eine robuste Sicherheitskultur aufzubauen (Wilson & Hash, 2003).

1. **Awareness:** Diese Sensibilisierungsstufe zielt darauf ab, allen Mitarbeitern das Erkennen von IT-Sicherheitsproblemen zu ermöglichen.
2. **Schulung:** Hier werden Mitarbeitern, die mit IT-Systemen arbeiten, spezifische Sicherheitskompetenzen vermittelt.
3. **Bildung:** Diese Stufe integriert das Wissen der verschiedenen Fachgebiete, um IT-Sicherheitsspezialisten auszubilden, die proaktiv handeln können.

4. **Professionelle Entwicklung:** Ziel ist es, dass IT-Fachkräfte das notwendige Wissen von den Grundlagen bis zur Spezialisierung erwerben. Dies wird schliesslich durch ein Zertifikat bestätigt.

4.4. Technische Einschränkungen

Weitere Herausforderungen, die während eines Incident Response auftreten können, sind technische Aspekte. Im folgenden Teil wird auf einige dieser Einschränkungen eingegangen.

4.4.1. Mangel an Automatisierung

Wie im Kapitel 3 bereits erläutert, werden für das Auffinden von Vorfällen oder Bedrohungen verschiedene Tools als Hilfsmittel verwendet. Ohne diese kann die Erkennung und Reaktion auf Vorfälle verlangsamt sein, da Abnormalitäten und verdächtiges Verhalten nicht durch das Tool angezeigt werden (Johansen, 2022). Dabei gibt die verzögerte Erkennung den Angreifern mehr Zeit, Schaden anzurichten oder sich in Netzwerken weiter auszubreiten.

4.4.2. Mangel an Autorisierung

Damit das Incident-Response-Team mit den Tools arbeiten kann, benötigen sie für diese den entsprechenden Zugriff und die Berechtigungen. Diese müssen oft in Form von Lizenzen gekauft werden. Dabei muss darauf geachtet werden, dass die Anzahl und die Berechtigungsformen beim Erwerb der Lizenzen stimmen, damit mit diesen gearbeitet werden kann.

4.4.3. Veraltete Systeme und Tools

Durch die Weiterentwicklung der Cyberangriffe entstehen laufend neue Bedrohungen. Um sich gegen diese schützen zu können, müssen verwendete Systeme und Tools auf dem neusten Stand sein. Veraltete Systeme werden nach einer gewissen Zeit nicht mehr vom Hersteller unterstützt und erhalten daher keine Sicherheitsupdates mehr (Microsoft, 2023).

Diese Schwachstellen können von Hackern ausgenützt werden. Auch Tools, wie das Sicherheitsinformations- und Ereignis-Management (SIEM), sollten regelmässig mit aktualisierten Regelsätzen aktualisiert werden. Diese verlieren sonst an ihrer Wirksamkeit, um festzustellen, welche Ereignisse als potenzielle Vorfälle eingestuft werden können (Johansen, 2022). Auf die verschiedenen Tools, wie SIEM wird im Kapitel 5 weiter eingegangen.

4.4.4. Lokalisation von Betroffenen Systemen

Die physikalische Lokalisierung von betroffenen Systemen zur Eindämmung eines Vorfalls, kann eine Herausforderung sein. In einem Rechenzentrum, in dem sich die betroffenen Systeme an einem Ort befinden, ist die Lokalisierung einfacher. Doch in einem örtlich getrennten System, wie bei einer grösseren Unternehmensumgebung, kann es sehr zeitaufwendig werden, die entsprechenden Geräte zu lokalisieren. Dies gibt dem Angreifer Zeit, sich über das Netzwerk auszubreiten (Johansen, 2022).

4.5. Rechtliche Einschränkungen / Rahmenbedingungen

Vorschriften bestimmten, wie bei IT-forensischen Untersuchungen vorzugehen ist und können die Unternehmung schützen, doch gleichzeitig schränken sie den Handlungsspielraum der Ermittler ein (Heinson, 2015).

4.5.1. Datenschutzrecht

Während eines Sicherheitsvorfalls können viele Daten, einschliesslich persönlicher Informationen, betroffen sein.

Der Artikel 1 des Schweizer Datenschutzgesetzes schützt den Einzelnen vor Verletzungen seines Persönlichkeitsrechts durch den Umgang mit seinen personenbezogenen Daten (Art 1, DSG). Wird im Rahmen einer Incident-Response-Ermittlung mit personenbezogenen Daten gearbeitet, muss das Datenschutzrecht beachtet werden. Ein Unternehmen muss beispielsweise bei der Sammlung und Analyse personenbezogener Daten, die von einem Sicherheitsvorfall betroffen sind, sicherstellen, dass diese Daten nur für den Zweck der Untersuchung genutzt und nicht unbefugt weitergegeben oder missbraucht werden.

4.5.2. Internationale Rechtsunterschiede

Bei grenzüberschreitenden Vorfällen kann die Zusammenarbeit mit Strafverfolgungsbehörden in verschiedenen Ländern kompliziert sein, da jedes Land unterschiedliche Datenschutz- und Cyberkriminalitätsgesetze hat. Beispielsweise müssen in der Schweiz gemäss Art. 24 des Datenschutzgesetzes Verletzungen von kritischen personenbezogenen Daten unverzüglich gemeldet werden. Im Gegensatz dazu müssen solche Vorfälle laut Artikel 33 der europäischen Datenschutz-Grundverordnung innerhalb von 72 Stunden gemeldet werden (Art. 24 DSG, Art. 33 DSGVO). Daher ist es wichtig, die verschiedenen länderspezifischen Gesetze, die bei einem Sicherheitsvorfall betroffen sind, zu analysieren und zu berücksichtigen.

4.6. Entscheidungskriterien im Incident Response

Im Laufe des Incident-Response-Prozesses müssen beteiligte Sicherheitsteams innerhalb einer kurzen Zeit viele wichtige Entscheidungen treffen, die oft Auswirkungen auf das ganze Unternehmen haben können. Ein geplanter Entscheidungsprozess ist wichtig, um effektiv auf Sicherheitsvorfälle zu reagieren und mögliche Schäden zu minimieren.

4.6.1. Einstufung / Klassifizierung des Vorfalls

Nicht alle Vorfälle sind gleich schwerwiegend oder bedrohlich für eine Unternehmung. Beispielsweise erfordert ein Virus, der mehrere Computer in einem Supportbereich des Unternehmens infiziert, eine andere Reaktion als ein aktiver Angriff auf einen wichtigen Server (Johansen, 2022). Daher ist es wichtig, sicherheitskritische Vorfälle mithilfe verschiedener Kriterien zu analysieren und anschliessend zu priorisieren, um eine geeignete Reihenfolge zur Abarbeitung zu finden, damit die Vorfälle, die am sicherheitskritischsten sind, zuerst bearbeitet werden.

Ein möglicher Faktor zur Priorisierung des Vorfalls ist der Schweregrad (siehe Abbildung 1). Dabei wird analysiert, wie sich der Vorfall auf die bestehenden Funktionalitäten der betroffenen Systeme, die Vertraulichkeit, die Integrität, die Verfügbarkeit von Informationen und die Wiederherstellbarkeit auswirkt (Cichonski et al., 2012).

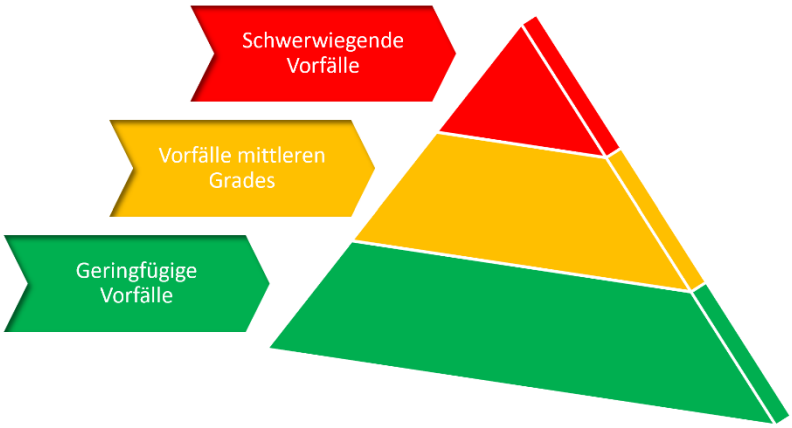

Abbildung 8 - Schweregrad eines Vorfalls (Isenring, 2023)

Ein schwerwiegender Vorfall kann zu erheblichen Schäden, Verfälschungen oder Verlusten von kritischen Unternehmens- oder Kundendaten führen, möglicherweise mit einem weitreichenden Verlust von System- oder Netzwerkressourcen. Solche Vorfälle können dem Unternehmensimage schaden und zu rechtlichen Konsequenzen führen (Johansen, 2022).

Ein Vorfall mittleren Grades ist ein Vorfall, der zur Beschädigung, Verfälschung oder zum Verlust ersetzbarer Informationen führen kann, ohne dass sensible Kundendaten gefährdet sind (Johansen, 2022). Er kann jedoch zu einer erheblichen Störung eines Systems oder einer Netzwerkressource führen.

Ein geringfügiger Vorfall ist ein Ereignis, das einen unbeabsichtigten Schaden oder den Verlust von wiederherstellbaren Informationen verursacht (Johansen, 2022). Diese Vorfälle haben nur eine geringe Auswirkung auf das Unternehmen.

4.6.2. Rechtliche und regulatorische Anforderungen

Im Incident-Response-Prozess müssen die rechtlichen und regulatorischen Anforderungen beachtet werden. Diese können Einfluss auf die Handhabung des Vorfalls haben. Insbesondere in den Bereichen des Informationsaustauschs, der Aufbewahrung von Beweisen, der Dokumentation und Kooperation mit Strafverfolgungsbehörden. Dabei müssen die verschiedenen Richtlinien und Gesetze eingehalten werden.

Datenschutz: Bei Vorfällen, die personenbezogene Daten betreffen, müssen spezifische Datenschutzgesetze und -vorschriften berücksichtigt werden (Art. 1 DSG).

Benachrichtigungspflicht: Datenschutzverletzungen müssen unverzüglich dem Datenschutzbeauftragten gemeldet werden, wenn ein hohes Risiko für die Persönlichkeitsrechte oder Grundrechte der betroffenen Personen besteht (Art. 24 DSG). Die Informationspflicht gegenüber den betroffenen Personen einer Datenschutzverletzung kann allerdings eingeschränkt, aufgeschoben oder darauf verzichtet werden. Dies gilt, wenn gesetzliche Gründe oder Geheimhaltungspflichten dies verbieten, eine Benachrichtigung unmöglich ist, dies zu grossem Aufwand führen würde oder die betroffene Person durch eine öffentliche Bekanntmachung bereits auf ähnliche Weise informiert wurde (Art. 24, Abs. 5 DSG).

4.6.3. Kommunikation

Sobald ein Sicherheitsvorfall analysiert und nach Prioritäten geordnet wurde, muss je nach Schwere des Vorfalls bestimmt werden, ob weitere Personen über den Vorfall benachrichtigt werden müssen. Je nach Schwere des Falls müssen Stakeholder oder die Rechtsabteilung informiert werden. Um die nötigen Meldungsmassnahmen für die interne und externe Kommunikation zu ergreifen, müssen die Organisationen diese intern besprechen, um Richtlinien und Verfahren für den Informationsaustausch festzulegen (Cichonski et al., 2012). Dabei muss besprochen werden, wer in welchen Fällen und zu welcher Zeit kontaktiert werden muss, sowie über welchen Kommunikationsweg dies geschieht. (International Organization for Standardization., 2015). Dies dient dazu, dass damit keine sensiblen Informationen über Vorfälle unbefugt weitergeleitet werden (Cichonski et al., 2012). Die Meldepflicht kann zwischen verschiedenen Organisationen variieren.

Medienkommunikation: Es sollten klare Kommunikationsrichtlinien für den Umgang mit den Medien festgelegt werden, um sicherzustellen, dass Informationen im Einklang mit den Richtlinien der Organisation weitergegeben werden. Ein geschulter Ansprechpartner für Medienkontakte sollte keine vertraulichen Daten weitergeben und kann dazu beitragen, Konsistenz und Klarheit in der Kommunikation zu gewährleisten (Cichonski et al., 2012).

Strafverfolgungsbehörden: Einige Vorfälle erfordern die Einbindung der Strafverfolgungsbehörden. Es ist wichtig, im Vorfeld zu wissen, wann und wie diese Behörden zu kontaktieren sind. Durch eine gute Beziehung zwischen dem Incident-Response-Team und der Strafverfolgung, sowie die korrekte Meldung eines Vorfalls, kann die Reaktionszeit im Krisenfall verkürzt werden (Cichonski et al., 2012).

Betroffene Personen: Bei Sicherheitsvorfällen, die personenbezogene Daten betreffen, müssen spezielle Benachrichtigungsverfahren und -richtlinien befolgt werden. Dabei ist

sicherzustellen, dass nur relevante Informationen kommuniziert werden, insbesondere vor einer Veröffentlichung durch Medien oder externe Institutionen (Cichonski et al., 2012).

4.6.4. Eindämmung

Die Isolierung betroffener Systeme ist ein entscheidender Schritt im Incident-Response-Prozess. Wenn ein System infiziert wurde, kann es als Ausgangspunkt für Angriffe aus anderen Systemen im Netzwerk dienen. Die Isolierung, oft durch Trennung des Systems vom Netzwerk, schränkt die Bewegungsfreiheit es Angreifers auf das betroffene System ein und verhindert die Ausbreitung des Sicherheitsvorfalls (Kebschull, 2023). Dies gibt den Sicherheitsteams Zeit, den Vorfall zu analysieren, ohne das Problem zu verschlimmern und dem Angreifer Möglichkeiten zu geben, weitere Systeme und Netzwerke zu beschädigen (Kral, 2011).

Um dies zu erreichen, sollte eine passende Eindämmungsstrategie gewählt werden, um den Schaden möglichst klein zu halten. Da die Strategie von der Art des Vorfalls abhängt, sollten Organisationen zur Erleichterung der Entscheidungsfindung für jede Art von Grossschadensereignis eine eigene Eindämmungsstrategie mit klar definierten Kriterien entwickeln (Kebschull, 2023).

Mögliche Kriterien einer Eindämmungsstrategie könnten folgende sein (Cichonski et al., 2012):

- Art des Vorfalls
- Betroffene Systeme
- Potenzieller Schaden an und Diebstahl von Ressourcen
- Notwendigkeit der Beweissicherung
- Verfügbarkeit von Diensten
- Zeit- & Ressourcenaufwand für die Umsetzung von Strategie
- Dauer der Lösung

Mögliche Eindämmungsstrategien sind:

Physische Eingrenzung: Hierbei wird die physische Verbindung zum Netz vom System getrennt. Dies kann durch das Trennen des Netzkabels, das Deaktivieren des drahtlosen Zugangs oder das Deaktivieren der Verbindung über das Betriebssystem erzielt werden. Dazu müssen die betroffenen Geräte identifiziert und ihr physischer Standort gefunden werden (Johansen, 2022).

Netzwerk Eingrenzung: Diese Strategie ist stark auf das Fachwissen von Netzwerkingenieuren und Netzwerkarchitekten angewiesen, weshalb diese, häufig Teil des technischen Supports im Incident-Response-Team sind. Hierbei werden Switch-Konfigurationen von Netzwerkadministratoren geändert, um den Datenverkehr von infizierten Systemen innerhalb eines Subnetzes zu anderen Netzwerksegmenten einzuschränken. Bei dieser Methode können Änderungen an einzelnen Netzwerkgeräten oder an der Managementkonsole erforderlich sein. Dabei sollten alle vorgenommenen Änderungen dokumentiert werden, damit sie während der Wiederherstellungsphase eines Vorfalls rückgängig gemacht oder angepasst werden können (Johansen, 2022).

Perimeter Eingrenzung: Die Perimeter-Firewall kann in einigen Fällen zusammen mit der Netzwerk-Eindämmung eingesetzt werden. Dabei dämmt das Incident-Response-Team zunächst den Netzwerkverkehr am Perimeter ein und arbeitet sich dann zu den betroffenen Subnetzen vor. Beispielsweise kann Malware oft zusätzlichen Code über Tools wie PowerShell nachladen. Sobald das Incident-Response-Team die externe IP-Adresse identifiziert hat, über die die Malware zusätzliche Pakete bezieht, können diese an der Firewall blockiert werden, um weiteren Schaden zu verhindern. Änderungen am Firewall-Regelset sollten, wie bei der Netzwerkeindämmung, berücksichtigt und dokumentiert werden (Johansen, 2022).

Virtuelle Eingrenzung: Viele Organisationen haben sich dazu entschieden, ihre Systeme zu virtualisieren. In diesen Unternehmen lassen sich durch den Einsatz von Hypervisor-Software wie beispielsweise VMware's ESXi eine gleichzeitige Netzwerktrennung mehrerer Systeme ermöglichen (Johansen, 2022). Die Hypervisor-Software wird dabei auf einem physischen Server installiert und dient als Host der virtuellen Systemen (siehe Abbildung 2). Darüber hinaus wird durch diese das Anhalten von Systemen der Virtualisierungssoftware während eines Vorfalls ermöglicht, was die Aufbewahrung von Beweisen für spätere Untersuchungen ermöglicht (Johansen, 2022).

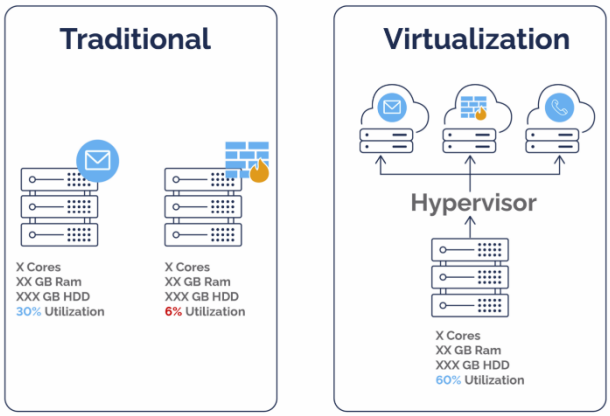

Abbildung 9- Unterschied zwischen traditioneller und virtueller Infrastruktur (MacPherson, 2022)

4.7. Schlussfolgerung

In diesem Kapitel wurden die verschiedenen operationellen Herausforderungen untersucht, die von den Unternehmen im Rahmen des Incident-Response-Prozesses zu berücksichtigen sind. Dabei wurden die personellen, technischen und rechtlichen Aspekte betrachtet. Sowie die Entscheidungskriterien während eines Incident-Response-Prozesses beleuchtet.

Ein zentrales Hindernis stellt der Fachkräftemangel in der Cybersicherheit dar. Dies kann zu erhöhten Sicherheitsrisiken und einer verzögerten Reaktionszeit führen. Daher ist es wichtig, genügend Personal zur Verfügung zu haben, um Burnouts und Überlastungen der Mitarbeiter vorzubeugen. Zusätzlich sollten alle Mitarbeiter regelmässig auf die aktuellen Sicherheitsbedrohungen geschult werden, um das Sicherheitsrisiko zu minimieren.

Technische Einschränkungen können den Prozess weiter erschweren, da bei nicht genügend Toollizenzen und veralteten Systemen, Tools nicht effizient eingesetzt werden können. Ein weiteres Hindernis stellen die rechtlichen Rahmenbedingungen dar. Vor allem bei länderüberschreitenden Vorfällen müssen die verschiedenen Sicherheitsgesetze beachtet werden.

Zudem müssen Sicherheitsteams während des Prozesses wichtige Entscheidungen, innerhalb einer kurzen Zeitspanne, treffen. Diese können sich auf das ganze Unternehmen auswirken. Dabei ist es entscheidend, die Schwere eines Vorfalls richtig einzuschätzen und entsprechend zu priorisieren, um den Schaden zu begrenzen. Damit dieses Verfahren schnell und reibungslos verläuft, sollten Unternehmen bereits im Vorhinein einen Plan für verschiedene Szenarien erarbeiten.

4.8. Literaturverzeichnis

Almanza, A. R. (2023, November 23). *Cybersecurity and Burnout: The Cybersecurity Professional's silent enemy.* ISACA. https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-48/cybersecurity-and-burnout-the-cybersecurity-professionals-silent-enemy, Aufgerufen am 03.12.2023.

Bättig, A., Horvath, S., Kryeziu, A., Mendil, S., Serretti, D., & Veseli, E. (2023). *Security Awareness, Herausforderungen und Lösungsansätze für Mitarbeiter und Unternehmen* (S. 67) [Projektarbeit], Hochschule Luzern.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology* (NIST SP 800-61r2; S. NIST SP 800-61r2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2, Aufgerufen am 05.10.2023.

Datenschutz-Grundverordnung (DSGVO). (2021, Mai 4). Art. 33 DSGVO, *Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde* https://dsgvo-gesetz.de/art-33-dsgvo/, Aufgerufen am 07.10.2023.

Heinson, D. (2015). *IT-Forensik* (Bd. 119). (S. 69-72) Mohr Siebeck.

International Organization for Standardization. (2022, Oktober 25). (*Information security management systems Requirements* (ISO/IEC 27001:2022) ISO. https://www.iso.org/standard/27001, Aufgerufen am 01.10.2023.

(ISC)² (2021). *„A Resilient Cybersecurity Profession Charts the Path Forward (ISC)2 CYBERSECURITY WORKFORCE STUDY, 2021"* [Workforce Study]. https://iapp.org/resources/article/isc2-2021-cybersecurity-workforce-study/, Aufgerufen am 01.10.2023.

Johansen, G. (2022). *Digital Forensics and Incident Response* (3. Aufl.). Packt Publishing. https://learning.oreilly.com/library/view/digital-forensics-and/9781803238678/B18571_FM.xhtml, Aufgerufen am 01.10.2023.

Kebschull, U. (2023). *Computer Hacking: Eine Einführung zur Verbesserung der Computersicherheit in komplexen IT-Infrastrukturen* (S. 237–249). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-67030-9_13, Aufgerufen am 15.10.2023.

Kral, P. (2011, Dezember 5). *33901.pdf on Egnyte.* SANS - The Incident Handlers Handbook. https://sansorg.egnyte.com/dl/6Btqoa63at, Aufgerufen am 15.10.2023.

Microsoft. (2023, August 28). *Ending Support in 2023—Microsoft Lifecycle*. https://learn.microsoft.com/en-us/lifecycle/end-of-support/end-of-support-2023, Aufgerufen am 15.10.2023.

Schweizerische Eidgenossenschaft (2020, September 25). Stand am 1. September 2023. *Bundesgesetz über den Datenschutz.* Fedex. https://www.fedlex.admin.ch/eli/cc/2022/491/de, Aufgerufen am 07.10.2023.

Wilson, M., & Hash, J. (2003). *Building an Information Technology Security Awareness and Training Program* (NIST SP 800-50). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-50, Aufgerufen am 01.10.2023.

Implementation von Chain of Custody in Incident-Response-Situationen

5. Herausforderungen der Chain of Custody in der Incident Response

Vorgelegt von: Schär Michelle

Abstract

Das finale Kapitel verknüpft das erarbeitete Wissen und betont die Herausforderung der Chain of Custody in der Incident Response. Das Kapitel beleuchtet Tools, Prozesse und Organisationsstrukturen für die erfolgreiche Umsetzung der Chain of Custody. Die Unterkapitel arbeiten schrittweise an der Verknüpfung von Erkenntnissen, und ein «Real-Life-Beispiel» erläutert den Incident-Response-Prozess.

5.1. Einleitung

In diesem Kapitel werden zunächst die grundlegenden Konzepte der Chain of Custody und deren Bedeutung im Kontext von Incident Response eingehend erläutert. Darauf aufbauend, die aktuellen Herausforderungen, denen sich Organisationen gegenübersehen, sowie innovative Technologien und Strategien, die zur Sicherung und Verarbeitung digitaler Beweise eingesetzt werden können. Dabei wird ein besonderer Fokus auf die effektive Nutzung von Spezialsoftware und die Implementierung von Best Practices gelegt, um die Authentizität und Zuverlässigkeit der Beweismittel sicherzustellen. Abschliessend werden praktische Fallbeispiele und Szenarien präsentiert, die die Anwendung dieser Technologien und Verfahren im realen Umfeld illustrieren.

5.2. Chain of Custody im Incident Response Prozess

In diesem Kapitel werden verschiedene Tools angeschaut, welche die Chain of Custody im Incident-Response-Prozess unterstützen können.

5.3. Tools

Es gibt verschiedene Tools, welche den Prozess von der Analyse bis hin zur Incident Response vereinfachen können. Die Tools, aus denen die Daten gezogen werden, sind z.B. Netzwerk-Logs, Proxy-Logs, Firewall-Logs, aber auch das Intrusion-Detection-System (IDS) und das Intrusion-Prevention-System (IPS).

5.3.1. Intrusion Detection System (IDS)

Ein Intrusion-Detection-System ist ein Überwachungssystem, das den Datenverkehr im Netzwerk oder auf Hosts analysiert, um verdächtige Aktivitäten oder Anomalien zu erkennen. (Auhood Alfaries, 2019) Es identifiziert mögliche Sicherheitsverletzungen, indem es nach Mustern und Signaturen sucht, die auf bekannte Angriffe hinweisen.

IDS kann in zwei Hauptkategorien unterteilt werden:

- **netzwerkbasiertes IDS (NIDS)**, das den Netzwerkverkehr überwacht (Auhood Alfaries, 2019), und
- **hostbasiertes IDS (HIDS)**, das Aktivitäten auf einzelnen Hosts oder Endgeräten überwacht. (Auhood Alfaries, 2019)

Ein Intrusion Detection System kann als eigenständiges Gerät oder als Teil einer umfassenderen Sicherheitslösung implementiert werden.

5.3.2. Intrusion Prevention System (IPS)

Ein Intrusion Prevention System geht einen Schritt weiter als ein Intrusion Detection System, da es nicht nur Bedrohungen erkennt, sondern auch aktiv Massnahmen zur Blockierung oder Drosselung des «potenziell schädlichen» Datenverkehrs ergreifen kann. Ein IPS kann aufgrund vordefinierter Richtlinien und Regeln auf Angriffe reagieren. (Auhood Alfaries, 2019) Es kann Schaden beheben, bevor er erst anschlägt. Ein IPS kann als eigenständiges Gerät oder als Teil einer umfassenderen Sicherheitslösung implementiert werden.

5.3.3. Security Information und Event Management (SIEM)

Ein Security Information und Event Management ist eine umfassende Lösung, die in der Informationssicherheit eingesetzt wird, um die Sicherheit von IT-Infrastrukturen zu gewährleisten und Angriffe auf Netzwerke und Systeme zu erkennen, analysieren und darauf zu reagieren.

Ein SIEM-System sammelt und korreliert Daten aus verschiedenen Quellen, darunter Netzwerkgeräte, Server, Endgeräte und Sicherheitsanwendungen. Diese Daten umfassen Logdateien, Sicherheitsmeldungen und Ereignisse, die auf potenzielle Sicherheitsbedrohungen hinweisen. (Dahj, 2022) Durch die zentrale Sammlung und Aggregation dieser Daten ermöglicht ein Security Information und Event Management eine umfassende Übersicht der Sicherheitslage. (Johansen, 2022)

Die Hauptfunktionen eines Security Management und Security Event Management Systems (Dicola & Kovacevic, 2023) (Microsoft, 2023) umfassen:

1. **Echtzeitüberwachung**: Das Tool ermöglicht die Echtzeitüberwachung des Datenverkehrs und der Aktivitäten in einem Netzwerk, um potenzielle Bedrohungen frühzeitig zu erkennen.

2. **Ereigniskorrelation**: Das Tool analysiert Daten, um Muster und Anomalien zu erkennen. Dies ermöglicht die Identifizierung von Sicherheitsvorfällen, die andernfalls unentdeckt bleiben würden.

3. **Benachrichtigungen und Sicherheitsmeldungen**: Das System erzeugt Alarme und Benachrichtigungen, wenn verdächtige Aktivitäten erkannt werden. Analysten können dann geeignete Massnahmen ergreifen.

4. **Detaillierte Berichterstattung**: Das Tool erstellt detaillierte Berichte über Sicherheitsvorfälle und Aktivitäten, die von Compliance-Anforderungen bis zur forensischen Analyse reichen.

5. **Datenspeicherung und Analyse**: Das System speichert Ereignisdaten langfristig, was für die Untersuchung vergangener Vorfälle und die Einhaltung von Compliance-Vorschriften von Bedeutung ist.

6. **Korrelationsregeln und Regelanpassung**: Analysten können eigene Korrelationsregeln erstellen oder vorhanden anpassen, um die spezifischen Anforderungen ihres Unternehmens zu erfüllen.

5.3.4. Extended Security Orchestration, Automation, and Response (XSOAR)

XSOAR ist ein Orchestrierungs- und Automatisierungstool für Sicherheitsbedrohungen. Es kann aus verschiedenen Quellen Daten holen, diese analysieren, kategorisieren und darstellen. Es bietet eine Möglichkeit, schnell auf Sicherheitsmeldungen zu reagieren, kann mit Machine Learning und Threat Intelligence ergänzt werden und bietet die Möglichkeit, vordefinierte Response Schritte und Playbooks zu definieren. (Dicola & Kovacevic, 2023) Dies erleichtert den Analysten die Arbeit und spart viel Analyse-Zeit ein.

Als Beispiel kann ein Phishing-Case genommen werden. Viele Firmen haben mit SPAM- und Phishing -Mails zu kämpfen. Der richtig eingestellte E-Mail-Filter ist einer der ersten Sicherheitsschritte gegen die Abwehr von Phishing. Cyberkriminelle werden jedoch immer geschickter. Jeden Fall einzeln anzuschauen und jedes Mal die ganze Analyse selbst zu machen, wäre zeitaufwendig. (Palo Alto Networks, 2023) XSOAR kann hier den grossen Teil der Arbeit übernehmen.

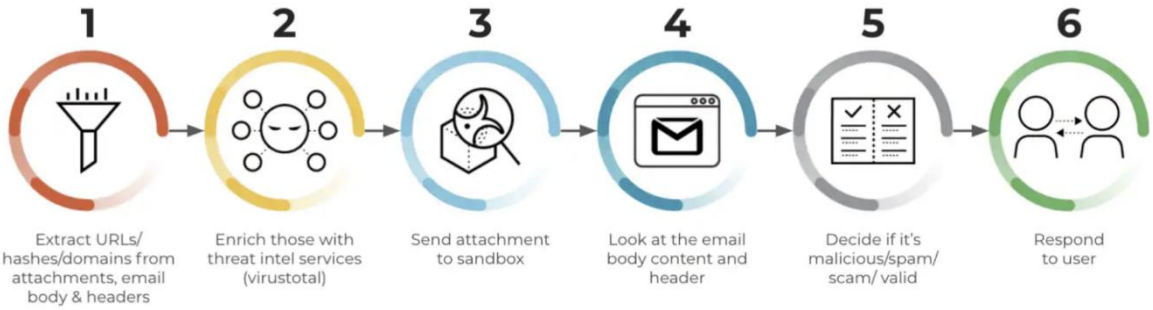

Abbildung 10 - Ablauf einer Phishing Automatisierung mit XSOAR (PaloAlto Networks, n.d.)

Folgende Schritte beziehen sich auf das oben dargestellte Bild (Palo Alto Networks, 2023):

1. Alle wichtigen Informationen werden aus dem Anhang extrahiert und mögliche IOC oder andere Indikatoren herausgepickt.
2. Die Daten werden durch ein «Enrichment» ergänzt, das heisst, dass aus anderen bekannten Quellen Daten gezogen werden. Andere Quellen können unter anderem sein: Virustotal, MISP-Framework (MISP, 2023) oder Abuse.ch. (abuse.ch, 2023).
3. Gefundene Daten, wie zum Beispiel ein .zip-File können jetzt automatisch an eine Sandbox übergeben werden und das Verhalten dieser analysiert.
4. Der Body-Content, sowie der Header der Mail werden auf weitere Indikatoren überprüft.
5. Anhand der vorliegenden Daten wird jetzt überprüft, wie das Mail kategorisiert wird.
6. Im letzten Schritt wird typischerweise der Benutzer informiert und eventuelle weitere Schritte eingeleitet.

Anmerkung: Hier wurde ein Fallbeispiel auf einem spezifischen System verwendet, dies kann jedoch auch verallgemeinert auf andere Systeme angewandt werden, wie z.B. eines klassischen Security Information und Event Management.

5.3.5. Microsoft Defender for Endpoint (MDE)

Es sollte angemerkt werden, dass es sehr viele Security Microsoft Produkte gibt, wie Defender for Cloud, welche sich mit dem Schutz von cloudbasierten Applikationen beschäftigt, (Microsoft D. f., 2023) oder Defender for Identity, welcher sich mit der Absicherung von Benutzer-Identitäten beschäftigt. (Microsoft D. f., 2023) Im Rahmen dieser Arbeit wird nur auf Microsoft Defender for Endpoint eingegangen.

Microsoft Defender for Endpoint, auch oft unter Microsoft Defender Advanced Threat Protection bekannt, kann auf den meisten Endgeräten ausgerollt werden, sprich on-premise Servern und Clients. Defender for Endpoint überwacht und loggt, unter anderem, alle Prozesse, sowie Netzwerkaktivitäten auf den Geräten. (Microsoft D. f., 2023) Zusätzlich kann es automatisierte Sicherheitsmeldungen erstellen, und Alerts kategorisieren. Diese Alerts können wiederum ins XSOAR geladen werden, um einen einheitlichen Platz zur Bearbeitung der Alerts zu haben.

Zusätzlich besitzt Microsoft Defender eine Timeline-Funktion. Diese Timeline zeigt alle Connections, Prozesse und ausgeführten Benutzeraktivitäten auf dem Endgerät aus. Hier kann der Zeitpunkt angeschaut werden, zu welchem das Phishing-Mail reingekommen ist und Schritt für Schritt, was danach passiert ist. (Microsoft D. f., Microsoft Defender for Endpoint device timeline, 2023) Der Benutzer kann z.B. sagen, dass er das Mail nicht angeklickt hat oder nicht geöffnet, um sicher zu gehen muss dies jedoch überprüft werden. Defender bietet hier die automatisierte Möglichkeit es in einem einheitlichen Tool zu machen, anstatt physisch den Laptop des Mitarbeiters abzuholen.

5.4. Dokumentationen

Die ordnungsgemässe Dokumentation ist ein wesentlicher Bestandteil jeder umfassenden Sicherheitsstrategie. Sie dient nicht nur dazu, Compliance-Anforderungen zu erfüllen, sondern auch dazu, die Effizienz der Sicherheitsmassnahmen zu verbessern, die Reaktionsfähigkeit auf Sicherheitsvorfälle zu beschleunigen und das Vertrauen der Stakeholder in die Sicherheitsmassnahmen eines Unternehmens zu stärken.

5.4.1. Technische Dokumentation

In einer technischen Dokumentation kann Hilfestellung zu einem Produkt gefunden werden. Dabei kann ein Produkt eine Software, Programmiersprache oder sonstiges sein. Hier sind die technischen Aspekte des Produktes beschrieben und gehen oft auch ins Detail rein (Jerry C. Whitaker, 2020). Die Software, mit welcher man arbeitet, sowie viele Details über die Funktionalitäten zu kennen, erleichtert die Arbeit und den Incident-Response-Prozess. Das Lesen der Dokumentation ist ein Teil, welcher erfahrungsgemäss von vielen übersprungen wird. Dabei könnte er ein tieferes Verständnis für ein Produkt und deren Funktionalitäten liefern.

5.4.2. Interne Dokumentation

Bei der internen Dokumentation ist die Dokumentation im Geschäft oder Arbeitsstelle gemeint. Idealerweise wird eine Dokumentation über die Prozesse und internen Tools geführt. So kann schnell nachgeschaut werden, wer die verantwortliche Person für ein gewisses Tool ist oder wie der Prozess einer z.B. Ticket-Erstellung funktioniert. Mit einer sauberen Dokumentation können sich auch neue Analysten schnell einleben und «verschwänden» nicht ihre eigene Arbeitszeit, wie auch nicht die der Mitarbeitenden. Weiter könnes auch Anpassungen von einer technischen Dokumentation erfasst sein, da Firmen oft eine «angepasste Eigenlösung» im Einsatz haben.

5.4.3. Sicherheitsmeldungs-Dokumentationen

Während der Bearbeitung einer Sicherheitsanalyse ist es wichtig, alle Schritte, Funde und eventuelle Überlegungen festzuhalten. Diese sind ein wichtiger Bestandteil bei der Übergabe einer Sicherheitsmeldung, an:

a.) den neuen Analysten bei der Schicht oder
b.) bei der Übergabe an das Incident-Response-Team.

Diese Dokumentation ist auch hilfreich, wenn ähnliche Sicherheitsmeldungen wiederholt vorkommen. So können diese gegeneinander abgeglichen werden und eventuelle Schritte,

welche lange gebraucht haben, um herausgefunden zu werden, sind jetzt nicht mehr so aufwendig.

5.4.4. Report / Bericht

Der Report ist die Dokumentation, welche nach Abarbeitung einer Sicherheitsmeldung geschrieben wird. Hier werden alle Funde, IOC's (Dahj, 2022) und wichtige technische Daten aufgeführt. Es kann beschrieben werden, wie welche Lücken repariert worden sind. Auch allfällige Empfehlungen und Vorgehensweisen können in den Bericht einspielen. Hier ist immer wichtig zu beachten, für wen der Report geschrieben wird. Wird dieser fürs Management erstellt nach sind andere Zahlen von Bedeutung, als wenn dieser für das technische Analytiker-Team erstellt wird.

5.4.5. Compliance-Dokumentation

Compliance-Anforderungen sind in vielen Branchen von entscheidender Bedeutung. Diese Dokumentationen müssen erstellt werden, um sicherzustellen, dass die Anforderungen und Vorschriften der DSGVO (Admin.ch, 2023) erfüllt sind.

5.5. Gruppen welche beim Incident Response Prozess von Bedeutung sind

Nachfolgend wird eine mögliche Aufstellung von verschiedenen Organisationsgruppen aufgezeigt. Dieses Beispiel basiert auf einer Grossfirma.

5.5.1. SOC

Das SOC ist das Security Operation Center. Im SOC arbeiten Analysten, welche die Sicherheitsmeldungen bearbeiten. Diese Sicherheitsmeldungen können wie oben beschrieben von einem Tool, wie z.B. XSOAR, zusammengefasst dargestellt werden. (Dahj, 2022) Das SOC macht die ganze Analyse der Sicherheitsmeldung und dokumentiert diese entsprechend. Anhand der Analyse kann der Analyst den Alert in mehrere Bereiche einteilen.

False-Positive: Bei der Detektierung gab es einen Fehler.

Benign-True-Positive: Auch als True Positive no impact bekannt. Hier war die Detektierung richtig, es gibt jedoch keine Auswirkungen. Dies kann z.B. durch einen legitimen Arbeitsprozess ausgelöst werden.

True-Positive: Die Sicherheitsmeldung wurde bestätigt und wird nun zu einem Security Vorfall.

Dieser wird jetzt in den meisten Fällen dem CSIRT übergeben. In dringenden Fällen bei einem True-Positiv kann der Analyst auch schon z.B. die Isolierung von einem Gerät selbst übernehmen.

5.5.2. CSIRT

Das CSIRT ist das Computer Security Incident Response Team und ist für die schnelle Reaktion bei einem Vorfall verantwortlich. Sie versuchen den Schaden so klein wie möglich zu halten. Durch eine saubere Voranalyse des Analysten vom SOC, weiss der Incident

Responder idealerweise gleich wo zu reagieren ist. Wenn eine Schwachstelle während des Prozesses gefunden worden ist, kann diese dem SECENG (Security Engineering) oder VUMS (Vulnerability Management) übergeben werden.

5.5.3. SECENG

Das SECENG ist das Security-Engineering-Team, welches für die Entwicklung und Implementierung von Sicherheitslösungen verantwortlich ist. Security Engineering konzentriert sich auf die Schaffung sicherer Systeme, Netzwerke und Anwendungen, um die Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Ressourcen zu gewährleisten.

5.5.4. VUMS

Das VUMS ist das Vulnerability Management und bezieht sich auf den Prozess der Identifizierung, Bewertung und Behandlung von Sicherheitsschwachstellen. Das Vulnerability Management umfasst auch das Patch-Management, um Sicherheitsupdates schnell zu implementieren und Sicherheit der IT-Infrastruktur zu gewährleisten.

5.6. Fallbeispiel von einer möglichen Malware Sicherheitsmeldung

Es wird ein Fallbeispiel von einer Malware Detection abgearbeitet, um so alle Schritte auf die bis jetzt hingearbeitet worden ist, zu vereinen. Dabei wird auch auf das gewonnen Vorwissen aus den vorherigen Kapiteln aufgebaut. Eine Malware-Analyse im Security Operations Center ist oft der erste Schritt bei der Identifizierung und Bewältigung von Sicherheitsvorfällen. Wenn die Analyse auf ein komplexeres oder schwerwiegenderes Bedrohungsszenario hinweist, kann sie an das Computer Security Incident Response Team eskaliert werden.

1. **Vorarbeit**

Aus mehreren Systemen werden Logs und weitere Daten geladen. Diese werden dann alle in ein gemeinsames Tool übertragen. Daten, welche angereichert werden können, werden mit Hilfe von anderen Tools ergänzt.

In diesem Anreicherungs-Prozess wurde jetzt ein möglicher Indicator of Compromise (Kompromittierungsindikator) gefunden. (Dicola & Kovacevic, 2023) Zum Beispiel durch einen Hash oder eine Signatur. (Abhijit Mohanta, 2020) Es wird jetzt eine Sicherheitsmeldung generiert, welche sich ein Analyst zuordnen kann.

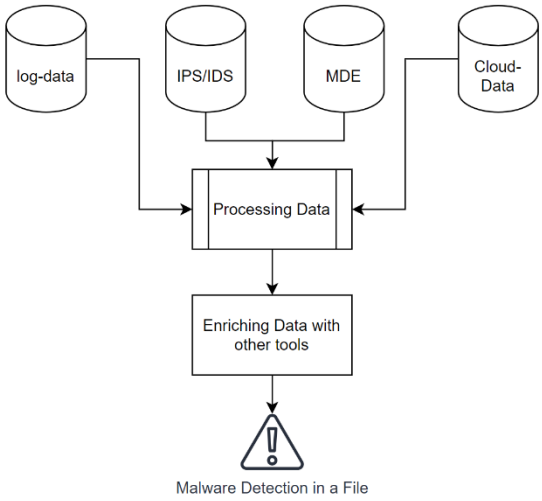

Abbildung 11 - System Zusammenführung von Systemen (Schär, 2023)

2. Bewertung

Im Security Operation Center wird die erste Bewertung des Vorfalls durchgeführt, um festzustellen, ob es sich um eine ernsthafte Bedrohung handelt. Diese Bewertung kann den Grad der Bedrohung, die betroffenen Systeme und die wahrscheinlichen Auswirkungen einschätzen. (Abhijit Mohanta, 2020)

Die erste Einschätzung entscheidet darüber, welche Systeme und wie schnell diese isoliert werden sollen.

Wichtige Punkte zu beachten sind:

- Wie kritisch ist das System auf diesem die Malware gefunden worden ist?
- Auf was hat die Detektion genau angeschlagen?
- Ist es ein Hash oder Name einer bekannten Malware, welche momentan im Umlauf ist?

3. Isolation/Eindämmung

Die verdächtige Datei kann jetzt je nach System isoliert werden (falls dies noch nicht automatisch durch ein Intrusion-Prevention-System oder Antivirus Software passiert ist). Dies kann danach extrahiert werden und in einer isolierten Umgebung, wie z.B. einer Sandbox ausgeführt werden. (Dicola & Kovacevic, 2023) So wird verhindert, dass die Malware andere Systeme oder Daten im Netzwerk beeinflusst.

In seltenen Fällen kann der Analyst auch das Gerät isolieren oder eine ganze Umgebung. Dies kann z.B. zum Zuge kommen, wenn ein starker Verdacht oder eine Bestätigung von Ransomware vorliegt. Trotzdem ist die Isolierung mit Vorsicht zu geniessen, da sie die laufende Arbeitsumgebung und somit Arbeitsprozesse beeinträchtigen kann.

4. **Statische Analyse**

Die statische Analyse wird ausgeführt, ohne die eigentliche Malware auszuführen. (Abhijit Mohanta, 2020) Die Konzentration liegt auf der Untersuchung der Datei selbst und ihrer Eigenschaften.

5. **Dateiattribute überprüfen**

Der Dateiname und Pfad kann auch verdächtige Namen oder Speicherungsorte hinweisen. Zudem kann die Dateigrösse einen Hinweis geben, dabei wird auf sehr kleine oder grosse Dateien geachtet. (Dahj, 2022) Natürlich kann diese auch eine unauffällige Grösse haben. Manchmal wird Malware in Dateien mit ungewöhnlichen Dateiendungen versteckt.

6. **Hash-Wert**

Der Hash-Werte (z.B. MD5, SHA1, SHA256) ermöglicht die Integrität der Datei im Laufe der Analyse zu überprüfen und sie in Datenbanken bekannter Malware zu vergleichen (Bouam, 2021).

7. **Metadaten**

Metadaten einer Datei können Hinweise auf den Ursprung oder Absicht der Malware geben.

8. **Strings und Klartext-Informationen**

In der Datei könnten Klartext-Strings vorhanden sein, welche auf bestimmte Verhaltensweisen oder Funktionalitäten der Malware hinweisen können.

9. **Dynamische Analyse**

Bei der dynamischen Analyse wird das Verhalten der Malware überprüft, um ihre Funktionsweise zu verstehen (Abhijit Mohanta, 2020).

10. **Sandbox-Umgebung**

Die verdächtige Malware wird in einer kontrollierten und isolierten Umgebung ausgeführt. Dies verhindert die Gefährdung anderer Systeme im Netzwerk (Abhijit Mohanta, 2020).

11. **Verhalten der Malware**

Während der Ausführung in der Sandbox wird das Verhalten der Malware überprüft. Die umfasst Aktivitäten wie Dateioperationen, Prozessdarstellung, Netzwerkkommunikation und allfällige Dateiänderungen (Abhijit Mohanta, 2020).

12. **Protokollierung und Aufzeichnung**

Die Aktivitäten der Malware werden entweder automatisch von der Sandbox (was bei den meisten der Fall ist) oder vom Analysten selbst aufgezeichnet.

13. **Netzwerkkommunikation**

Es wird überprüft, ob die Malware versucht hat mit z.B. Remote-Servern zu kommunizieren, welches auf Befehls- und Kontrollserver hinweisen kann.

14. **Code-Verhalten**

Es wird das Verhalten des ausführbaren Codes angeschaut, um festzustellen, ob die Maware versucht, potenziell schädlichen Code auszuführen (Abhijit Mohanta, 2020).

15. Gegenmassnahmen und Berichterstattung
Basieren auf den Ergebnissen der Analyse, können jetzt Gegenmassnahmen definiert werden. Es wird ein ausführlicher Bericht erstellt über die Art der Malware, ihre Funktionsweise und empfohlene Massnahmen zur Abwehr.

16. Eskalation ans Computer Security Incident Response Team
Wenn die Malware-Analyse auf eine schwerwiegende und komplexe Bedrohung hinweist, oder auf ein Szenario, dass die Ressourcen und/oder Fachwissen des SOC-Analysten übersteigt, wird der Vorfall ans Computer Security Incident Response Team übergeben.

17. Übergabe an das CSIRT
Das Security Operation Center übergibt den Vorfall an das Computer-Security-Incident-Response-Team und stellt dabei alle Informationen, den vorläufigen Bericht und andere relevante Daten zur Verfügung.

18. Vertiefte Analyse und Reverse Engineering
Das Computer-Security-Incident-Response-Team führt eine vertiefte Analyse und bei Bedarf Reverse Engineering der Malware durch. (Abhijit Mohanta, 2020) Dies kann dazu beitragen, die Funktionsweise der Malware vollständig zu verstehen und möglicherweise weitere Information über den Angreifer zu sammeln.

19. Erstellung eines ausführlichen Berichts
Es wird ein ausführlicher Bericht erstellt, ähnlich wie dies beim Security Operation Team gemacht wurde. Der vorherige Bericht kann hierbei auch als Grundlage verwendet werden.

20. Kommunikation und Koordination
Das Cyber-Security-Response-Team koordiniert die erforderlichen Massnahmen, um die Malware zu entfernen, Sicherheitslücken zu schliessen und die Auswirkungen des Vorfalls zu begrenzen. Dies kann die Zusammenarbeit mit anderen Teams und gegebenenfalls die Einbindung Experten oder Behörden einschliessen.

5.7. Herausforderungen der Zukunft

Zukunftsorientierte Ansätze der Chain of Custody und die Herausforderungen, die sich in einem ständig veränderndem Cybersicherheitsumfeld ergeben.

5.7.1. Künstliche Intelligenz und maschinelles Lernen

Beide Ansätze können bei der Überwachung und Aufrechterhaltung der Chain of Custody helfen. Anomalien können erkannt werden und auf Unregelmässigkeiten hingewiesen. Prozesse können «automatisierter» ablaufen.

5.7.2. Blockchain-Technologie

Die Implementierung von Blockchain in der Chain of Custody bietet eine unveränderliche und transparente Aufzeichnung von Daten und deren Veränderungen. Dadurch wird die Integrität von Beweisen und Informationen der Incident Response verbessert.
Schnelllebigkeit von Bedrohungen

Cybersicherheitsbedrohungen entwickeln sich ständig weiter. Es ist schwierig mitzuhalten und immer auf dem neusten Stand zu bleiben und gleichzeitig die Chain of Custody aufrecht zu erhalten (Ali, 2022).

5.7.3. Internationale Zusammenarbeit

Die Zusammenarbeit mit anderen Behörden und Ländern bietet jetzt schon eine Herausforderung, welche in Zukunft sicherlich nicht einfacher wird. Sicherheitsrelevante Vorfälle über Landesgrenzen hinweg erfordern eine klare und transparente Dokumentation, um Missverständnisse zu vermeiden.

5.7.4. Menschliches Fehlverhalten

Eine der grössten Herausforderungen ist und bleibt der Mensch. Ob es sich hierbei um zu wenig Wissen der Mitarbeiter, fahrlässiges Verhalten, zu schlechte Dokumentation und Kommunikation handelt oder die nicht Einhaltung von Richtlinien.

5.8. Schlussfolgerung

In diesem Kapitel wurde die Implementierung einer lückenlosen Chain of Custody (Beweiskette) in Incident-Response-Situationen systematisch untersucht, eine Aufgabe von höchster Bedeutung für die Integrität forensischer Untersuchungen und die Wahrung der organisatorischen Sicherheit. Die Untersuchung verschiedener Werkzeuge wie Intrusion-Detection-Systeme, Intrusion Prevention Systeme, Security Information and Event Management und andere unterstreicht ihre unverzichtbare Rolle bei der Steigerung der Effizienz und Zuverlässigkeit des Incident Response-Prozesses. Diese Werkzeuge erleichtern nicht nur die Identifizierung und Analyse von Sicherheitsvorfällen, sondern gewährleisten auch, dass die Beweiskette ununterbrochen und rechtlich haltbar bleibt.

Zusammenfassend lässt sich sagen, dass trotz bedeutender Fortschritte bei der Implementierung einer effektiven Chain of Custody in Incident Response das Feld dynamisch und herausfordernd bleibt. Zukünftige Forschungen sollten sich auf die Integration neuer Technologien in bestehende Rahmenbedingungen, die Entwicklung robuster Schulungsprogramme für Incident Response-Fachkräfte und die Erforschung neuer Methoden zur Minderung der Risiken menschlicher Fehler konzentrieren. Das ultimative Ziel bleibt klar: eine sichere, zuverlässige und rechtlich einwandfreie Incident Response gewährleisten, die sich an die ständig verändernde Landschaft von Cybersecurity-Bedrohungen anpassen kann.

5.9. Literaturverzeichnis

Abhijit Mohanta, A. S. (2020). *Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware*.

abuse.ch. *URLHaus*. Von https://urlhaus.abuse.ch/. Aufgerufen am 30. 10 2023.

Admin.ch. Von https://www.kmu.admin.ch/kmu/de/home/fakten-trends/digitalisierung/datenschutz/eu-regelung-zum-datenschutz.html. Aufgerufen am 1. 11 2023.

Ali, M., Ismail, A., Elgohary, H., Darwish, S., & Mesbah, S. (2022). *A procedure for tracing chain of custody in digital image forensics: A paradigm based on grey hash and Blockchain. Symmetry*, 14(2). https://doi.org/10.3390/sym14020334

Auhood Alfaries, H. M. (12 2019). *Cybersecurity: Design and Implementation of an Intrusion Detection and Prevention System.* Riyadh, Saudi Arabia.

Bouam. (2021). M., Bouillaguet, C., Delaplace, C., & Noûs, C. Von *Controlling half the output of SHA-256*: https://doi.org/10.1016/j.parco.2021.102804 Aufgerufen am 18.11.2023

Dahj, J. N. (2022). *Master in Cyber Intelligence*.

Dicola, N., & Kovacevic, B. (2023). *Security Orchestration, Automation, and Response for Security Analysts.* https://doi.org/10.1109/trustcom.2016.0274 .

Jerry C. Whitaker, R. K. (2020). *Technical Documentation and Process*.

Johansen, G. (2022). *Digital Forensics and Incident Response - Third Edition*. In G. Johansen, Digital Forensics and Incident Response - Third Edition (S. 532). Packt Publishing.

Microsoft. https://azure.microsoft.com/en-us/products/microsoft-sentinel#resources. Von Microsoft Sentinel. Aufgerufen am 31. 10 2023.

Microsoft, D. f. https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction. Von Microsfot. Aufgerufen am 2. 11 2023.

Microsoft, D. f. https://learn.microsoft.com/en-us/defender-for-identity/what-is. Aufgerufen am 2. 11 2023.

Microsoft, D. f. https://www.microsoft.com/en-us/security/business/endpoint-security/microsoft-defender-endpoint. Aufgerufen am 02. 11 2023.

Microsoft, D. f. *Microsoft Defender for Endpoint device timeline*. Von https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/device-timeline-event-flag?view=o365-worldwide. Aufgerufen am 10. 22 2023.

MISP. *MISP Threat Sharing*. Von https://www.misp-project.org/. Aufgerufen am 30. 10 2023.

Palo Alto Networks. (2023, 12:55). *How Does Automation Help the SOC?* Von https://www.paloaltonetworks.com/cortex/cortex-xsoar-safe. Abgerufen am 31. 10 2023

Fazit und Ausblick der Arbeit

Die Chain of Custody ist nicht nur ein Werkzeug zur Beweissicherung, sondern ein dynamisches System, das sich ständig an neue Technologien und rechtliche Rahmenbedingungen anpassen muss. Die Bedeutung der Chain of Custody geht über die Erhaltung der Integrität von Beweismitteln hinaus und beeinflusst massgeblich die Effektivität des gesamten Incident-Response-Prozesses. Im Zeitalter der digitalen Transformation und zunehmender Cyber-Bedrohungen ist eine robuste Chain of Custody unerlässlich, um die Glaubwürdigkeit und Rechtskonformität von Sicherheitsvorfällen zu gewährleisten.

Das Buch betont die wichtige Rolle der Chain of Custody (CoC) bei der Handhabung digitaler Beweise in rechtlichen Fällen, wo genaue Dokumentation und forensische Techniken von entscheidender Bedeutung sind. Im zweiten Kapitel wurden besprochene technische Massnahmen zur Sicherung von IT-Infrastrukturen erläutert, welche entscheidend für Datenschutz und Datenintegrität sind. Kapitel drei konzentriert sich auf Strategien zur Vorfallbehandlung, welche es Unternehmen ermöglichen, schnell und effektiv auf Sicherheitsprobleme zu reagieren und den Betrieb wiederherzustellen. Kapitel vier behandelte wichtige Einschränkungen und Kriterien für das Krisenmanagement, um unter Druck die richtigen Entscheidungen zu treffen. Schliesslich wurde in Kapitel 5 aufgezeigt, wie Technologien wie KI und Blockchain die Beweissicherung verbessern und Organisationen auf zukünftige Sicherheitsbedrohungen vorbereiten können.

Zukünftige Forschungsschwerpunkte:

- Forschung zur Integration fortschrittlicher Technologien in die Chain of Custody, um deren Effektivität und Anpassungsfähigkeit zu erhöhen.
- Forschung zur Optimierung der Chain of Custody unter neuen rechtlichen und regulatorischen Rahmenbedingungen.
- Entwicklung von Best Practices und Trainingsprogrammen, die das Bewusstsein und die Kompetenz der Mitarbeiter im Umgang mit der Chain of Custody stärken.
- Internationale Kooperationen zur Harmonisierung der Chain-of-Custody-Praktiken und zur Bewältigung globaler Cybersicherheit-Herausforderungen.

In der Zukunft wird die Chain of Custody in Incident-Response-Szenarien von ständigen Veränderungen und Entwicklungen geprägt sein. Um die Chain-of-Custody-Methoden stets zu aktualisieren und zu verbessern, ist eine enge Zusammenarbeit zwischen Forschung und Praxis erforderlich. Dies erfordert eine kontinuierliche Anpassung an neue technologische Trends und eine fortlaufende Auseinandersetzung mit den sich ändernden rechtlichen Bedingungen.

Das Buch «Implementierung der Chain of Custody in Incident-Response-Situationen» endet mit der Erkenntnis, dass die Chain of Custody ein wichtiger Teil der modernen Cybersicherheit ist. Es bietet einen umfassenden Einblick in aktuelle bewährte Verfahren und zukünftige Entwicklungen und betont die Bedeutung einer kontinuierlichen Anpassung und Verbesserung Chain-of-Custody-Praktiken. Fortlaufende Forschung und Entwicklung in diesem Bereich unterstützt Organisationen dabei, wirksam auf die Herausforderungen in der sich ständig ändernden Welt der Cybersicherheit zu reagieren.

Literaturverzeichnis

(ISC)² (2021). „*A Resilient Cybersecurity Profession Charts the Path Forward (ISC)2 CYBERSECURITY WORKFORCE STUDY, 2021*“ [Workforce Study]. https://iapp.org/resources/article/isc2-2021-cybersecurity-workforce-study/, Aufgerufen am 01.10.2023.

030 Datenrettung Berlin. (2023, June 23). *Write-blocker in der it-forensik und Datenrettung*. 030 Datenrettung Berlin: Datenrettung und Datenwiederherstellung Festplatte RAID NAS Server SSD und Flash. https://www.030-datenrettung.de/datenrettung-lexikon/write-blocker, Aufgerufen am 19.11.2023.

Abhijit Mohanta, A. S. (2020). *Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware.*

abuse.ch. URLHaus. Von https://urlhaus.abuse.ch/. Aufgerufen am 30. 10 2023.

Admin.ch. Von https://www.kmu.admin.ch/kmu/de/home/fakten-trends/digitalisierung/datenschutz/eu-regelung-zum-datenschutz.html. Aufgerufen am 1. 11 2023.

Ali, M., Ismail, A., Elgohary, H., Darwish, S., & Mesbah, S. (2022). *A procedure for tracing chain of custody in digital image forensics: A paradigm based on grey hash and Blockchain. Symmetry*, 14(2). https://doi.org/10.3390/sym14020334

Almanza, A. R. (2023, November 23). *Cybersecurity and Burnout: The Cybersecurity Professional's silent enemy.* ISACA. https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-48/cybersecurity-and-burnout-the-cybersecurity-professionals-silent-enemy, Aufgerufen am 03.12.2023.

Auhood Alfaries, H. M. (2019). *Cybersecurity: Design and Implementation of an Intrusion Detection and Prevention System.* Riyadh, Saudi Arabia.

Badiye, A., Kapoor, N., & G. Menezes, R. (2023, February 13). *Chain of Custody. Europe PMC*. https://europepmc.org/article/nbk/nbk551677

Bättig, A., Horvath, S., Kryeziu, A., Mendil, S., Serretti, D., & Veseli, E. (2023). *Security Awareness, Herausforderungen und Lösungsansätze für Mitarbeiter und Unternehmen* (S. 67) [Projektarbeit], Hochschule Luzern.

Belkasoft. (n.d.). *Preserving chain of custody in digital forensics*. https://belkasoft.com/preserving_chain_of_custody, Aufgerufen am 19.11.2023.

Bouam, M., Bouillaguet, C., Delaplace, C., & Noûs, C. (2021). *Computational Records with aging hardware: Controlling half the output of SHA-256.* Parallel Computing, 106, 102804. https://doi.org/10.1016/j.parco.2021.102804

Bouam. (2021). M., Bouillaguet, C., Delaplace, C., & Noûs, C. Von *Controlling half the output of SHA-256*: https://doi.org/10.1016/j.parco.2021.102804 Aufgerufen am 18.11.2023

Buckbee, M. (n.d.). Datenintegrität : *Was ist das und wie ist sie aufrecht zu erhalten?*. Varonis. https://www.varonis.com/de/blog/datenintegritat-was-ist-das-und-wie-ist-sie-aufrecht-zu-erhalten, Aufgerufen am 19.11.2023.

Buckbee, M. (n.d.). *Datenintegrität : Was ist das und wie ist sie aufrecht zu erhalten?*. Varonis. https://www.varonis.com/de/blog/datenintegritat-was-ist-das-und-wie-ist-sie-aufrecht-zu-erhalten, Aufgerufen am 19.11.2023.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology* (NIST SP 800-61r2; S. NIST SP 800-61r2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2, Aufgerufen am 05.10.2023.

CRU. (2020, December 2). *Write blockers*. https://www.cru-inc.com/data-protection-topics/write-blockers/, Aufgerufen am 19.11.2023.

Dahj, J. N. (2022). *Master in Cyber Intelligence*.

Datenschutz-Grundverordnung (DSGVO). (2021, Mai 4). Art. 33 DSGVO, *Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde* https://dsgvo-gesetz.de/art-33-dsgvo/, Aufgerufen am 07.10.2023.

Dicola, N., & Kovacevic, B. (2023). *Security Orchestration, Automation, and Response for Security Analysts.*

Eran Salfati Michael Pease (2022). *Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT).* https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8428.pdf, Aufgerufen am 15.10.2023

George Grispos, Tim Storer, William Bradley Glisson (2023). *Security incident response criteria: A practitioner's perspective*. (2023). https://arxiv.org/pdf/1508.02526, Aufgerufen am 15.10.2023

Gopalan, Dr. S. H., Suba, S. A., Ashmithashree, C., Gayathri, A., & Andrews, V. J. (2019). *Digital forensics using blockchain. International Journal of Recent Technology and Engineering*. https://doi.org/10.35940/ijrte.b1030.0982s1119

Hathaway, M. (2020). *What is a timestamping authority*? ascertia. November 19, 2023, https://blog.ascertia.com/what-is-a-timestamping-authority

Heinson, D. (2015). *IT-Forensik* (Bd. 119). (S. 69-72) Mohr Siebeck.

IBM. (n.d.). *Was ist datensicherheit? definition von Datensicherheit und übersicht*. https://www.ibm.com/de-de/topics/data-security, Aufgerufen am 19.11.2023.

IBM. (n.d.). *Was ist ein storage area network (SAN)?* San-definiert. IBM. https://www.ibm.com/de-de/topics/storage-area-network

IBM. (n.d.). *Was IST network attached storage (NAS)?* https://www.ibm.com/de-de/topics/network-attached-storage

Ilbiz, E., & Kaunert, C. (2021). *Europol and cybercrime: Europol's sharing decryption platform.* Journal of Contemporary European Studies, 30(2), 270–283. https://doi.org/10.1080/14782804.2021.1995707

International Organization for Standardization. (2022, Oktober 25). *Information security management systems Requirements* (ISO/IEC 27001:2022) ISO. https://www.iso.org/standard/27001, Aufgerufen am 01.10.2023.

Jansen, W., & Ayers, R. (2004). 34-38. In Guidelines on PDA forensics: *Recommendations of the National Institute of Standards and Technology* (pp. 1–67). essay, Computer Security Division, Information Technology Laboratory.

Jerry C. Whitaker, R. K. (2020). *Technical Documentation and Process*.

Johansen, G. (2022). *Digital Forensics and Incident Response* (3. Aufl.). Packt Publishing. https://learning.oreilly.com/library/view/digital-forensics-and/9781803238678/B18571_FM.xhtml, Aufgerufen am 01.10.2023.

Kebschull, U. (2023). *Computer hacking*. SpringerLink. https://link.springer.com/book/10.1007/978-3-662-67030-9#about-this-book, Aufgerufen am 10.10.2023

Kebschull, U. (2023). *Computer Hacking: Eine Einführung zur Verbesserung der Computersicherheit in komplexen IT-Infrastrukturen* (S. 237–249). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-67030-9_13, Aufgerufen am 15.10.2023.

Kebschull, U. (2023). *IT-Forensik*. In Computer Hacking: Eine Einführung zur Verbesserung der Computersicherheit in komplexen IT-Infrastrukturen (S. 237–249). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-67030-9_13, Aufgerufen am 11.10.2023

Kral, P. (2011, Dezember 5). 33901.pdf on Egnyte. SANS - The Incident Handlers Handbook. https://sansorg.egnyte.com/dl/6Btqoa63at, Aufgerufen am 15.10.2023.

Kumar, M. (2021). *Solid state drive forensics analysis—challenges and recommendations*. Concurrency and Computation: Practice and Experience, 33(24). https://doi.org/10.1002/cpe.6442

Meier, D. (2020, June 29). *Vorgehen eines it-forensikers und Deren Ethischen Grundsätze sowie die beweisverwertbarkeit der Erstellten Analysen in der Schweiz und EU*. Wirtschaftsinformatik reloaded. https://www.fhnw.ch/plattformen/iwi/2020/06/24/homeoffice-und-onlinekonferenzen-4-9-2-3-2-12/%C2%A0

Michael J., H. (2020). *The importance of volatile computer memory evidence, the tradeoffs between acquiring potential evidence from volatile memory on a running computer, and the defense perspective*. Computer and Internet Lawyer. https://www.proquest.com/docview/2523185919/fulltextPDF/56625A661CBF453FPQ/1?accountid=169375

Microsoft, D. f. https://www.microsoft.com/en-us/security/business/endpoint-security/microsoft-defender-endpoint. Aufgerufen am 02. 11 2023.

Microsoft, D. f. *Microsoft Defender for Endpoint device timeline*. Von https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/device-timeline-event-flag?view=o365-worldwide. Aufgerufen am 10. 22 2023.

Microsoft, D. f. https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction. Von Microsfot. Aufgerufen am 2. 11 2023.

Microsoft, D. f. https://learn.microsoft.com/en-us/defender-for-identity/what-is. Aufgerufen am 2. 11 2023.

Microsoft. (2023, August 28). *Ending Support in 2023—Microsoft Lifecycle*. https://learn.microsoft.com/en-us/lifecycle/end-of-support/end-of-support-2023, Aufgerufen am 15.10.2023.

Microsoft. https://azure.microsoft.com/en-us/products/microsoft-sentinel#resources. Von Microsoft Sentinel. Aufgerufen am 31. 10 2023.

MISP. *MISP Threat Sharing*. Von https://www.misp-project.org/. Aufgerufen am 30. 10 2023.

Obbayi, L. (2019, July 6). *Computer forensics: Chain of custody* [updated 2019]. Infosec. https://resources.infosecinstitute.com/topics/digital-forensics/computer-forensics-chain-custody/, Aufgerufen am 19.11.2023.

Oelmaier, F., Knebelsberger, U., & Naefe, A. (2023). *Krisenfall ransomware*. SpringerLink. https://link.springer.com/book/10.1007/978-3-658-41614-0, Aufgerufen am 11.10.2023

Palo Alto Networks. (2023, 12:55). *How Does Automation Help the SOC?* Abgerufen am 31. 10 2023 von https://www.paloaltonetworks.com/cortex/cortex-xsoar-safe

Pietro. (2022, June 9). *What is a timestamp and how does it work?.* Namirial Magazine. https://focus.namirial.global/what-is-a-timestamp/, Aufgerufen am 19.11.2023.

Prayudi, Y., & SN, A. (2015). International Journal of Computer Applications. *Digital Chain of Custody: State of the Art*, 1–10. https://doi.org/10.5120/19971-1856

Sarantinos, N., Benzaid, C., Arabiat, O., & Al-Nemrat, A. (2016). *Forensic malware analysis: The value of fuzzy hashing algorithms in identifying similarities.* 2016 IEEE Trustcom/BigDataSE/ISPA. https://doi.org/10.1109/trustcom.2016.0274

Schweizerische Eidgenossenschaft (2020, September 25). Stand am 1. September 2023. Bundesgesetz über den Datenschutz. Fedex. https://www.fedlex.admin.ch/eli/cc/2022/491/de, Aufgerufen am 07.10.2023.

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). *A survey on the internet of things (IOT) forensics: Challenges, approaches, and open issues. IEEE Communications Surveys & Tutorials*, 22(2), 1191–1221. https://doi.org/10.1109/comst.2019.2962586

Strafprozessordnung (stpo). Schweizerische Strafprozessordnung. (2007, October 5). https://www.rhf.admin.ch/rhf/de/home/strafrecht/rechtsgrundlagen/national/sr-312-0.html

Trebo, M., & Meier, R. (2023, June 15). *Aufdecken digitaler Beweise Durch Dokumentenanalyse.* Analyse von Bildern und Dokumenten. https://www.scip.ch/?labs.20230615

Wilson, M., & Hash, J. (2003). *Building an Information Technology Security Awareness and Training Program (NIST SP 800-50).* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-50, Aufgerufen am 01.10.2023.

Zola, A. (2021, June 3). *What is hashing and how does it work?.* Data Management. https://www.techtarget.com/searchdatamanagement/definition/hashing, Aufgerufen am 19.11.2023.

Anhang

CRAAP Test Kapitel 1

Titel: ***Vorgehen eines it-forensikers und Deren Ethischen Grundsätze sowie die beweisverwertbarkeit der Erstellten Analysen in der Schweiz und EU***
Autor: Dominik Meier
Ist es aktuell?
☒ Wurde sie kürzlich genug geschrieben, um korrekt zu sein? ☒ Wurde sie in zeitlichem Zusammenhang zum Ereignis/Thema geschrieben? ☒ Funktionieren die Links? Bemerkung: Es handelt sich um eine Wissenschaftliche Arbeit aus dem Jahr 2023
Ist es bedeutsam für mein Forschungsfrage?
☒ Beziehen sich die Informationen auf das Thema oder beantworten sie meine Frage? ☒ Wer ist das Zielpublikum? An wen richtet sich die Quelle? ☒ Bietet diese Quelle eine neue Perspektive oder Information? ☒ Ist sie technisch genug? Bemerkung: Der Artikel bezieht sich auf das Thema.
Ist es verlässlich/vertrauenswürdig?
☒ Wer hat sie geschrieben, veröffentlicht oder bekannt gemacht? ☒ Sind Kontaktangaben vorhanden? ☒ Was macht die Autorschaft zu einem Experten? ☒ Wird sie von einer Institution unterstützt? ☐ Hat die Autorschaft auch weitere Publikationen veröffentlicht? Bemerkung: Die Arbeit wurde von dem Absolventen der fhnw (Fachhochschule Nordwestschweiz Hochschule für Witrschaft) veröffentlicht
Ist die Quelle korrekt?
☒ Gibt es unterstützende Beweise? ☒ Wird die Quelle zitiert und gibt es seriöse Querverweise? ☒ Wurden die Informationen von Experten oder Faktenprüfern überprüft? Was sagen andere Experten dazu? ☐ Gibt es Rechtschreib- oder andere Fehler? ☒ Stimmt diese Quelle mit anderen Quellen überein, die dieses Thema behandeln? Bemerkung: In der Arbeit wurden die zitierte Quellen vermerkt.
Was ist die Absicht hinter der Quelle?
☒ Warum wurde diese Information erstellt? Sollen sie etwas fördern? Anzeigen verkaufen? Stimmen werben? ☒ Ist der Zweck klar? Welchen Zweck verfolge ich und welche Vorurteile haben ich? Welche Vorurteile kann ich bei mir feststellen? ☒ Ist die Quelle objektiv und sachlich? ☒ Ist die Absicht klar ersichtlich? Bemerkung:

Titel: Aufdecken digitaler Beweise Durch Dokumentenanalyse. Analyse von Bildern und Dokumenten.
Autor: Michèle Trebo, Ralph Meier
Ist es aktuell?
☒ Wurde sie kürzlich genug geschrieben, um korrekt zu sein? ☒ Wurde sie in zeitlichem Zusammenhang zum Ereignis/Thema geschrieben? ☒ Funktionieren die Links? Bemerkung:
Ist es bedeutsam für mein Forschungsfrage?
☒ Beziehen sich die Informationen auf das Thema oder beantworten sie meine Frage? ☒ Wer ist das Zielpublikum? An wen richtet sich die Quelle? ☒ Bietet diese Quelle eine neue Perspektive oder Information? ☒ Ist sie technisch genug? Bemerkung: Der Artikel bezieht sich auf das Thema.
Ist es verlässlich/vertrauenswürdig?
☒ Wer hat sie geschrieben, veröffentlicht oder bekannt gemacht? ☒ Sind Kontaktangaben vorhanden? ☒ Was macht die Autorschaft zu einem Experten? ☐ Wird sie von einer Institution unterstützt? ☒ Hat die Autorschaft auch weitere Publikationen veröffentlicht? Bemerkung:
Ist die Quelle korrekt?
☒ Gibt es unterstützende Beweise? ☒ Wird die Quelle zitiert und gibt es seriöse Querverweise? ☒ Wurden die Informationen von Experten oder Faktenprüfern überprüft? Was sagen andere Experten dazu? ☐ Gibt es Rechtschreib- oder andere Fehler? ☒ Stimmt diese Quelle mit anderen Quellen überein, die dieses Thema behandeln? Bemerkung: In der Arbeit wurden die zitierte Quellen vermerkt.
Was ist die Absicht hinter der Quelle?
☒ Warum wurde diese Information erstellt? Sollen sie etwas fördern? Anzeigen verkaufen? Stimmen werben? ☒ Ist der Zweck klar? Welchen Zweck verfolge ich und welche Vorurteile haben ich? Welche Vorurteile kann ich bei mir feststellen? ☒ Ist die Quelle objektiv und sachlich? ☒ Ist die Absicht klar ersichtlich? Bemerkung:

Titel: Digital Chain of Custody: State of the Art
Autor: Yudi Prayudi, Azhari SN
Ist es aktuell?
☐ Wurde sie kürzlich genug geschrieben, um korrekt zu sein? ☒ Wurde sie in zeitlichem Zusammenhang zum Ereignis/Thema geschrieben? ☒ Funktionieren die Links? Bemerkung: Es handelt sich um eine Wissenschaftliche Arbeit aus dem Jahr 2015
Ist es bedeutsam für mein Forschungsfrage?
☒ Beziehen sich die Informationen auf das Thema oder beantworten sie meine Frage? ☒ Wer ist das Zielpublikum? An wen richtet sich die Quelle? ☒ Bietet diese Quelle eine neue Perspektive oder Information? ☒ Ist sie technisch genug? Bemerkung: Der Artikel bezieht sich auf das Thema.
Ist es verlässlich/vertrauenswürdig?
☒ Wer hat sie geschrieben, veröffentlicht oder bekannt gemacht? ☒ Sind Kontaktangaben vorhanden? ☒ Was macht die Autorschaft zu einem Experten? ☐ Wird sie von einer Institution unterstützt? ☐ Hat die Autorschaft auch weitere Publikationen veröffentlicht? Bemerkung:
Ist die Quelle korrekt?
☒ Gibt es unterstützende Beweise? ☒ Wird die Quelle zitiert und gibt es seriöse Querverweise? ☒ Wurden die Informationen von Experten oder Faktenprüfern überprüft? Was sagen andere Experten dazu? ☐ Gibt es Rechtschreib- oder andere Fehler? ☒ Stimmt diese Quelle mit anderen Quellen überein, die dieses Thema behandeln? Bemerkung: In der Arbeit wurden die zitierte Quellen vermerkt.
Was ist die Absicht hinter der Quelle?
☒ Warum wurde diese Information erstellt? Sollen sie etwas fördern? Anzeigen verkaufen? Stimmen werben? ☒ Ist der Zweck klar? Welchen Zweck verfolge ich und welche Vorurteile haben ich? Welche Vorurteile kann ich bei mir feststellen? ☒ Ist die Quelle objektiv und sachlich? ☒ Ist die Absicht klar ersichtlich? Bemerkung:

CRAAP Test Kapitel 2

Titel: Write Blocker
Author: 030 Datenrettung Berlin
Ist es aktuell?
☒ Wurde sie kürzlich genug geschrieben, um korrekt zu sein? ☒ Wurde sie in zeitlichem Zusammenhang zum Ereignis/Thema geschrieben? ☒ Funktionieren die Links? Bemerkung:
Ist es bedeutsam für mein Forschungsfrage?
☒ Beziehen sich die Informationen auf das Thema oder beantworten sie meine Frage? ☒ Wer ist das Zielpublikum? An wen richtet sich die Quelle? ☒ Ist sie technisch genug? Bemerkung: Der Artikel bezieht sich auf das Thema.
Ist es verlässlich/vertrauenswürdig?
☒ Wer hat sie geschrieben, veröffentlicht oder bekannt gemacht? ☒ Sind Kontaktangaben vorhanden? ☒ Was macht die Autorschaft zu einem Experten? ☒ Hat die Autorschaft auch weitere Publikationen veröffentlicht? Bemerkung: Der Author ist ein Serviceanbieter in diesem Gebiet.
Ist die Quelle korrekt?
☒ Wird die Quelle zitiert und gibt es seriöse Querverweise? ☒ Gibt es Rechtschreib- oder andere Fehler? ☒ Stimmt diese Quelle mit anderen Quellen überein, die dieses Thema behandeln? Bemerkung:
Was ist die Absicht hinter der Quelle?
☒ Warum wurde diese Information erstellt? Sollen sie etwas fördern? Anzeigen verkaufen? Stimmen werben? ☒ Ist der Zweck klar? Welchen Zweck verfolge ich und welche Vorurteile haben ich? Welche Vorurteile kann ich bei mir feststellen? ☒ Ist die Quelle objektiv und sachlich? ☒ Ist die Absicht klar ersichtlich? Bemerkung: Die Absicht ist Write-Blocker zu erläutern.

Titel: Preserving chain of custody in digital forensics
Author: Belkasoft
Ist es aktuell?
☒ Wurde sie kürzlich genug geschrieben, um korrekt zu sein? ☒ Wurde sie in zeitlichem Zusammenhang zum Ereignis/Thema geschrieben? ☒ Funktionieren die Links? Bemerkung:
Ist es bedeutsam für mein Forschungsfrage?
☒ Beziehen sich die Informationen auf das Thema oder beantworten sie meine Frage? ☒ Wer ist das Zielpublikum? An wen richtet sich die Quelle? ☒ Bietet diese Quelle eine neue Perspektive oder Information? ☒ Ist sie technisch genug? Bemerkung: Der Artikel bezieht sich auf das Thema.
Ist es verlässlich/vertrauenswürdig?
☒ Wer hat sie geschrieben, veröffentlicht oder bekannt gemacht? ☒ Sind Kontaktangaben vorhanden? ☒ Was macht die Autorschaft zu einem Experten? ☒ Hat die Autorschaft auch weitere Publikationen veröffentlicht? Bemerkung: Der Author ist ein Serviceanbieter in diesem Gebiet.
Ist die Quelle korrekt?
☒ Gibt es unterstützende Beweise? ☒ Wird die Quelle zitiert und gibt es seriöse Querverweise? ☒ Gibt es Rechtschreib- oder andere Fehler? ☒ Stimmt diese Quelle mit anderen Quellen überein, die dieses Thema behandeln? Bemerkung:
Was ist die Absicht hinter der Quelle?
☒ Warum wurde diese Information erstellt? Sollen sie etwas fördern? Anzeigen verkaufen? Stimmen werben? ☒ Ist der Zweck klar? Welchen Zweck verfolge ich und welche Vorurteile haben ich? Welche Vorurteile kann ich bei mir feststellen? ☒ Ist die Quelle objektiv und sachlich? ☒ Ist die Absicht klar ersichtlich? Bemerkung: Die Quelle erklärt die Chain of Custody.

Titel: Computer forensics: Chain of custody
Author: Lester Obbayi
Ist es aktuell?
☒ Wurde sie kürzlich genug geschrieben, um korrekt zu sein? ☒ Wurde sie in zeitlichem Zusammenhang zum Ereignis/Thema geschrieben? ☒ Funktionieren die Links? Bemerkung: Keine
Ist es bedeutsam für mein Forschungsfrage?
☒ Beziehen sich die Informationen auf das Thema oder beantworten sie meine Frage? ☒ Wer ist das Zielpublikum? An wen richtet sich die Quelle? ☒ Bietet diese Quelle eine neue Perspektive oder Information? ☒ Ist sie technisch genug? Bemerkung: Der Artikel bezieht sich auf das Thema.
Ist es verlässlich/vertrauenswürdig?
☒ Wer hat sie geschrieben, veröffentlicht oder bekannt gemacht? ☒ Sind Kontaktangaben vorhanden? ☒ Was macht die Autorschaft zu einem Experten? ☒ Hat die Autorschaft auch weitere Publikationen veröffentlicht? Bemerkung: Keine
Ist die Quelle korrekt?
☒ Gibt es unterstützende Beweise? ☒ Wird die Quelle zitiert und gibt es seriöse Querverweise? ☒ Gibt es Rechtschreib- oder andere Fehler? ☒ Stimmt diese Quelle mit anderen Quellen überein, die dieses Thema behandeln? Bemerkung: Keine
Was ist die Absicht hinter der Quelle?
☒ Warum wurde diese Information erstellt? Sollen sie etwas fördern? Anzeigen verkaufen? Stimmen werben? ☒ Ist der Zweck klar? Welchen Zweck verfolge ich und welche Vorurteile haben ich? Welche Vorurteile kann ich bei mir feststellen? ☒ Ist die Quelle objektiv und sachlich? ☒ Ist die Absicht klar ersichtlich? Bemerkung: Erläutert Chain of Custody.

Titel: hashing
Author: Andrew Zola
Ist es aktuell?
☒ Wurde sie kürzlich genug geschrieben, um korrekt zu sein? ☒ Wurde sie in zeitlichem Zusammenhang zum Ereignis/Thema geschrieben? ☒ Funktionieren die Links? Bemerkung: Keine
Ist es bedeutsam für mein Forschungsfrage?
☒ Beziehen sich die Informationen auf das Thema oder beantworten sie meine Frage? ☒ Wer ist das Zielpublikum? An wen richtet sich die Quelle? ☒ Bietet diese Quelle eine neue Perspektive oder Information? ☒ Ist sie technisch genug? Bemerkung: Der Artikel bezieht sich auf das Thema.
Ist es verlässlich/vertrauenswürdig?
☒ Wer hat sie geschrieben, veröffentlicht oder bekannt gemacht? ☒ Sind Kontaktangaben vorhanden? ☒ Was macht die Autorschaft zu einem Experten? ☒ Hat die Autorschaft auch weitere Publikationen veröffentlicht? Bemerkung: Keine
Ist die Quelle korrekt?
☒ Gibt es unterstützende Beweise? ☒ Wird die Quelle zitiert und gibt es seriöse Querverweise? ☒ Gibt es Rechtschreib- oder andere Fehler? ☒ Stimmt diese Quelle mit anderen Quellen überein, die dieses Thema behandeln? Bemerkung: Keine
Was ist die Absicht hinter der Quelle?
☒ Warum wurde diese Information erstellt? Sollen sie etwas fördern? Anzeigen verkaufen? Stimmen werben? ☒ Ist der Zweck klar? Welchen Zweck verfolge ich und welche Vorurteile haben ich? Welche Vorurteile kann ich bei mir feststellen? ☒ Ist die Quelle objektiv und sachlich? ☒ Ist die Absicht klar ersichtlich? Bemerkung: Erklärt was Hashing ist.

Titel: Datenintegrität: Was ist das und wie ist sie aufrecht zu erhalten?
Author: Michael Buckbee
Ist es aktuell?
☒ Wurde sie kürzlich genug geschrieben, um korrekt zu sein? ☒ Wurde sie in zeitlichem Zusammenhang zum Ereignis/Thema geschrieben? ☒ Funktionieren die Links? Bemerkung:
Ist es bedeutsam für mein Forschungsfrage?
☒ Beziehen sich die Informationen auf das Thema oder beantworten sie meine Frage? ☒ Wer ist das Zielpublikum? An wen richtet sich die Quelle? ☒ Bietet diese Quelle eine neue Perspektive oder Information? ☒ Ist sie technisch genug? Bemerkung: Der Artikel bezieht sich auf das Thema.
Ist es verlässlich/vertrauenswürdig?
☒ Wer hat sie geschrieben, veröffentlicht oder bekannt gemacht? ☒ Sind Kontaktangaben vorhanden? ☒ Was macht die Autorschaft zu einem Experten? ☒ Wird sie von einer Institution unterstützt? ☒ Hat die Autorschaft auch weitere Publikationen veröffentlicht? Bemerkung: Der Author ist eine Security Firma.
Ist die Quelle korrekt?
☒ Gibt es unterstützende Beweise? ☒ Wird die Quelle zitiert und gibt es seriöse Querverweise? ☒ Gibt es Rechtschreib- oder andere Fehler? ☒ Stimmt diese Quelle mit anderen Quellen überein, die dieses Thema behandeln? Bemerkung:
Was ist die Absicht hinter der Quelle?
☒ Warum wurde diese Information erstellt? Sollen sie etwas fördern? Anzeigen verkaufen? Stimmen werben? ☒ Ist der Zweck klar? Welchen Zweck verfolge ich und welche Vorurteile haben ich? Welche Vorurteile kann ich bei mir feststellen? ☒ Ist die Quelle objektiv und sachlich? ☒ Ist die Absicht klar ersichtlich? Bemerkung: Aufklärung über Datenintegrität.

Titel: Write Blockers
Author: CRU
Ist es aktuell?
☒ Wurde sie kürzlich genug geschrieben, um korrekt zu sein? ☒ Wurde sie in zeitlichem Zusammenhang zum Ereignis/Thema geschrieben? ☒ Funktionieren die Links? Bemerkung:
Ist es bedeutsam für mein Forschungsfrage?
☒ Beziehen sich die Informationen auf das Thema oder beantworten sie meine Frage? ☒ Wer ist das Zielpublikum? An wen richtet sich die Quelle? ☒ Bietet diese Quelle eine neue Perspektive oder Information? ☒ Ist sie technisch genug? Bemerkung: Der Artikel bezieht sich auf das Thema.
Ist es verlässlich/vertrauenswürdig?
☒ Wer hat sie geschrieben, veröffentlicht oder bekannt gemacht? ☒ Sind Kontaktangaben vorhanden? ☒ Was macht die Autorschaft zu einem Experten? ☒ Hat die Autorschaft auch weitere Publikationen veröffentlicht? Bemerkung:
Ist die Quelle korrekt?
☒ Gibt es unterstützende Beweise? ☒ Wird die Quelle zitiert und gibt es seriöse Querverweise? ☒ Gibt es Rechtschreib- oder andere Fehler? ☒ Stimmt diese Quelle mit anderen Quellen überein, die dieses Thema behandeln? Bemerkung:
Was ist die Absicht hinter der Quelle?
☒ Warum wurde diese Information erstellt? Sollen sie etwas fördern? Anzeigen verkaufen? Stimmen werben? ☒ Ist der Zweck klar? Welchen Zweck verfolge ich und welche Vorurteile haben ich? Welche Vorurteile kann ich bei mir feststellen? ☒ Ist die Quelle objektiv und sachlich? ☒ Ist die Absicht klar ersichtlich? Bemerkung: Aufklärung über Write-Blocker

Titel: What is a timestamping authority?
Author: Mike Hathaway
Ist es aktuell?
☒ Wurde sie kürzlich genug geschrieben, um korrekt zu sein? ☒ Wurde sie in zeitlichem Zusammenhang zum Ereignis/Thema geschrieben? ☒ Funktionieren die Links? Bemerkung: Keine
Ist es bedeutsam für mein Forschungsfrage?
☒ Beziehen sich die Informationen auf das Thema oder beantworten sie meine Frage? ☒ Wer ist das Zielpublikum? An wen richtet sich die Quelle? ☒ Bietet diese Quelle eine neue Perspektive oder Information? ☒ Ist sie technisch genug? Bemerkung: Der Artikel bezieht sich auf das Thema.
Ist es verlässlich/vertrauenswürdig?
☒ Wer hat sie geschrieben, veröffentlicht oder bekannt gemacht? ☒ Sind Kontaktangaben vorhanden? ☒ Was macht die Autorschaft zu einem Experten? ☒ Hat die Autorschaft auch weitere Publikationen veröffentlicht? Bemerkung: Keine
Ist die Quelle korrekt?
☒ Gibt es unterstützende Beweise? ☒ Wird die Quelle zitiert und gibt es seriöse Querverweise? ☒ Gibt es Rechtschreib- oder andere Fehler? ☒ Stimmt diese Quelle mit anderen Quellen überein, die dieses Thema behandeln? Bemerkung: Keine
Was ist die Absicht hinter der Quelle?
☒ Warum wurde diese Information erstellt? Sollen sie etwas fördern? Anzeigen verkaufen? Stimmen werben? ☒ Ist der Zweck klar? Welchen Zweck verfolge ich und welche Vorurteile haben ich? Welche Vorurteile kann ich bei mir feststellen? ☒ Ist die Quelle objektiv und sachlich? ☒ Ist die Absicht klar ersichtlich? Bemerkung: Klärt auf, was eine Timestamp Authority ist.

Titel: Was ist Datensicherheit?
Author: IBM
Ist es aktuell?
☒ Wurde sie kürzlich genug geschrieben, um korrekt zu sein? ☒ Wurde sie in zeitlichem Zusammenhang zum Ereignis/Thema geschrieben? ☒ Funktionieren die Links? Bemerkung: Keine
Ist es bedeutsam für mein Forschungsfrage?
☒ Beziehen sich die Informationen auf das Thema oder beantworten sie meine Frage? ☒ Wer ist das Zielpublikum? An wen richtet sich die Quelle? ☒ Bietet diese Quelle eine neue Perspektive oder Information? ☒ Ist sie technisch genug? Bemerkung: Der Artikel bezieht sich auf das Thema.
Ist es verlässlich/vertrauenswürdig?
☒ Wer hat sie geschrieben, veröffentlicht oder bekannt gemacht? ☒ Sind Kontaktangaben vorhanden? ☒ Was macht die Autorschaft zu einem Experten? ☒ Hat die Autorschaft auch weitere Publikationen veröffentlicht? Bemerkung: Keine
Ist die Quelle korrekt?
☒ Gibt es unterstützende Beweise? ☒ Wird die Quelle zitiert und gibt es seriöse Querverweise? ☒ Wurden die Informationen von Experten oder Faktenprüfern überprüft? Was sagen andere Experten dazu? ☒ Gibt es Rechtschreib- oder andere Fehler? ☒ Stimmt diese Quelle mit anderen Quellen überein, die dieses Thema behandeln? Bemerkung: Keine
Was ist die Absicht hinter der Quelle?
☒ Warum wurde diese Information erstellt? Sollen sie etwas fördern? Anzeigen verkaufen? Stimmen werben? ☒ Ist der Zweck klar? Welchen Zweck verfolge ich und welche Vorurteile haben ich? Welche Vorurteile kann ich bei mir feststellen? ☒ Ist die Quelle objektiv und sachlich? ☒ Ist die Absicht klar ersichtlich? Bemerkung: Erklärt den Begriff Datensicherheit.

Titel: What is a timestamp and how does it work?
Author: Namirial
Ist es aktuell?
☒ Wurde sie kürzlich genug geschrieben, um korrekt zu sein? ☒ Wurde sie in zeitlichem Zusammenhang zum Ereignis/Thema geschrieben? ☒ Funktionieren die Links? Bemerkung: Keine
Ist es bedeutsam für mein Forschungsfrage?
☒ Beziehen sich die Informationen auf das Thema oder beantworten sie meine Frage? ☒ Wer ist das Zielpublikum? An wen richtet sich die Quelle? ☒ Bietet diese Quelle eine neue Perspektive oder Information? ☒ Ist sie technisch genug? Bemerkung: Der Artikel bezieht sich auf das Thema.
Ist es verlässlich/vertrauenswürdig?
☒ Wer hat sie geschrieben, veröffentlicht oder bekannt gemacht? ☒ Sind Kontaktangaben vorhanden? ☒ Was macht die Autorschaft zu einem Experten? ☒ Hat die Autorschaft auch weitere Publikationen veröffentlicht? Bemerkung: Keine
Ist die Quelle korrekt?
☒ Gibt es unterstützende Beweise? ☒ Wird die Quelle zitiert und gibt es seriöse Querverweise? ☒ Gibt es Rechtschreib- oder andere Fehler? ☒ Stimmt diese Quelle mit anderen Quellen überein, die dieses Thema behandeln? Bemerkung: Keine
Was ist die Absicht hinter der Quelle?
☒ Warum wurde diese Information erstellt? Sollen sie etwas fördern? Anzeigen verkaufen? Stimmen werben? ☒ Ist der Zweck klar? Welchen Zweck verfolge ich und welche Vorurteile haben ich? Welche Vorurteile kann ich bei mir feststellen? ☒ Ist die Quelle objektiv und sachlich? ☒ Ist die Absicht klar ersichtlich? Bemerkung: Erklärt wie Timestamps funktionieren.

CRAAP Test Kapitel 3

Titel: Krisenfall Ransomware
Author: Florian Oelmaier, Uwe Knebelsberger, Arthur Naefe
Ist es aktuell?
☒ Wurde sie kürzlich genug geschrieben, um korrekt zu sein? ☒ Wurde sie in zeitlichem Zusammenhang zum Ereignis/Thema geschrieben? ☒ Funktionieren die Links? Bemerkung:
Ist es bedeutsam für mein Forschungsfrage?
☒ Beziehen sich die Informationen auf das Thema oder beantworten sie meine Frage? ☒ Wer ist das Zielpublikum? An wen richtet sich die Quelle? ☒ Bietet diese Quelle eine neue Perspektive oder Information? ☒ Ist sie technisch genug? Bemerkung: Der Artikel bezieht sich auf das Thema.
Ist es verlässlich/vertrauenswürdig?
☒ Wer hat sie geschrieben, veröffentlicht oder bekannt gemacht? ☒ Sind Kontaktangaben vorhanden? ☒ Was macht die Autorschaft zu einem Experten? ☒ Wird sie von einer Institution unterstützt? ☒ Hat die Autorschaft auch weitere Publikationen veröffentlicht? Bemerkung:
Ist die Quelle korrekt?
☒ Gibt es unterstützende Beweise? ☒ Wird die Quelle zitiert und gibt es seriöse Querverweise? ☒ Wurden die Informationen von Experten oder Faktenprüfern überprüft? Was sagen andere Experten dazu? ☒ Gibt es Rechtschreib- oder andere Fehler? ☒ Stimmt diese Quelle mit anderen Quellen überein, die dieses Thema behandeln? Bemerkung:
Was ist die Absicht hinter der Quelle?
☒ Warum wurde diese Information erstellt? Sollen sie etwas fördern? Anzeigen verkaufen? Stimmen werben? ☒ Ist der Zweck klar? Welchen Zweck verfolge ich und welche Vorurteile haben ich? Welche Vorurteile kann ich bei mir feststellen? ☒ Ist die Quelle objektiv und sachlich? ☒ Ist die Absicht klar ersichtlich? Bemerkung:

Titel: Computer Hacking
Author: Udo Kebschull
Ist es aktuell?
☒ Wurde sie kürzlich genug geschrieben, um korrekt zu sein? ☒ Wurde sie in zeitlichem Zusammenhang zum Ereignis/Thema geschrieben? ☒ Funktionieren die Links? Bemerkung: Das Buch ist aktuell, aus dem Jahr 2023.
Ist es bedeutsam für mein Forschungsfrage?
☒ Beziehen sich die Informationen auf das Thema oder beantworten sie meine Frage? ☒ Wer ist das Zielpublikum? An wen richtet sich die Quelle? ☒ Bietet diese Quelle eine neue Perspektive oder Information? ☒ Ist sie technisch genug? Bemerkung: Der Artikel bezieht sich auf das Thema.
Ist es verlässlich/vertrauenswürdig?
☒ Wer hat sie geschrieben, veröffentlicht oder bekannt gemacht? ☒ Sind Kontaktangaben vorhanden? ☒ Was macht die Autorschaft zu einem Experten? ☒ Wird sie von einer Institution unterstützt? ☒ Hat die Autorschaft auch weitere Publikationen veröffentlicht? Bemerkung:
Ist die Quelle korrekt?
☒ Gibt es unterstützende Beweise? ☒ Wird die Quelle zitiert und gibt es seriöse Querverweise? ☒ Wurden die Informationen von Experten oder Faktenprüfern überprüft? Was sagen andere Experten dazu? ☒ Gibt es Rechtschreib- oder andere Fehler? ☒ Stimmt diese Quelle mit anderen Quellen überein, die dieses Thema behandeln? Bemerkung: Der Autor hat in seiner Arbeit jeweils seine Quellen angegeben.
Was ist die Absicht hinter der Quelle?
☒ Warum wurde diese Information erstellt? Sollen sie etwas fördern? Anzeigen verkaufen? Stimmen werben? ☒ Ist der Zweck klar? Welchen Zweck verfolge ich und welche Vorurteile haben ich? Welche Vorurteile kann ich bei mir feststellen? ☒ Ist die Quelle objektiv und sachlich? ☒ Ist die Absicht klar ersichtlich? Bemerkung:

CRAAP Test Kapitel 4

Titel: Cybersecurity and Burnout: The Cybersecurity Professional's Silent Enemy
Autor: Andres Ricardo Almanza
Ist es aktuell?
☒ Wurde sie kürzlich genug geschrieben, um korrekt zu sein? ☒ Wurde sie in zeitlichem Zusammenhang zum Ereignis/Thema geschrieben? ☒ Funktionieren die Links? Bemerkung: Der Artikel ist aktuell. Er wurde am 29 November 2023 veröffentlicht und der Link funktioniert.
Ist es bedeutsam für mein Forschungsfrage?
☒ Beziehen sich die Informationen auf das Thema oder beantworten sie meine Frage? ☒ Wer ist das Zielpublikum? An wen richtet sich die Quelle? ☒ Bietet diese Quelle eine neue Perspektive oder Information? ☒ Ist sie technisch genug? Bemerkung: Der Artikel bezieht sich auf das Thema und richtet sich an Fachleute.
Ist es verlässlich/vertrauenswürdig?
☒ Wer hat sie geschrieben, veröffentlicht oder bekannt gemacht? ☒ Sind Kontaktangaben vorhanden? ☒ Was macht die Autorschaft zu einem Experten? ☐ Wird sie von einer Institution unterstützt? ☐ Hat die Autorschaft auch weitere Publikationen veröffentlicht? Bemerkung: Der Autor ist ein Fachexperte im Bereich Infomation Security.
Ist die Quelle korrekt?
☒ Gibt es unterstützende Beweise? ☒ Wird die Quelle zitiert und gibt es seriöse Querverweise? ☒ Wurden die Informationen von Experten oder Faktenprüfern überprüft? Was sagen andere Experten dazu? ☐ Gibt es Rechtschreib- oder andere Fehler? ☒ Stimmt diese Quelle mit anderen Quellen überein, die dieses Thema behandeln? Bemerkung: In dem Artikel wurden die verwendeten Quellen korrekt zitiert.
Was ist die Absicht hinter der Quelle?
☒ Warum wurde diese Information erstellt? Sollen sie etwas fördern? Anzeigen verkaufen? Stimmen werben? ☒ Ist der Zweck klar? Welchen Zweck verfolge ich und welche Vorurteile haben ich? Welche Vorurteile kann ich bei mir feststellen? ☒ Ist die Quelle objektiv und sachlich? ☒ Ist die Absicht klar ersichtlich? Bemerkung: Der Artikel ist objektiv und sachlich geschrieben.

Titel: Security Awareness, Herausforderungen und Lösungsansätze für Mitarbeiter und Unternehmen
Autor: A. Bättig, S. Horvath, A. Kryeziu, S. Mendil, D. Serretti, E. Veseli
Ist es aktuell?
☒ Wurde sie kürzlich genug geschrieben, um korrekt zu sein? ☒ Wurde sie in zeitlichem Zusammenhang zum Ereignis/Thema geschrieben? ☐ Funktionieren die Links? Bemerkung: Es handelt sich um eine Wissenschaftliche Arbeit aus dem Jahr 2023.
Ist es bedeutsam für mein Forschungsfrage?
☒ Beziehen sich die Informationen auf das Thema oder beantworten sie meine Frage? ☒ Wer ist das Zielpublikum? An wen richtet sich die Quelle? ☒ Bietet diese Quelle eine neue Perspektive oder Information? ☒ Ist sie technisch genug? Bemerkung: Der Artikel bezieht sich auf das Thema.
Ist es verlässlich/vertrauenswürdig?
☒ Wer hat sie geschrieben, veröffentlicht oder bekannt gemacht? ☒ Sind Kontaktangaben vorhanden? ☒ Was macht die Autorschaft zu einem Experten? ☐ Wird sie von einer Institution unterstützt? ☐ Hat die Autorschaft auch weitere Publikationen veröffentlicht? Bemerkung: Die Arbeit wurde an der Hochschule Luzern im Rahmen eines Moduls erstellt, jedoch nicht veröffentlicht. Alle Kontaktangaben und wichtigen Informationen sind in der Arbeite ersichtlich.
Ist die Quelle korrekt?
☒ Gibt es unterstützende Beweise? ☒ Wird die Quelle zitiert und gibt es seriöse Querverweise? ☒ Wurden die Informationen von Experten oder Faktenprüfern überprüft? Was sagen andere Experten dazu? ☐ Gibt es Rechtschreib- oder andere Fehler? ☒ Stimmt diese Quelle mit anderen Quellen überein, die dieses Thema behandeln? Bemerkung: In der Arbeit wurden die zitierte Quellen vermerkt.
Was ist die Absicht hinter der Quelle?
☒ Warum wurde diese Information erstellt? Sollen sie etwas fördern? Anzeigen verkaufen? Stimmen werben? ☒ Ist der Zweck klar? Welchen Zweck verfolge ich und welche Vorurteile haben ich? Welche Vorurteile kann ich bei mir feststellen? ☒ Ist die Quelle objektiv und sachlich? ☒ Ist die Absicht klar ersichtlich? Bemerkung:

Titel: Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology
Autor: P. Cichonski, T. Millar, T. Grance, K. Scarfone von National Institute of Standards and Technology
Ist es aktuell?
☒ Wurde sie kürzlich genug geschrieben, um korrekt zu sein? ☒ Wurde sie in zeitlichem Zusammenhang zum Ereignis/Thema geschrieben? ☒ Funktionieren die Links? Bemerkung: Das Framewoke wurde im Jahr 2003 geschrieben, ist aber noch aktuell und wird noch heute verwendet. (Gibt noch kein nachfolgendes Framework, oder Update).
Ist es bedeutsam für mein Forschungsfrage?
☒ Beziehen sich die Informationen auf das Thema oder beantworten sie meine Frage? ☒ Wer ist das Zielpublikum? An wen richtet sich die Quelle? ☒ Bietet diese Quelle eine neue Perspektive oder Information? ☒ Ist sie technisch genug? Bemerkung: Der Artikel bezieht sich auf das Thema.
Ist es verlässlich/vertrauenswürdig?
☒ Wer hat sie geschrieben, veröffentlicht oder bekannt gemacht? ☒ Sind Kontaktangaben vorhanden? ☒ Was macht die Autorschaft zu einem Experten? ☒ Wird sie von einer Institution unterstützt? ☒ Hat die Autorschaft auch weitere Publikationen veröffentlicht? Bemerkung: Der Autor hat schon mehrere Standards und Frameworks veröffentlicht, die international verwendet werden.
Ist die Quelle korrekt?
☒ Gibt es unterstützende Beweise? ☒ Wird die Quelle zitiert und gibt es seriöse Querverweise? ☒ Wurden die Informationen von Experten oder Faktenprüfern überprüft? Was sagen andere Experten dazu? ☐ Gibt es Rechtschreib- oder andere Fehler? ☒ Stimmt diese Quelle mit anderen Quellen überein, die dieses Thema behandeln? Bemerkung: Die Quelle richtet sich an Fachleute und Internehmen in diesem Bereich.
Was ist die Absicht hinter der Quelle?
☒ Warum wurde diese Information erstellt? Sollen sie etwas fördern? Anzeigen verkaufen? Stimmen werben? ☒ Ist der Zweck klar? Welchen Zweck verfolge ich und welche Vorurteile haben ich? Welche Vorurteile kann ich bei mir feststellen? ☒ Ist die Quelle objektiv und sachlich? ☒ Ist die Absicht klar ersichtlich? Bemerkung: Die Quelle ist objektiv und sachlich geschrieben und beinhalten allgemeine Praktiken zum Schutz von Infrastrukturen.

Titel: IT-Forensik
Autor: Dennis Heinson
Ist es aktuell?
☒ Wurde sie kürzlich genug geschrieben, um korrekt zu sein? ☒ Wurde sie in zeitlichem Zusammenhang zum Ereignis/Thema geschrieben? ☒ Funktionieren die Links? Bemerkung: Artikel wurde im 2015 geschrieben, der Inhalt der Verwendet wurde bezieht sich aufs Thema und hat sich bis heute nicht verändert. Ist aktuell.
Ist es bedeutsam für mein Forschungsfrage?
☒ Beziehen sich die Informationen auf das Thema oder beantworten sie meine Frage? ☒ Wer ist das Zielpublikum? An wen richtet sich die Quelle? ☒ Bietet diese Quelle eine neue Perspektive oder Information? ☒ Ist sie technisch genug? Bemerkung: Der Artikel bezieht sich auf das Thema.
Ist es verlässlich/vertrauenswürdig?
☒ Wer hat sie geschrieben, veröffentlicht oder bekannt gemacht? ☒ Sind Kontaktangaben vorhanden? ☒ Was macht die Autorschaft zu einem Experten? ☒ Wird sie von einer Institution unterstützt? ☒ Hat die Autorschaft auch weitere Publikationen veröffentlicht? Bemerkung: Der Autor hat schon mehrere Fachliteraturen veröffentlicht. Die ISBN dieses Buches ist bekannt. ISBN 978-3-16-153701-1
Ist die Quelle korrekt?
☒ Gibt es unterstützende Beweise? ☒ Wird die Quelle zitiert und gibt es seriöse Querverweise? ☒ Wurden die Informationen von Experten oder Faktenprüfern überprüft? Was sagen andere Experten dazu? ☐ Gibt es Rechtschreib- oder andere Fehler? ☒ Stimmt diese Quelle mit anderen Quellen überein, die dieses Thema behandeln? Bemerkung: Der Autor hat in seiner Arbeit jeweils seine Quellen angegeben.
Was ist die Absicht hinter der Quelle?
☒ Warum wurde diese Information erstellt? Sollen sie etwas fördern? Anzeigen verkaufen? Stimmen werben? ☒ Ist der Zweck klar? Welchen Zweck verfolge ich und welche Vorurteile haben ich? Welche Vorurteile kann ich bei mir feststellen? ☒ Ist die Quelle objektiv und sachlich? ☒ Ist die Absicht klar ersichtlich? Bemerkung: Die Quelle ist objektiv und sachlich.

Titel: Information security management systems Requirements (ISO/IEC 27001:2022)
Autor: International Organization for Standardization
Ist es aktuell?
☒ Wurde sie kürzlich genug geschrieben, um korrekt zu sein? ☒ Wurde sie in zeitlichem Zusammenhang zum Ereignis/Thema geschrieben? ☒ Funktionieren die Links? Bemerkung: Der Standard wurde im Jahr 2022 veröffentlicht und wird aktuell verwendet.
Ist es bedeutsam für mein Forschungsfrage?
☒ Beziehen sich die Informationen auf das Thema oder beantworten sie meine Frage? ☒ Wer ist das Zielpublikum? An wen richtet sich die Quelle? ☒ Bietet diese Quelle eine neue Perspektive oder Information? ☒ Ist sie technisch genug? Bemerkung: Der Standard bezieht sich auf das Thema.
Ist es verlässlich/vertrauenswürdig?
☒ Wer hat sie geschrieben, veröffentlicht oder bekannt gemacht? ☒ Sind Kontaktangaben vorhanden? ☒ Was macht die Autorschaft zu einem Experten? ☒ Wird sie von einer Institution unterstützt? ☒ Hat die Autorschaft auch weitere Publikationen veröffentlicht? Bemerkung: Der Autor hat schon mehrere Standards veröffentlicht, die international verwendet werden.
Ist die Quelle korrekt?
☒ Gibt es unterstützende Beweise? ☒ Wird die Quelle zitiert und gibt es seriöse Querverweise? ☒ Wurden die Informationen von Experten oder Faktenprüfern überprüft? Was sagen andere Experten dazu? ☐ Gibt es Rechtschreib- oder andere Fehler? ☒ Stimmt diese Quelle mit anderen Quellen überein, die dieses Thema behandeln? Bemerkung: Die Quelle richtet sich an Fachleute und Internehmen in diesem Bereich.
Was ist die Absicht hinter der Quelle?
☒ Warum wurde diese Information erstellt? Sollen sie etwas fördern? Anzeigen verkaufen? Stimmen werben? ☒ Ist der Zweck klar? Welchen Zweck verfolge ich und welche Vorurteile haben ich? Welche Vorurteile kann ich bei mir feststellen? ☒ Ist die Quelle objektiv und sachlich? ☒ Ist die Absicht klar ersichtlich? Bemerkung: Die Quelle ist objektiv und sachlich geschrieben und wird als Best Practice akzeptiert.

Titel: ISC2 Cybersecurity Workforce Study 2021
Autor: (ISC)²
Ist es aktuell?
☒ Wurde sie kürzlich genug geschrieben, um korrekt zu sein? ☒ Wurde sie in zeitlichem Zusammenhang zum Ereignis/Thema geschrieben? ☒ Funktionieren die Links? Bemerkung: Artikel wurde am 15.10.2021 veröffentlicht. Der Link funktioniert.
Ist es bedeutsam für mein Forschungsfrage?
☒ Beziehen sich die Informationen auf das Thema oder beantworten sie meine Frage? ☒ Wer ist das Zielpublikum? An wen richtet sich die Quelle? ☒ Bietet diese Quelle eine neue Perspektive oder Information? ☒ Ist sie technisch genug? Bemerkung: Der Artikel bezieht sich auf das Thema.
Ist es verlässlich/vertrauenswürdig?
☒ Wer hat sie geschrieben, veröffentlicht oder bekannt gemacht? ☒ Sind Kontaktangaben vorhanden? ☒ Was macht die Autorschaft zu einem Experten? ☒ Wird sie von einer Institution unterstützt? ☒ Hat die Autorschaft auch weitere Publikationen veröffentlicht? Bemerkung: Der Autor hat schon mehrere Statistiken und Forschungen veröffentlicht.
Ist die Quelle korrekt?
☒ Gibt es unterstützende Beweise? ☒ Wird die Quelle zitiert und gibt es seriöse Querverweise? ☒ Wurden die Informationen von Experten oder Faktenprüfern überprüft? Was sagen andere Experten dazu? ☐ Gibt es Rechtschreib- oder andere Fehler? ☒ Stimmt diese Quelle mit anderen Quellen überein, die dieses Thema behandeln? Bemerkung: Die Quelle richtet sich an Fachleute in diesem Bereich.
Was ist die Absicht hinter der Quelle?
☒ Warum wurde diese Information erstellt? Sollen sie etwas fördern? Anzeigen verkaufen? Stimmen werben? ☒ Ist der Zweck klar? Welchen Zweck verfolge ich und welche Vorurteile haben ich? Welche Vorurteile kann ich bei mir feststellen? ☒ Ist die Quelle objektiv und sachlich? ☒ Ist die Absicht klar ersichtlich? Bemerkung:

Titel: Digital Forensics and Incident Response
Autor: Gerard Johansen
Ist es aktuell?
☒ Wurde sie kürzlich genug geschrieben, um korrekt zu sein? ☒ Wurde sie in zeitlichem Zusammenhang zum Ereignis/Thema geschrieben? ☒ Funktionieren die Links? Bemerkung: Das Buch ist aktuell. Es wurde im Dezember 2022 veröffentlich.
Ist es bedeutsam für mein Forschungsfrage?
☒ Beziehen sich die Informationen auf das Thema oder beantworten sie meine Frage? ☒ Wer ist das Zielpublikum? An wen richtet sich die Quelle? ☒ Bietet diese Quelle eine neue Perspektive oder Information? ☒ Ist sie technisch genug? Bemerkung: Das Buch bezieht sich auf das Thema.
Ist es verlässlich/vertrauenswürdig?
☒ Wer hat sie geschrieben, veröffentlicht oder bekannt gemacht? ☒ Sind Kontaktangaben vorhanden? ☒ Was macht die Autorschaft zu einem Experten? ☐ Wird sie von einer Institution unterstützt? ☒ Hat die Autorschaft auch weitere Publikationen veröffentlicht? Bemerkung: Der Autor hat schon mehrere Fachbücher veröffentlicht. Er hat zuvor bereits verschiedene Bücher zu diesem Thema veröffentlicht. Bei diesem Buch handelt es sich um die dritte Auflage mit der ISBN 978-1-80323-867-8.
Ist die Quelle korrekt?
☒ Gibt es unterstützende Beweise? ☒ Wird die Quelle zitiert und gibt es seriöse Querverweise? ☒ Wurden die Informationen von Experten oder Faktenprüfern überprüft? Was sagen andere Experten dazu? ☐ Gibt es Rechtschreib- oder andere Fehler? ☒ Stimmt diese Quelle mit anderen Quellen überein, die dieses Thema behandeln? Bemerkung: Die Quelle richtet sich an Fachleute und Unternehmen in diesem Bereich.
Was ist die Absicht hinter der Quelle?
☒ Warum wurde diese Information erstellt? Sollen sie etwas fördern? Anzeigen verkaufen? Stimmen werben? ☒ Ist der Zweck klar? Welchen Zweck verfolge ich und welche Vorurteile haben ich? Welche Vorurteile kann ich bei mir feststellen? ☒ Ist die Quelle objektiv und sachlich? ☒ Ist die Absicht klar ersichtlich? Bemerkung: Das Buch ist objektiv und sachlich geschrieben. Die Absicht hinter dieser Quelle besteht darin, Wissen im Bereich der Incident Response zu vermitteln.

Titel: Computer Hacking: Eine Einführung zur Verbesserung der Computersicherheit in komplexen IT-Infrastrukturen
Autor: Udo Kebschull
Ist es aktuell?
☒ Wurde sie kürzlich genug geschrieben, um korrekt zu sein? ☒ Wurde sie in zeitlichem Zusammenhang zum Ereignis/Thema geschrieben? ☒ Funktionieren die Links? Bemerkung: Das Buch ist aktuell. Es wurde im Jahr 2023 veröffentlich.
Ist es bedeutsam für mein Forschungsfrage?
☒ Beziehen sich die Informationen auf das Thema oder beantworten sie meine Frage? ☒ Wer ist das Zielpublikum? An wen richtet sich die Quelle? ☒ Bietet diese Quelle eine neue Perspektive oder Information? ☒ Ist sie technisch genug? Bemerkung: Das Buch bezieht sich auf das Thema.
Ist es verlässlich/vertrauenswürdig?
☒ Wer hat sie geschrieben, veröffentlicht oder bekannt gemacht? ☒ Sind Kontaktangaben vorhanden? ☒ Was macht die Autorschaft zu einem Experten? ☒ Wird sie von einer Institution unterstützt? ☒ Hat die Autorschaft auch weitere Publikationen veröffentlicht? Bemerkung: Der Autor Prof. Dr. Udo Kebschull hat schon mehrere Fachbücher veröffentlicht. ISBN: 978-3-662-67030-9
Ist die Quelle korrekt?
☒ Gibt es unterstützende Beweise? ☒ Wird die Quelle zitiert und gibt es seriöse Querverweise? ☒ Wurden die Informationen von Experten oder Faktenprüfern überprüft? Was sagen andere Experten dazu? ☐ Gibt es Rechtschreib- oder andere Fehler? ☒ Stimmt diese Quelle mit anderen Quellen überein, die dieses Thema behandeln? Bemerkung: Die Quelle richtet sich an Fachleute und Unternehmen in diesem Bereich.
Was ist die Absicht hinter der Quelle?
☒ Warum wurde diese Information erstellt? Sollen sie etwas fördern? Anzeigen verkaufen? Stimmen werben? ☒ Ist der Zweck klar? Welchen Zweck verfolge ich und welche Vorurteile haben ich? Welche Vorurteile kann ich bei mir feststellen? ☒ Ist die Quelle objektiv und sachlich? ☒ Ist die Absicht klar ersichtlich? Bemerkung: Das Buch ist objektiv und sachlich geschrieben. Das Buch wurde als Lehrbuch geschrieben, und hat die Absicht Wissen zu vermitteln.

Titel: SANS - The Incident Handlers Handbook
Autor: Patrick Kral
Ist es aktuell?
☒ Wurde sie kürzlich genug geschrieben, um korrekt zu sein? ☒ Wurde sie in zeitlichem Zusammenhang zum Ereignis/Thema geschrieben? ☒ Funktionieren die Links? Bemerkung: Die Arbeit wurde im Jahr 2011 veröffentlicht. Diese Quelle behandelt operationelle Aspekte, welche sich in der Zeit nicht gross verändert haben und wozu es nicht viele neuere Quellen gibt. Daher kann diese noch als aktuell angesehen werden. Der Link zur Quelle funktioniert.
Ist es bedeutsam für mein Forschungsfrage?
☒ Beziehen sich die Informationen auf das Thema oder beantworten sie meine Frage? ☒ Wer ist das Zielpublikum? An wen richtet sich die Quelle? ☒ Bietet diese Quelle eine neue Perspektive oder Information? ☒ Ist sie technisch genug? Bemerkung: Das Arbeit bezieht sich auf das Thema und bietet einen überblick, wie man bei einem Sicherheitsvorfall umgehen sollte.
Ist es verlässlich/vertrauenswürdig?
☒ Wer hat sie geschrieben, veröffentlicht oder bekannt gemacht? ☒ Sind Kontaktangaben vorhanden? ☒ Was macht die Autorschaft zu einem Experten? ☒ Wird sie von einer Institution unterstützt? ☒ Hat die Autorschaft auch weitere Publikationen veröffentlicht? Bemerkung: Die Institution SANS Institute, die die Arbeit veröffentlicht hat, ist in der IT-Sicherheitsbranche anerkannt.
Ist die Quelle korrekt?
☒ Gibt es unterstützende Beweise? ☒ Wird die Quelle zitiert und gibt es seriöse Querverweise? ☒ Wurden die Informationen von Experten oder Faktenprüfern überprüft? Was sagen andere Experten dazu? ☐ Gibt es Rechtschreib- oder andere Fehler? ☒ Stimmt diese Quelle mit anderen Quellen überein, die dieses Thema behandeln? Bemerkung: Die Quelle richtet sich an Fachleute und Unternehmen in diesem Bereich. In der Arbeit wurden die verwendeten Quellen korrekt zitiert.
Was ist die Absicht hinter der Quelle?
☒ Warum wurde diese Information erstellt? Sollen sie etwas fördern? Anzeigen verkaufen? Stimmen werben? ☒ Ist der Zweck klar? Welchen Zweck verfolge ich und welche Vorurteile haben ich? Welche Vorurteile kann ich bei mir feststellen? ☒ Ist die Quelle objektiv und sachlich? ☒ Ist die Absicht klar ersichtlich? Bemerkung: Das Arbeit ist objektiv und sachlich geschrieben. Die Absicht hinter dieser Quelle besteht darin, Informationen im Bereich Incident Handlichg zu vermitteln.

Titel: Ending Support in 2023—Microsoft Lifecycle.
Autor: Microsoft
Ist es aktuell?
☒ Wurde sie kürzlich genug geschrieben, um korrekt zu sein? ☒ Wurde sie in zeitlichem Zusammenhang zum Ereignis/Thema geschrieben? ☒ Funktionieren die Links? Bemerkung: Artikel wurde am 28.08.2023 veröffentlicht. Der Link funktioniert.
Ist es bedeutsam für mein Forschungsfrage?
☒ Beziehen sich die Informationen auf das Thema oder beantworten sie meine Frage? ☒ Wer ist das Zielpublikum? An wen richtet sich die Quelle? ☒ Bietet diese Quelle eine neue Perspektive oder Information? ☒ Ist sie technisch genug? Bemerkung: Der Artikel bezieht sich auf das Thema und scheint an Kunden oder Fachpersonen von Microsoft ausgerichtet zu sein.
Ist es verlässlich/vertrauenswürdig?
☒ Wer hat sie geschrieben, veröffentlicht oder bekannt gemacht? ☒ Sind Kontaktangaben vorhanden? ☒ Was macht die Autorschaft zu einem Experten? ☒ Wird sie von einer Institution unterstützt? ☒ Hat die Autorschaft auch weitere Publikationen veröffentlicht? Bemerkung: Der Autor ist eine grosse Betriebssystemunternehmung. Die Quelle wurde direkt vom Hersteller veröffentlicht.
Ist die Quelle korrekt?
☒ Gibt es unterstützende Beweise? ☒ Wird die Quelle zitiert und gibt es seriöse Querverweise? ☒ Wurden die Informationen von Experten oder Faktenprüfern überprüft? Was sagen andere Experten dazu? ☐ Gibt es Rechtschreib- oder andere Fehler? ☒ Stimmt diese Quelle mit anderen Quellen überein, die dieses Thema behandeln? Bemerkung: Die Quelle ist eine offizielle Anerkündigung von einer bekannten Unternehmung.
Was ist die Absicht hinter der Quelle?
☒ Warum wurde diese Information erstellt? Sollen sie etwas fördern? Anzeigen verkaufen? Stimmen werben? ☒ Ist der Zweck klar? Welchen Zweck verfolge ich und welche Vorurteile haben ich? Welche Vorurteile kann ich bei mir feststellen? ☒ Ist die Quelle objektiv und sachlich? ☒ Ist die Absicht klar ersichtlich? Bemerkung: Die Absicht dieser Quelle ist informativ, um Kunden über wichtige Änderungen in der Unterstützung von Produkten zu informieren.

Titel: Building an Information Technology Security Awareness and Training Program (NIST SP 800-50)
Autor: M.Wilson, J. Hash von National Institute of Standards and Technology
Ist es aktuell?
☒ Wurde sie kürzlich genug geschrieben, um korrekt zu sein? ☒ Wurde sie in zeitlichem Zusammenhang zum Ereignis/Thema geschrieben? ☒ Funktionieren die Links? Bemerkung: Das Framewoke wurde im Jahr 2003 geschrieben, ist aber noch aktuell und wird noch heute verwendet. Es gibt seit dem 28. August 2023 ein neuer upgedateter Entwurf, der jedoch noch nicht offiziell ist und es noch weitere Änderungen geben kann. Es gibt keine Änderungen, die das Kapitel betreffen.
Ist es bedeutsam für mein Forschungsfrage?
☒ Beziehen sich die Informationen auf das Thema oder beantworten sie meine Frage? ☒ Wer ist das Zielpublikum? An wen richtet sich die Quelle? ☒ Bietet diese Quelle eine neue Perspektive oder Information? ☒ Ist sie technisch genug? Bemerkung: Der Artikel bezieht sich auf das Thema.
Ist es verlässlich/vertrauenswürdig?
☒ Wer hat sie geschrieben, veröffentlicht oder bekannt gemacht? ☒ Sind Kontaktangaben vorhanden? ☒ Was macht die Autorschaft zu einem Experten? ☒ Wird sie von einer Institution unterstützt? ☒ Hat die Autorschaft auch weitere Publikationen veröffentlicht? Bemerkung: Der Autor hat schon mehrere Standards und Frameworks veröffentlicht, die international verwendet werden.
Ist die Quelle korrekt?
☒ Gibt es unterstützende Beweise? ☒ Wird die Quelle zitiert und gibt es seriöse Querverweise? ☒ Wurden die Informationen von Experten oder Faktenprüfern überprüft? Was sagen andere Experten dazu? ☐ Gibt es Rechtschreib- oder andere Fehler? ☒ Stimmt diese Quelle mit anderen Quellen überein, die dieses Thema behandeln? Bemerkung: Die Quelle richtet sich an Fachleute und Internehmen in diesem Bereich.
Was ist die Absicht hinter der Quelle?
☒ Warum wurde diese Information erstellt? Sollen sie etwas fördern? Anzeigen verkaufen? Stimmen werben? ☒ Ist der Zweck klar? Welchen Zweck verfolge ich und welche Vorurteile haben ich? Welche Vorurteile kann ich bei mir feststellen? ☒ Ist die Quelle objektiv und sachlich? ☒ Ist die Absicht klar ersichtlich? Bemerkung: