Digitale Forensik in Unternehmen

Stefan Meier

Die zunehmende und komplexer werdende Vernetzung und die stetige Digitalisierung in Unternehmen werfen oft auch neue Risiken für Angriffe auf die Informationssysteme der Unternehmen auf. Gerade durch das Aufbrechen von Unternehmensnetzen und der immer komplexer werdenden gegenseitigen Integration von Unternehmen, Behörden und Privatpersonen entstehen neue Angriffsvektoren und Risiken. Durch die Digitalisierung wächst zudem die Menge der digitalen Daten, die unter Umständen auch als digitale Spuren zur Aufklärung von Verbrechen verwertet werden müssen, da der Prozentsatz der ausgedruckten oder anderweitig analog vorhandenen Spuren im Vergleich zu den digitalen Spuren beständig schrumpft.

Die digitale Forensik als forensische Wissenschaft, die sich mit der Sicherung und Analyse von digitalen Spuren beschäftigt ist aber eine vergleichsweise junge forensische Wissenschaft. Aus diesem Grund untersucht diese Arbeit die grundlegenden Prinzipien und Definitionen der digitalen Forensik und betrachtet anschließend die speziell für digitale forensische Untersuchungen in Unternehmen vorhandenen Problemlösungsstrategien.

Auf Basis der Erkenntnisse aus der Betrachtung der vorhandenen Problemlösungsstrategien wird dann eine Methodik für unternehmensforensische Untersuchungen vorgeschlagen. Die Methodik selbst basiert auf dem ebenfalls in dieser Arbeit entwickelten digitalen Spurenverständnis im Kontext der Informations- und Anwendungssysteme von Unternehmen sowie der Definition der Unternehmensforensik, als Teildisziplin der digitalen Forensik.

0012455 27X

Cover-Design/Illustration: Stefanie Prison
Foto: © agsandrew / Fotolia

Digitale Forensik in Unternehmen

Dissertation zur Erlangung des Grades eines
Doktors der Wirtschaftswissenschaft

eingereicht an der Fakultät für Wirtschaftswissenschaften
der Universität Regensburg

vorgelegt von:
Stefan Meier

Berichterstatter:

Prof. Dr. Günther Pernul

Prof. Dr.-Ing. Felix Freiling

Tag der Disputation:

2. Dezember 2016

Stefan Meier, Ortsstraße 33, 92364 Leutenbach, Germany
Internet: http://www.stefanm.com, E-Mail: sm@stefanm.com

Geleitwort

Die digitale Forensik beschäftigt sich mit der Sichtung und Analyse digitaler Spuren in IT-Systemen, mit dem Ziel, im Falle von Computerkriminalität Tatbestände und etwaige Täter festzustellen und digitale Beweismittel und Analyseschritte gerichtsfest aufzubereiten, d. h. in einer Art und Weise darzustellen, sodass diese den strengen Anforderungen von Gerichten an Beweismittel genügen. Die forensische Informatik ist der wissenschaftliche Teilbereich der digitalen Forensik und widmet sich der Erforschung der wissenschaftlichen informatischen Grundlagen und Methoden.

Obwohl die digitale Forensik versucht, ihre Standards und Methoden in der Praxis zu etablieren, scheinen Unternehmen bisher noch kaum zu profitieren. Dies scheint dem Umstand geschuldet, dass die digitale Forensik bisher zu stark technikgetrieben ist, innerhalb der Abstraktionsebenen eines IT-Systems vornehmlich auf die tieferen Ebenen fokussiert und das Wissen über die Organisation und das Funktionieren der Unternehmen und ihrer zentralen Prozesse und Systeme bisher vernachlässigt hat. Eine wissenschaftlich fundierte Methodik, die sowohl die Prozesse im Unternehmen als auch ihre Verbindung mit den zentralen IT-Systemen und den durch sie generierten Daten und Zuständen berücksichtigt, ist bislang in der digitalen Forensik nicht bekannt.

Vor diesem Hintergrund ist es das Ziel der vorliegenden Arbeit, Problemlösungsstrategien für digitale unternehmensforensische Untersuchungen, insb. im Kontext der in Unternehmen etablierten Prozesse und eingesetzten Informations- und Anwendungssysteme zu entwickeln. Um auf diese Schwerpunktsetzung zu verweisen und die Arbeit auch von bestehenden Problemlösungsstrategien der digitalen Forensik (z. B. forensic readyness) abzugrenzen, prägt der Autor die neue Begrifflichkeit einer digitalen Unternehmensforensik bzw. die kurze Form Unternehmensforensik. Die Arbeit setzt die folgenden Schwerpunkte:

- Entwicklung eines Verständnisses über die Maßnahmen, die ein Unternehmen zur Vorbereitung auf digitale forensische Untersuchungen implementieren sollte und

Validation, inwieweit solche Maßnahmen heute in Unternehmen bereits umgesetzt sind.

- Dokumentation und Analyse der wissenschaftlichen Grundsätze, Methoden und Prinzipien der digitalen Forensik, insb. unter besonderer Berücksichtigung der Belange der höheren Abstraktionsebenen der informationstechnischen Systeme.
- Entwicklung, prototypische Umsetzung und Bewertung einer eigenen Methodik für digitale unternehmensforensische Untersuchungen.

Mit der vorliegenden Arbeit hat es der Autor verstanden, eine Vielzahl von Grundlagen, Einflussfaktoren und Entwicklungen solide aufzuarbeiten und im Zusammenhang zu bewerten. Dabei ist es ihm gelungen, einen eigenen Ansatz zu entwickeln, der sowohl hohes Potential zur praktischen Anwendung beinhaltet, als auch auf einer theoretisch fundierten Basis aufbaut. Die Arbeit zeichnet sich einerseits durch ein hohes wissenschaftliches Niveau, andererseits aber auch durch die Fähigkeit des Verfassers aus, pragmatische Lösungen zu finden und umzusetzen. Aufgrund der gut strukturierten Darstellung der Ergebnisse hat die Arbeit die Chance, zu einem praktisch verwertbaren Beitrag auf dem Gebiet der digitalen Forensik zu werden. Das Buch sei allen Entscheidungsträgern empfohlen, die ihre Interessen im Bereich des Managements der Informationssicherheit bzw. der digitalen Forensik im Unternehmen haben.

Prof. Dr. Günther Pernul
Regensburg, im Januar 2017

Vorwort

Die zunehmende und komplexer werdende Vernetzung und die stetige Digitalisierung in Unternehmen werfen oft auch neue Risiken für Angriffe auf die Informationssysteme der Unternehmen auf. Gerade durch das Aufbrechen von Unternehmensnetzen und der immer komplexer werdenden gegenseitigen Integration von Unternehmen, Behörden und Privatpersonen entstehen neue Angriffsvektoren und Risiken. Durch die Digitalisierung wächst zudem die Menge der digitalen Daten, die unter Umständen auch als digitale Spuren zur Aufklärung von Verbrechen verwertet werden müssen, da der Prozentsatz der ausgedruckten oder anderweitig analog vorhandenen Spuren im Vergleich zu den digitalen Spuren beständig schrumpft.

Die digitale Forensik als forensische Wissenschaft, die sich mit der Sicherung und Analyse von digitalen Spuren beschäftigt ist aber eine vergleichsweise junge forensische Wissenschaft. Aus diesem Grund untersucht diese Arbeit die grundlegenden Prinzipien und Definitionen der digitalen Forensik und betrachtet anschließend die speziell für digitale forensische Untersuchungen in Unternehmen vorhandenen Problemlösungsstrategien. Auf Basis der Erkenntnisse aus der Betrachtung der vorhandenen Problemlösungsstrategien wird dann eine Methodik für unternehmensforensische Untersuchungen vorgeschlagen. Die Methodik selbst basiert auf dem ebenfalls in dieser Arbeit entwickelten digitalen Spurenverständnis im Kontext der Informations- und Anwendungssysteme von Unternehmen sowie der Definition der Unternehmensforensik, als Teildisziplin der digitalen Forensik.

Durch die anschließende Evaluation der Methodik anhand einer Fallstudie sowie in der Praxis wird sowohl ihr Nutzen als auch die Praxistauglichkeit bestätigt. Es zeigen sich aber auch weiterer Forschungsbedarf und neue Problemstellungen für die Unternehmensforensik, die durch zukünftige Arbeiten adressiert werden müssen. Insgesamt kann die Methodik aber den zukünftigen Nutzen und das Potential der Unternehmensforensik aufzeigen.

Die Erstellung der Dissertation und das Ergebnis wären ohne die Hilfe vieler Unterstützer nicht möglich gewesen. Aus diesem Grund möchte ich mich an dieser Stelle bei allen bedanken, die mich beim Erstellen der Dissertation unterstützt haben. Ein besonderer Dank gilt meinem Doktorvater Günther Pernul für die Betreuung der Dissertation. Der Dank gilt dabei besonders für die inhaltliche Betreuung in Form der vielen Diskussionen und Gespräche, die immer neuen Denkanstöße und die konstruktive Kritik. Zudem möchte ich mich bei ihm auch für die Schaffung des entsprechenden und stets guten Arbeitsumfeldes an seinem Lehrstuhl bedanken.

Ein großer Dank gilt auch meinem Zweitgutachter Felix Freiling von der FAU Erlangen-Nürnberg, der nicht nur der Betreuung und Begutachtung der Dissertation zugestimmt hat, sondern auch mit wertvollem Feedback und neuen Denkanstößen zum Fortschritt und zur Qualität der Arbeit beigetragen hat.

Auch meiner Familie gilt es einen großen Dank auszusprechen. Besonders bedanken möchte ich mich bei meiner Ehefrau Johanna und meiner Tochter Emma, die mir den Rücken freigehalten und mir immer wieder neue Motivation gaben. Weiter danke ich meinen Eltern Marga und Manfred, die meinen Lebensweg immer mit all ihren Möglichkeiten unterstützt haben. Ein besonderer Dank gilt zudem meiner Mutter Marga und meiner Schwester Maria, die diese Arbeit gelesen und mir Verbesserungen und Korrekturen vorgeschlagen haben.

Bedanken möchte ich mich auch bei allen Studenten, die im Rahmen dieses Forschungsvorhabens ihre eigenen Seminar-, Bachelor- und Masterarbeiten geschrieben und mir den ein oder anderen Denkanstoß gegeben haben. Besonders bedanke ich mich bei Karolin Härtl, Miriam Däs, Georg Lindner und Wolfgang Ostermeier, die mich bei den Studien zur digitalen Forensik in Unternehmen tatkräftig unterstützt haben.

Auch bei den Mitarbeitern von Felix Freiling möchte ich mich bedanken. Ein besonderer Dank gilt Andreas Dewald und Sven Kälber für die konstruktive Kritik und die Denkanstöße.

Zu guter Letzt möchte ich mich bei meinen Kollegen am Lehrstuhl Wirtschaftsinformatik I der Universität Regensburg bedanken. Der Dank gilt besonders für die vielen konstruktiven Diskussionen und zum anderen natürlich für den sozialen Zusammenhalt und das gute Arbeitsklima.

Stefan Meier
Leutenbach, im Juni 2016

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AWS Anwendungssysteme . . . 37
BPMN Business Process Modeling Notation . . . 43
DFA Differential Forensic Analysis . . . 33
DFR Digital Forensic Readiness . . . 3
EA Enterprise Architecture . . . 42
EAI Enterprise Application Integration . . . 42
EAM Enterprise Architecture Management . . . 42
GoBD Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff . . . 131
GRR GRR Rapid Response . . . 55
IS Informationssysteme . . . 37

KAPITEL 1

Einleitung

In diesem Kapitel wird zunächst das Thema der vorliegenden Arbeit motiviert und dessen Relevanz aufgezeigt. Anschließend werden die zentralen Forschungsfragen sowie die zur Bearbeitung der Fragen ausgewählte Methodik in den Abschnitten 1.2 und 1.3 vorgestellt. Im letzten Abschnitt 1.4 des Kapitels wird der Aufbau dieser Arbeit im Detail erläutert.

1.1 Motivation und Zielsetzung

Die zunehmende und fortschreitende Automatisierung und Digitalisierung in allen Bereichen des Lebens führt zu immer komplexer vernetzten digitalen Infrastrukturen und Anwendungssystemen [MS12],[Bun14a, S. 7]. Unternehmen vernetzen sich untereinander, mit Behörden sowie mit privaten Personen [FS13, S. 3]. Neben vielen Vorteilen birgt diese Vernetzung aber auch oft neue Risiken für die Unternehmen. Die Risiken kommen vor allem von der immer größer werdenden Abhängigkeit der Unternehmen von diesen Systemen sowie dem Aufbrechen der klassischen Trennung von internem Unternehmensnetzwerk und dem Internet [Pal01, MS12]. IT-Sicherheitsvorfälle, bei denen oft Daten jeglicher Art entwendet oder gar Produktionsanlagen physisch beschädigt werden [Bun14a, S. 31], zählen dabei zu den öffentlichkeitswirksamsten Fällen. Die spektakulären und durch Presseorgane veröffentlichten Angriffe stellen aber nur einen Bruchteil der tatsächlich stattfindenden Attacken dar. In vielen Statistiken wird von einer hohen Dunkelziffer für IT-Sicherheitsvorfälle ausgegangen [Ges11, S. 25],[Bun14a, S. 26]. Die Dunkelziffer bezieht sich dabei zum einen auf die nicht gemeldeten Fälle, auf Fälle, die überhaupt nicht als solche erkannt wurden sowie auf Fälle, die aufgrund eines drohenden oder erwarteten Reputationsverlustes nicht gemeldet wurden.

Neben den von externen Angreifern verursachten IT-Sicherheitsvorfällen, gibt es auch eine zunehmende Zahl von Innentätern [GFWS15]. Weiter sind die Vorfälle in Unternehmen nicht mehr nur auf die klassischen IT-Sicherheitsvorfälle, wie z.B. Datendiebstahl oder Malware, beschränkt. Auch Fälle aus dem Gebiet der Wirtschaftskriminalität, z.B. im Bereich der Manipulation von Konto- und Finanzdaten sowie von Buchhaltungs- oder Zahlungssystemen, nehmen zu [GFWS15]. Unter anderem im Bereich der Manipulation von Zahlungssystemen sind auch einzelne Fälle mit globalem Ausmaß bekannt [FQ16]. Hierbei war nicht nur eine isolierte Organisation betroffen, sondern eine Reihe global verteilter und über das Zahlungssystem verbundene Unternehmen und Organisationen [Fin16].

Die skizzierten Fälle und Risiken machen deutlich, dass der hohe Automatismus, die stetig fortschreitende Digitalisierung und das Verbinden und Integrieren von Informationssystemen unterschiedlichster Organisationen digitale Spuren aus den IT-Systemen der Unternehmen zu einer wichtigen Quelle für Spuren und Indizien zur umfassenden Aufklärung von Delikten machen [Car09],[Cas11, S. 3]. Bereits heute werden mehr als 90% aller geschäftlichen Dokumente und geschäftsrelevanten Informationen elektronisch erzeugt und zu einem großen Teil nie ausgedruckt [MZ11, S. 214],[Bec15, S. 319]. Zur Sicherung, Analyse und Aufbereitung von digitalen Spuren aus diesen Datenbeständen für die Verwendung vor Gericht ist daher analog zu anderen forensischen Wissenschaften die digitale Forensik entstanden [DF11, S. 1f]. Die Methoden und Tools, die für digitale forensische Untersuchungen eingesetzt werden, basieren aber oft noch nicht auf wissenschaftlich anerkannten Methoden [Pal01, Bee09]. Die forensische Informatik als wissenschaftlicher Teilbereich der digitalen Forensik beschäftigt sich daher nun mit der Entwicklung von wissenschaftlichen Methoden und dem Aufbau der digitalen Forensik als Wissenschaftsdisziplin [DF11, S. 2].

Obwohl in der digitalen Forensik über die letzten Jahre versucht wurde Standards und wissenschaftliche Methoden zu etablieren [Cas09], scheinen Unternehmen aber noch kaum von den Methoden der digitalen Forensik zu profitieren. Eine Befragung hat ergeben, dass die vorhandenen Methoden von den Organisationen entweder nicht eingesetzt oder als unzureichend betrachtet werden [MP14]. Weiter zeigt die Studie [MP14], dass viele Unternehmen keine ausreichenden Ressourcen haben, um Methoden der digitalen Forensik präventiv in die IT-Prozesse zu integrieren oder dann im Falle eines Schadensereignisses zu verwenden. Dabei könnten insbesondere Unternehmen von einer guten Aufklärungsquote profitieren [BSJ10], da zum einen die Schäden über eine Abwälzung auf die Täter kompensiert werden könnten und zum anderen auch die Hemmschwelle für einen Angriff durch eine erhöhte Aufklärungsquote auf der Täterseite steigen würde [ABB+12].

Zur Aufklärung von Fällen besonders aus dem Bereich der Wirtschaftskriminalität, wie sie in Form der Manipulation von Konto- und Finanzdaten oben bereits genannt wurden, oder auch bei allgemeinen Fällen, bei denen die Kontrolle interner Richtlinien wie das Vier-Augen-Prinzip oder die Funktionstrennung (Separation of Duties) nach-

gewiesen werden müssen, ist die Einbindung von Wissen über die Organisation und das Funktionieren des Unternehmens, z.B. in Form von Geschäftsprozessen essentiell [Val10, Bec15]. Eine wissenschaftlich fundierte Methodik, die sowohl die Prozesse als auch ihre Verbindung mit den Informationssystemen und den darin enthaltenen Daten im Kontext der digitalen Forensik betrachtet, ist bislang allerdings in der digitalen Forensik nicht bekannt.

Motiviert durch diese Forschungslücke sowie der Tatsache, dass es zukünftig mangels Papierausdrucken immer weniger Spuren außerhalb der elektronischen Datenbestände der Unternehmen gibt, wird im Folgenden die digitale Forensik im Kontext von Unternehmen betrachtet. Das zentrale Ziel ist die digitale Spur und ihre Verwertbarkeit bei digitalen forensischen Untersuchungen in Unternehmen detailliert zu analysieren und zu beschreiben. Hierbei werden besonders die digitalen Datenbestände in den Informationssystemen der Unternehmen sowie die Rolle der Prozesse betrachtet und eine Methodik zur Ver- und Bewertung von digitalen Spuren aus diesen Systemen, unter Einbindung der Prozesse, vorgestellt.

Die im vorigen Absatz skizzierten Ziele werden im folgenden Abschnitt 1.2 nochmals konkreter in Form von Forschungsfragen gefasst. Im Abschnitt 1.3 werden dann das Vorgehen und die verwendete Methodik zur Lösung der Forschungsfragen in dieser Arbeit vorgestellt. Eine inhaltliche Übersicht und der Aufbau der Arbeit finden sich abschließend in Abschnitt 1.4.

1.2 Forschungsfragen

Zur Lösung der im vorherigen Abschnitt 1.1 dargestellten Probleme werden die folgenden Forschungsfragen aufgeworfen:

1. Was sind die wesentlichen organisatorischen, personellen und technischen Maßnahmen welche in einem Unternehmen zur Vorbereitung auf digitale forensische Untersuchungen implementiert werden sollten und wie etabliert sind diese Maßnahmen in der Praxis?

   Das Themenfeld Digital Forensic Readiness (DFR) beschäftigt sich seit einigen Jahren mit der Vorbereitung auf digitale forensische Untersuchungen. Diese Forschungsfrage hat zum Ziel, die in der Literatur vorgestellten Maßnahmen zu beleuchten und zusammenzufassen. Weiter wird auch die praktische Umsetzung der Maßnahmen in Unternehmen näher untersucht.

2. Wie funktionieren digitale forensische Untersuchungen? Welche grundlegenden Methoden und Prinzipien gibt es in der digitalen Forensik?

   Diese Forschungsfrage geht den wissenschaftlichen Grundsätzen, Methoden und Prinzipien in der digitalen Forensik nach. Durch die Antworten auf diese Forschungsfrage werden Anforderungen an Methoden der digitalen Forensik sowie deren grundlegende Arbeitsweise identifiziert.

3. Was ist eine digitale Spur aus Sicht der Informationssysteme von Unternehmen?

   Im Rahmen dieser Forschungsfrage wird untersucht, welche Spuren von den IT-Systemen der Unternehmen erstellt werden. Dabei werden der Prozess der Spurenentstehung beleuchtet und die Grundlagen für eine wissenschaftlich fundierte digitale forensische Rekonstruktion geschaffen.

4. Wie kann man die grundlegenden digitalen forensischen Prinzipien im Kontext der Informationssysteme von Unternehmen anwenden?

   Die in den vorherigen Forschungsfragen erarbeiteten theoretischen Grundlagen werden im Rahmen dieser Forschungsfrage genutzt, um eine Methodik zur forensischen Assoziation und Rekonstruktion im Kontext der IT-Systeme von Unternehmen zu entwickeln. Im Zuge der Beantwortung dieser Forschungsfrage werden sowohl die Funktionsweise der Methodik als auch deren Grenzen betrachtet.

1.3 Forschungsmethodik

Die Forschungsmethodik stellt eine Sammlung von Aktivitäten dar, die zur Erzeugung von neuem Wissen von einer Forschungsgemeinschaft anerkannt ist [VK07]. In der Wirtschaftsinformatik dominieren die beiden Methodenparadigmen verhaltensorientierte Forschung und gestaltungs- bzw. konstruktionsorientierte Forschung [HMPR04, WH07]. Die gestaltungorientierte Forschung, auch Design Science Research genannt [ÖBF+10], strebt nach einer Vergrößerung der Wissensbasis durch die Gestaltung neuer, innovativer und in der Praxis nützlicher Artefakte in Form von Konstrukten, Modellen, Methoden oder Instanzen [HMPR04, VK07, ÖBF+10]. Bei verhaltensorientierten Forschungsvorhaben werden dagegen aus der Beobachtung des Verhaltens von Benutzern oder der Eigenschaften von Informationssystemen neue Erkenntnisse abgeleitet [ÖBF+10].

Das zentrale Ziel dieser Arbeit ist, wie im vorherigen Abschnitt 1.2 in Form der Forschungsfragen dargestellt, eine Methodik für digitale forensische Untersuchungen im Kontext der IT-Systeme von Unternehmen zu entwickeln. Dementsprechend orientiert sich diese Arbeit am Design Research Paradigma. Das zentrale Artefakt im Sinne des Design Science Research Paradigmas stellt die Methodik für die digitalen forensischen Untersuchungen in Unternehmen dar. Das Forschungsvorhaben, dessen Ergebnisse im Folgenden vorgestellt werden, folgt dem in [VK07] auf Basis von [TVTY90] vorgestellten Erkenntnisprozess. Abbildung 1.1 zeigt diesen Prozess sowie die in jedem Schritt erwarteten Ergebnisse. Weiter zeigt das Vorgehensmodell in Abbildung 1.1 auch, dass der Prozess mehrere Iterationen durchlaufen kann. Dadurch wird ein Artefakt über mehrere Iterationen des Erkenntnisprozesses stetig verbessert [VK07, ÖBF+10].

Im Folgenden werden die einzelnen Phasen des Prozesses kurz beschrieben und den jeweiligen Kapiteln dieser Arbeit zugeordnet.

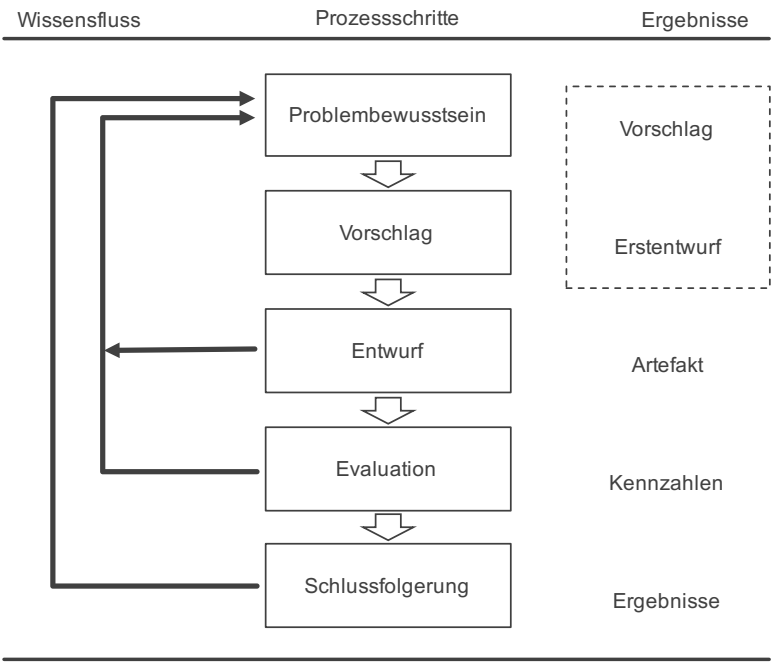


Abbildung 1.1 – Design Science Research Prozess (nach [VK07])

Problembewusstsein
Die Entwicklung eines Problembewusstseins ist der erste Schritt des Erkenntnisprozesses nach [VK07]. Hierbei geht es vor allem um die Analyse der aktuellen Problemlösungsansätze in Wissenschaft und Praxis innerhalb einer abgegrenzten Umgebung [HMPR04, ÖBF+10]. Das Ziel ist die Formulierung einer Problemstellung und der Vorschlag von Forschungszielen [VK07, ÖBF+10].

In dieser Arbeit wurden die Forschungsziele in Form der Forschungsfragen im vorherigen Abschnitt 1.2 definiert. Die Analyse der bestehenden Problemlösungsansätze in der Wissenschaft wird im Kapitel 4 beschrieben. Der aktuelle Stand des Themas digitale Forensik in der Praxis wurde anhand einer Studie ermittelt. Die Ergebnisse dieser Studie werden in Kapitel 5 vorgestellt.

Vorschlag
Nachdem die Problemstellung sowie die Forschungsziele formuliert sind, geht es in der Vorschlagsphase um Ideen hinsichtlich einer möglichen Lösung der aufgeworfenen Probleme. Das Ziel der Vorschlagsphase ist die kreative Vergegenwärtigung einer Lösung und die Erstellung eines ersten Entwurfs [VK07].

Die Problemstellung sowie Vorschläge zur Lösung werden in dieser Arbeit im Abschnitt 6.1 umfassend diskutiert und vertieft.

Entwurf
Auf Basis des provisorischen ersten Entwurfs für eine Lösung der Problemstellung wird im Entwurfs- oder Entwicklungsschritt ein Artefakt anhand anerkannter Methoden hergeleitet [VK07, ÖBF+10]. Weiter wird das Artefakt gegen bekannte Lösungen abgegrenzt [ÖBF+10].

Der Entwurf und die Herleitung der Methodik für digitale forensische Untersuchungen in Unternehmen finden sich in den Kapiteln 6 und 7. Hierbei wird durch den Rückgriff auf und die Integration von etablierten Theorien der digitalen Forensik sowie der forensischen Wissenschaften im Allgemeinen eine neue Methodik für unternehmensforensische Untersuchungen entworfen.

Evaluation
Das Ziel der Evaluation ist zu überprüfen, ob das entworfene Artefakt den quantitativen und qualitativen Anforderungen, die in der ersten Phase des Prozesses im Rahmen der Formulierung der Problemstellung aufgeworfen wurden, gerecht wird [VK07, ÖBF+10]. Weiter soll die Evaluation auch die Praktikabilität und Relevanz des Artefaktes in seiner Anwendungsumgebung feststellen [HMPR04, HC10].

Die Evaluation der Methodik für digitale forensische Untersuchungen in Unternehmen sowie die Ergebnisse der Evaluation werden im Kapitel 8 vorgestellt.

Schlussfolgerung
Die Schlussfolgerungsphase ist der letzte Schritt eines Forschungsvorhabens. Typischerweise ist der Schritt das Ergebnis des sogenannten *Satisficing*, bei der das Artefakt als gut genug zur Lösung des Problems wahrgenommen wird, wenngleich noch Abweichungen von den gewünschten Eigenschaften existieren. In dieser Phase werden die Ergebnisse des Forschungsvorhabens konsolidiert, aufgeschrieben und Problemstellungen für zukünftige Forschungsvorhaben aus den Evaluationsergebnissen abgeleitet. [VK07]

In dieser Arbeit werden Problemstellungen für zukünftige Forschungsvorhaben im Kapitel 9 beschrieben. Die Zusammenfassung der Ergebnisse sowie die Schlussfolgerungen finden sich im Kapitel 10.

1.4 Aufbau der Arbeit

Der Aufbau der Arbeit folgt im Wesentlichen der im vorigen Abschnitt 1.3 vorgestellten Forschungsmethodik in Form der in Abbildung 1.1 dargestellten Prozessschritte. Abbildung 1.2 zeigt dementsprechend den Aufbau der Arbeit. Die Arbeit ist, wie in Abbildung 1.2 erkennbar, in vier Teile gegliedert. Im ersten Teil werden die Grundlagen

der digitalen Forensik sowie zentrale Begriffe definiert und beschrieben. Die verwandten Forschungsarbeiten und der Stand der Forschung zur digitalen Forensik in Unternehmen werden im zweiten Teil der Arbeit vorgestellt. Im dritten Teil erfolgt dann die Beschreibung der Methodik für unternehmensforensische Untersuchungen. Hierbei werden, wie in Abbildung 1.2 dargestellt, die digitale Forensik und die darin etablierten Problemlösungsstrategien aus den Kapiteln 2, 4 und 5 mit den Erkenntnissen aus dem Kapitel 3 zu Informationssystemen und Prozessen in Unternehmen integriert. Im viertel Teil der Arbeit werden dann die Evaluation der Methodik im Kapitel 8 sowie die zukünftigen Problemstellungen im Kapitel 9 vorgestellt. In Kapitel 10 werden die Erkenntnisse der Arbeit schließlich zusammengefasst. Im Folgenden werden die Inhalte der einzelnen Teile nochmals detailliert beschrieben.

Teil I: Grundlagen
Nach dem einleitenden Kapitel werden die Grundlagen der Themen digitale Forensik sowie Informationssysteme und Prozesse betrachtet. Im Kapitel 2 werden dazu die digitale Forensik als forensische Wissenschaft, wie sie in dieser Arbeit verstanden wird, definiert und anschließend die Entstehung und die Eigenschaften digitaler Spuren diskutiert. Weiter beantwortet dieses Kapitel die Forschungsfrage 2.

Im anschließenden Kapitel 3 wird das Umfeld der digitalen Forensik in Unternehmen definiert. Dazu werden zum einen Informationssysteme und ihre Bedeutung erläutert und zum anderen Prozesse und ausgewählte, in den späteren Kapiteln wichtige Aspekte des Prozessmanagements in Unternehmen, beleuchtet.

Teil II: Digitale Forensik in Unternehmen
Auf Kapitel 3 folgt ein thematischer Sprung zum aktuellen Stand der Forschung in der digitalen Forensik für Unternehmen im Kapitel 4. Wie in Abbildung 1.2 dargestellt schließt das Kapitel 4 an die Grundlagen zur digitalen Forensik aus Kapitel 2 an. In Kapitel 4 werden aber speziell die vorhandenen Problemlösungsstrategien für digitale forensische Untersuchungen in Unternehmen sowie Maßnahmen zur Vorbereitung auf digitale forensische Untersuchungen aus der Wissenschaft vorgestellt.

Im Kapitel 5 werden dann die Verwendung digitaler forensischer Methoden und Tools in der Praxis anhand der Ergebnisse aus der bereits in [MP14] veröffentlichten Studie zur digitalen Forensik in der Unternehmenspraxis beschrieben. Weiter enthält Kapitel 5 auch Ergebnisse zum aktuellen Stand der Unternehmen bezüglich der Vorbereitung auf digitale forensische Untersuchungen.

Teil II schließt den ersten Schritt des in dieser Arbeit verwendeten Erkenntnisprozesses ab. Weiter wird die Forschungsfrage 1 über die Ergebnisse aus den Kapiteln 4 und 5 beantwortet.

Teil III: Unternehmensforensik
Nach der umfassenden Darstellung des Status Quo werden in Kapitel 6 die Grundlagen

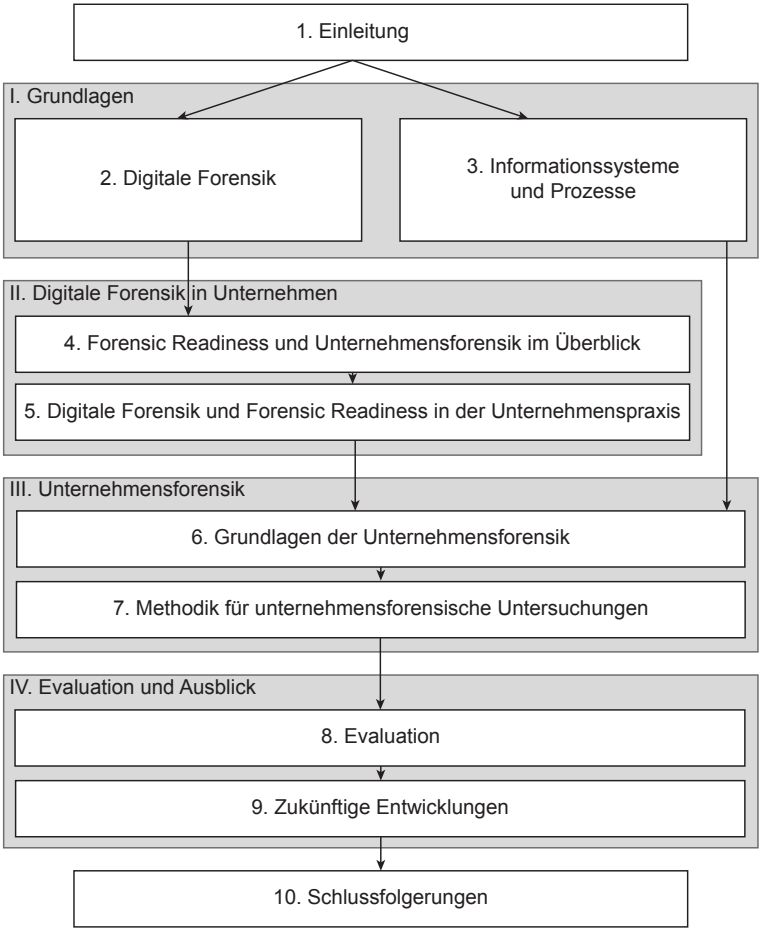


Abbildung 1.2 – Aufbau der Arbeit

der Unternehmensforensik erarbeitet und die digitalen Spuren und die, die Spuren betreffenden Informationen aus den Geschäftsprozessen in Form eines Modells abgeleitet. Hierbei werden die beiden Grundlagenkapitel, wie auch in Abbildung 1.2 dargestellt, wieder zusammengeführt und integriert.

Basierend auf den Grundlagen aus Kapitel 6 wird in Kapitel 7 dann eine Methodik zur Durchführung unternehmensforensischer Untersuchung unter Anwendung der in Kapitel 2 vorgestellten Grundprinzipien der forensischen Wissenschaften vorgestellt.

Die beiden Kapitel beantworten die zentralen Forschungsfragen 3 und 4. Forschungsfrage 3 wird in Kapitel 6 beantwortet. Für Forschungsfrage 4 wird in Kapitel 7, auf Basis der Grundlagen aus Kapitel 6 eine Lösung vorgestellt.

Teil IV: Evaluation und Ausblick

Die Ergebnisse aus der Evaluation der Methodik aus Kapitel 7 werden dann in Kapitel 8 dargestellt und bewertet. Anschließend wird in Kapitel 9 ein Ausblick auf zukünftige Verbesserungen der Methodik aus Kapitel 7 gegeben und weitere, durch die Ergebnisse dieser Arbeit identifizierte Forschungslücken diskutiert.

In Kapitel 10 werden die Ergebnisse dieser Arbeit abschließend zusammengefasst. Weiter werden die Antworten für die in Abschnitt 1.2 aufgeworfenen Forschungsfragen anhand der Ergebnisse diskutiert und dargestellt.

Teil I

Grundlagen

KAPITEL 2

Digitale Forensik

Die digitale Forensik als forensische Wissenschaft ist eine, im Vergleich zu anderen forensischen Wissenschaften, noch sehr junge Disziplin. In den letzten Jahren hat es daher eine Reihe von Veröffentlichungen gegeben, die sich mit der digitalen Forensik als wissenschaftlicher Disziplin und den grundlegenden Prinzipien und Methodiken beschäftigen [Pal01, Bee09, Coh10, DF12, Cas13a]. Die digitale Forensik wird dabei unter anderem in eine Reihe mit anderen forensischen Wissenschaften wie z.B. der Serologie, der Toxikologie oder der Ballistik gestellt [Bee09].

Eine nähere und vertiefende Betrachtung der digitalen Forensik als forensischer Wissenschaft sowie der forensischen Wissenschaften im Allgemeinen findet im nächsten Abschnitt 2.1 statt. Der Abschnitt 2.2 beschäftigt sich anschließend detailliert mit den allgemeinen forensischen Prinzipien und deren Anwendung bzw. Anwendbarkeit in der digitalen Forensik. Im Abschnitt 2.3 werden dann digitale Spuren im Allgemeinen betrachtet und es wird auf die Eigenschaften digitaler Spuren eingegangen. Digitale Spuren von konkreten Aktionen im System werden anschließend im Abschnitt 2.4 detailliert dargestellt und zudem eine Methodik zur experimentellen Erhebung einer Wissensbasis, die als Begründung für Schlussfolgerungen von digitalen Spuren auf Aktionen des Systems verwendet werden kann, vorgestellt. Schließlich werden die Erkenntnisse dieses Kapitels im Abschnitt 2.5 zusammengefasst und ein Modell zum besseren Verständnis digitaler Spuren sowie der digital forensischen Prozesse und anerkannten Vorgehensweisen vorgestellt.

2.1 Digitale Forensik und forensische Wissenschaften

Die forensischen Wissenschaften beschäftigen sich im Allgemeinen mit der Anwendung wissenschaftlicher Methoden auf Fragen des Rechtssystems [MW03],[KCGD06], [DF11, S. 5]. Dabei müssen die forensischen Wissenschaftler die Fragen des Rechtssystems in wissenschaftliche Fragen übersetzen und mit geeigneten und wissenschaftlich anerkannten Methoden beantworten [IR00, S. 15f],[Dew12, S. 17]. Als wissenschaftlich wird in diesem Zusammenhang eine wohldefinierte und wohlverstandene Wissensbasis, eine wissenschaftliche Methodik sowie eine experimentelle Basis verstanden [Pal01, Coh10]. Im Bereich der digitalen Forensik sind die Standards hinsichtlich der wissenschaftlichen Strenge und Relevanz (Rigor and Relevance) bislang allerdings niedriger als in anderen etablierten Forschungsfeldern [Pal01, Bee09, Cas09]. Dies wird unter anderem durch die, im Vergleich zu anderen forensischen Wissenschaften, wenige wissenschaftliche Literatur offenkundig [YM01, Kes12]. Weiter gibt es hinsichtlich grundsätzlicher Paradigmen und der Definition des Gebietes ebenfalls noch keinen breiten wissenschaftlichen Konsens in der digitalen Forensik [MW03, CLP11, OG13]. Slay et al. [SLT+09] schlussfolgern, dass das oberste Ziel der digitalen Forensik die Bereitstellung von legitimen und fehlerlosen digitalen Spuren für die Verwendung bei Gerichtsprozessen ist. Dazu decken sie eine Reihe von Definitionen auf und diskutieren diese [SLT+09]. Eine breiter genutzte Definition ist die Definition vom ersten Digital Forensic Research Workshop:

> „The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.“ [Pal01, S. 16]

Die Definition wird unter anderem in [Car03],[Bee09] oder [BJS11] verwendet. Die Definition ist zudem eine der ersten bekannten Definitionen der digitalen Forensik, die auch die Wissenschaftlichkeit der Disziplin mit ausdrückt. Sie deckt allerdings vor allem den praktischen Prozess der Spurensicherung, der Analyse und der Präsentation vor Gericht ab und weniger die im folgenden Abschnitt 2.2 vorgestellten Grundprinzipien forensischer Wissenschaften. In dieser Arbeit wird die digitale Forensik daher als forensische Wissenschaft nach Dewald und Freiling [Dew12, S. 59],[DF11, S. 49] verstanden:

> „Wir definieren forensische Informatik als die Anwendung wissenschaftlicher Methoden der Informatik auf Fragen des Rechtssystems. Insbesondere stellt die forensische Informatik Methoden zur gerichtsfesten Sicherung und Verwertung digitaler Spuren bereit.“ [Dew12, S. 59],[DF11, S. 49]

Die Definition drückt vor allem den wissenschaftlichen Aspekt der digitalen Forensik aus [Dew12, S. 59]. Dies wird durch den in der Definition verwendeten Begriff der forensischen Informatik verdeutlicht, der als synonymer Begriff zur digitalen Forensik eingeführt wurde, um den wissenschaftlichen Aspekt der digitalen Forensik hervor zu heben [DF11, S. 49]. Weitere synonyme Begriffe für digitale Forensik sind Computerforensik oder IT-Forensik [Cas11, S. 37],[DF11, S. 1],[Ges11, S. 2],[FHPP11, S. 1]. Neben der wissenschaftlichen Methode zur Spurensicherung wird durch die Definition auch deutlich, dass die digitale Forensik auf digitale Beweismittel bzw. Spuren beschränkt ist [BFGK09].

Durch die Nutzung wissenschaftlich akzeptierter Methoden wird eine größtmögliche Objektivität bei digitalen forensischen Untersuchungen garantiert [DF11, S. 2]. Die Erfüllung dieses Kriteriums ist enorm wichtig. Fehler bei der Durchführung digitaler forensischer Untersuchungen oder das Ziehen falscher Schlüsse aus den gefundenen digitalen Spuren können zu erheblichen Konsequenzen für die Existenz, die Freiheit oder das Leben von Menschen führen [Car09, MD10, Cas13a]. Ohne wissenschaftlich fundierte Methoden basieren die Untersuchungserkenntnisse im Zweifel auf Vermutungen oder sind im schlimmsten Fall intuitiv [Pal01]. Um die Arbeitsweise und internen Prozesse von Computern verlässlich nachzuweisen, braucht es wissenschaftliche Experimente. Dabei ist vor allem auf die Fehlerfreiheit des Experimentaufbaus, auf äußere Einflüsse, die Reproduzierbarkeit von Ergebnissen sowie die richtige Interpretation zu achten [MD10, Cas13a]. In einer steigenden Zahl von Fällen werden aber immer noch fehlerhafte Schlussfolgerungen, basierend auf falschen oder falsch interpretierten Ergebnissen wissenschaftlicher Experimente, vor Gericht präsentiert [FHPP11, S. 4],[Cas13a].

2.2 Grundprinzipien der digitalen Forensik

Die allgemeinen theoretischen Konzepte hinter der Anwendung forensischer Wissenschaften haben sich im Laufe der Jahrzehnte entwickelt [IR02]. Inman und Rudin [IR02] fassen diese Konzepte zusammen und erweitern diese in [IR00] bzw. [IR02]. Die Anwendung der Paradigmen von Inman und Rudin [IR02] auf die digitale Forensik wird dann initial von Pollitt vorgeschlagen [Pol08, DF12]. Ein umfassender Transfer der Paradigmen von Inman und Rudin erfolgt schließlich durch Dewald und Freiling [DF11, DF12, Dew12, DF14]. Sowohl Pollitt [Pol08] als auch Dewald und Freiling [DF11, DF12, Dew12, DF14] bauen dabei explizit auf den Grundlagen von Inman und Rudin aus [IR00] bzw. [IR02] auf.

Nach Inman und Rudin [IR02] sind die historisch entstandenen Paradigmen, die bei jeder Anwendung forensischer Wissenschaften berücksichtigt werden, Transfer (Locards Austauschprinzip), Identifikation (Einordnen von Objekten in eine Klasse), Individualisierung (Verkleinerung der Klasse auf ein Objekt), Assoziation (Herstellen einer Verbindung zwischen einer Person und dem Tatort) und Rekonstruktion (Erkenntnis über eine Sequenz von vergangenen Ereignissen). Inman und Rudin [IR02]

verfeinern bzw. erweitern diese Konzepte und teilen die Paradigmen in zwei Gruppen ein. Abbildung 2.1 zeigt die Paradigmen nach Inman und Rudin [IR02]. Dabei wird zwischen der Gruppe, die die Entstehung von Spuren beschreibt und der Gruppe, die den Prozess der Anwendung forensischer Wissenschaften beschreibt unterschieden. Das Verbrechen stellen Inman und Rudin [IR02] mittels der vier überlappenden Domänen Tatort, Verdächtige, Opfer und Zeugen dar. Das Verbrechen definiert zudem die Grenze zwischen der Entstehung von Spuren und der Erkennung und anschließenden Analyse und Interpretation der Spuren [IR02].

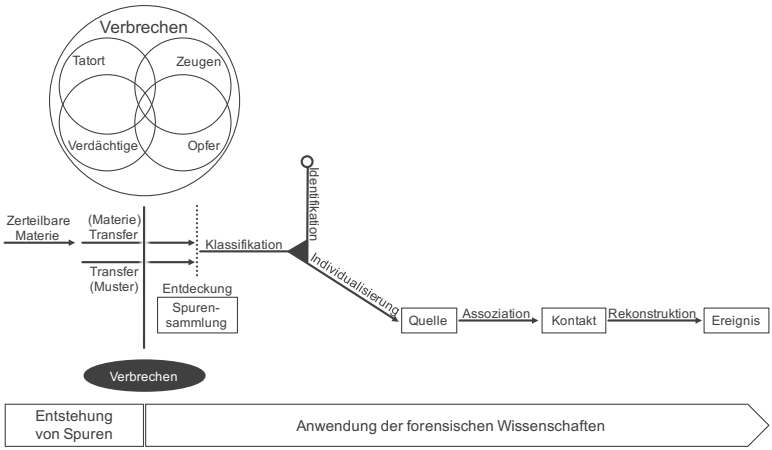


Abbildung 2.1 – Grundprinzipien der forensischen Wissenschaften: Entstehung von Spuren und forensischer Prozess (nach [IR02])

Die Entstehung von Spuren wird über die Paradigmen zerteilbare Materie und Transfer von Materie bzw. Mustern erklärt. Der Transfer von Spuren erfolgt dabei explizit im Rahmen eines Verbrechens. Spuren entstehen demnach nur in Verbindung mit einem Verbrechen, obwohl der Transfer von Materie bzw. Mustern ständig, auch ohne ein Verbrechen erfolgt. Der Transfer von Mustern beschreibt dabei die Entstehung einer großen Zahl von Spuren, z.B. Abdrücke oder Abformungen. Dabei betonen Inman und Rudin [IR02], dass beim Austausch von Mustern grundsätzlich kein Austausch von physischer Materie notwendig ist, sondern allein das ausgetauschte Muster von Interesse ist. [IR02]

Beginnend mit der Erkennung eines Elementes als Spur startet die Anwendung forensischer Wissenschaften. Die wesentlichen Prozesse bei der Anwendung forensischer Wissenschaften sind Identifikation, Klassifikation oder Individualisierung, Assoziation und Rekonstruktion. Mithilfe dieser Prozesse versucht man die folgenden Fragen der Untersuchung zu lösen: *wer*, *was*, *wo*, *warum*, *wann* und *wie*. [IR02]

Im Detail sind die einzelnen Prozessschritte wie folgt definiert:

Identifikation Der Prozess der Identifikation bezeichnet die Wahrnehmung einer Spur als solche und die Einordnung der Spur in eine Klasse. Der Prozess beantwortet die Frage: *Was ist es?* [IR02] Weiter wird im Rahmen der Identifikation die Tauglichkeit einer Spur als Beweismittel geprüft [Dew12, S. 50].

Individualisierung Nach der Identifizierung eines Elementes werden, über den Zwischenschritt der Klassifizierung, die Alleinstellungsmerkmale eines Elements mit mindestens einem anderen Element verglichen [IR02]. Man geht in diesem Schritt davon aus, dass jedes individuelle Objekt einzigartig ist [IR02]. Der Prozess der Individualisierung geht im Detail der Frage nach, ob zwei Objekte den gleichen Ursprung besitzen [IR02]. Dabei werden die individuellen Merkmale der Elemente betrachtet und die Menge der infrage kommenden Elemente durch die Betrachtung ihrer Eigenschaften eingegrenzt, bis im Idealfall nur noch die Spur und das Referenzobjekt übrig bleiben [IR02],[Dew12, S. 31].

Assoziation Die Assoziation bezeichnet die Schlussfolgerung des Kontaktes zwischen zwei Elementen. Die Schlussfolgerung basiert dabei auf den vorangegangenen Nachweisen des Transfers von Spuren. Der Transfer kann dabei auch in beide Richtungen erkannt werden, d.h. die Spur kann sowohl Ziel als auch Quelle des Transfers sein. Im Rahmen des Prozesses der Assoziation werden dann konkurrierende Hypothesen für und gegen das Stattfinden des Kontaktes zwischen zwei Elementen untersucht. Unter Einbeziehung der Wahrscheinlichkeit wird dann entsprechend geschlussfolgert, dass es entweder einen Kontakt zwischen dem Element und dem anderen Element gab, oder dass es wahrscheinlicher ist, dass das Element in Kontakt mit einem anderen, nicht verwandten Element war. [IR02]

Rekonstruktion Der Prozess der Rekonstruktion bezeichnet die Einordnung der einzelnen Assoziation in Raum und Zeit. Der Rekonstruktionsprozess versucht die Fragen *wo*, *wie* und *wann* zu beantworten. [IR02]

Die obige Definition des Prozesses der Assoziation erwähnt bereits die Nutzung von Hypothesen, um Schlüsse aus dem Ergebnis von digitalen forensischen Untersuchungen zu ziehen. Das Testen von Hypothesen ist neben der in Abschnitt 2.1 geforderten Nutzung anerkannter Methoden der jeweiligen forensischen Wissenschaft ein weiterer Bestandteil für ein wissenschaftliches Vorgehen zur Wahrung einer größtmöglichen Objektivität bei digitalen forensischen Untersuchungen [Cas11, S. 24],[Dew12, S. 14].

Hypothesen sind generell ein wesentlicher Bestandteil einer wissenschaftlichen Vorgehensweise in klassischen Wissenschaften. Die wissenschaftliche Methodik funktioniert, vereinfacht ausgedrückt, durch das Vorschlagen einer Hypothese, z.B. in Form einer Aussage oder einer Behauptung durch einen Wissenschaftler. Anschließend werden

Experimente durchgeführt, um die Hypothese zu überprüfen. Die Ergebnisse der Experimente führen dann entweder zur Annahme oder zur Ablehnung der Hypothese. [IR00, S. 5f],[Dew12, S. 13]

Analog zu den klassischen Wissenschaften werden auch bei forensischen Untersuchungen Hypothesen aufgeworfen. Anschließend werden die Hypothesen auf ihre Gültigkeit überprüft. Solange keine Gründe gegen eine Hypothese sprechen, wird diese angenommen. Die Richtigkeit einer Assoziation kann daher nicht überprüft werden. Im Umkehrschluss heißt das, dass keine Analyse den echten Ursprung von Spuren bestimmen kann, auch wenn der wahre Ursprung gefunden und mit verglichen wird. [IR00, S. 5f],[IR02]

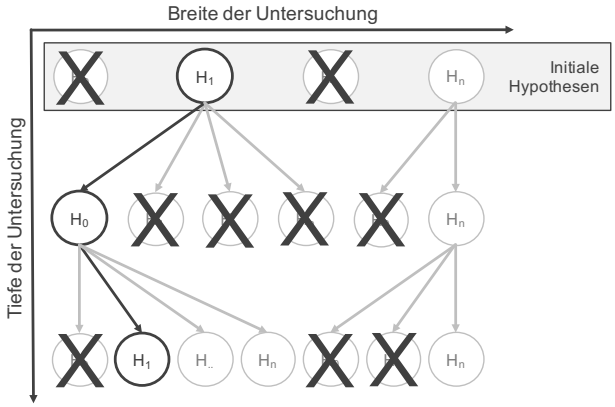


Abbildung 2.2 – Breite und Tiefe einer hypothesenbasierten forensischen Untersuchung (nach [Dew12, S. 13])

Abbildung 2.2 zeigt die Verwendung von Hypothesen bei forensischen Untersuchungen. Eine Untersuchung startet dabei mit initialen Hypothesen, die den Umständen eines Verbrechens, möglichen Tathergängen bzw. einer möglichen Erklärung für die Entstehung einer Spur entsprechen. Dies wird auch als die Breite einer Untersuchung bezeichnet. Durch die Verfeinerung der initial nicht widerlegbaren Hypothesen versucht ein Ermittler bzw. ein forensischer Gutachter die Hypothesen auf einer feineren Ebene zu stützen bzw. zu widerlegen. Die stetige Verfeinerung entspricht der Tiefe einer Untersuchung. Hypothesen, die auch mit größerem Aufwand nicht widerlegt werden können, gelten als wahrscheinlich und werden angenommen. [Dew12, S. 13f]

Kennzeichnend für das wissenschaftliche Vorgehen ist auch die Nachvollziehbarkeit bzw. die Überprüfbarkeit der Ergebnisse einer Untersuchung. Die zur Überprüfung von Hypothesen durchgeführten Experimente müssen daher durch einen Dritten wiederholt werden können [Cas11, S. 25]. Dadurch wird eine unabhängige Überprüfung der

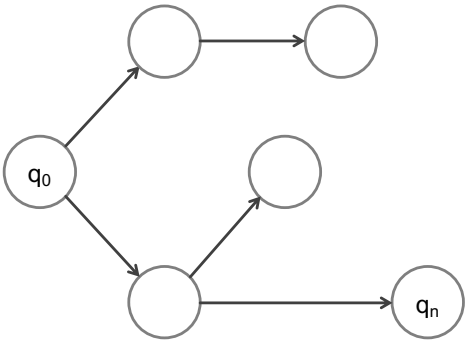
Ergebnisse bzw. die Überprüfung der gezogenen Schlüsse ermöglicht [Cas11, S. 25].

Die Grundprinzipien der forensischen Wissenschaften sowie das Testen von Hypothesen finden auch in der digitalen Forensik ihre Anwendung. Die Entstehung von digitalen Spuren ist im Vergleich zur Entstehung von Spuren in der physischen Welt auf das Paradigma des Transfers von Mustern begrenzt, weshalb die Übertragung von Mustern auch die Basis für Assoziationen darstellt [Coh10],[Dew12, S. 48f],[DEPG+14, S. 156]. Die oben genannten Prozesse Rekonstruktion von Ereignissen, Assoziation, Individualisierung und Identifikation sowie das Testen von Hypothesen lassen sich dagegen auf digitale forensische Untersuchungen ebenso anwenden [CS04, Car06, CS06, Pol08],[Dew12, S. 50ff].

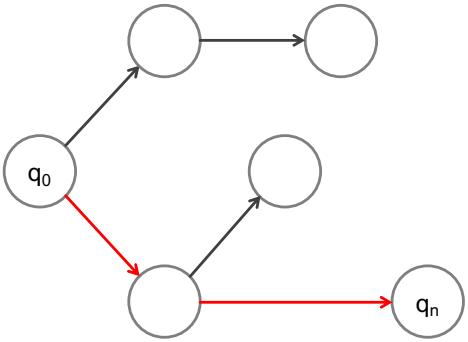
Die Rekonstruktion von Ereignissen bedeutet in der digitalen Forensik konkret die Rekonstruktion von bzw. das Schließen auf vorherige Zustände des digitalen Systems mittels der Informationen aus digitalen Spuren [CS04, Car06, Car09],[Dew12, S. 69]. Digitale Spuren werden demnach durch Ereignisse bzw. einzelne Aktionen in einem digitalen System hervorgerufen [Dew12, S. 69]. Abbildung 2.3(a) zeigt ein System in Form eines Zustandsautomaten. Die Kreise repräsentieren die Zustände des Systems und die gerichteten Kanten die Ereignisse, durch die sich der Zustand des Systems verändert. Aufgabe der digitalen Forensik ist nun den in Abbildung 2.3(b) dargestellten Pfad bzw. die Ereignisse zu rekonstruieren, durch die das System in den Zustand q_n wechseln konnte. Hierbei kann aber, wie in Abbildung 2.3(c) dargestellt, das Problem auftreten, dass es mehrere Ereignisabfolgen gibt, die alle zum selben Endzustand führen [Dew12, S. 70f].

Die Probleme bei der Rekonstruktion sowie das Rekonstruktionsproblem selbst werden unter anderem von Gladyshev und Patel [GP04], Carrier [Car06] und Dewald [Dew12] adressiert. Sowohl Gladyshev und Patel [GP04] als auch Dewald [Dew12] betrachten ein reales System dazu als endlichen Automaten. Die Rekonstruktion von Aktionen erfolgt durch eine Rückwärtssuche im Automaten. Für eine Rückwärtssuche nach allen Zuständen, die einen am Tatort vorgefundenen Zustand hervorrufen können, muss das komplette System allerdings vollständig als endlicher Automat modelliert sein [GP04],[Dew12, S. 152f]. Sowohl Gladyshev und Patel [GP04] als auch Dewald [Dew12] kommen zum „Schluss, dass die vollständige formale Modellierung realer Systeme [..] in der Praxis (noch) nicht möglich [ist]“ [Dew12, S. 153]. Dewald [Dew12] definiert deshalb nicht nur das einfache Rekonstruktionsproblem, sondern auch schwächere Problemstellungen und untersucht deren Lösbarkeit, da diese in der Praxis relevanter sind [Dew12, S. 153f].

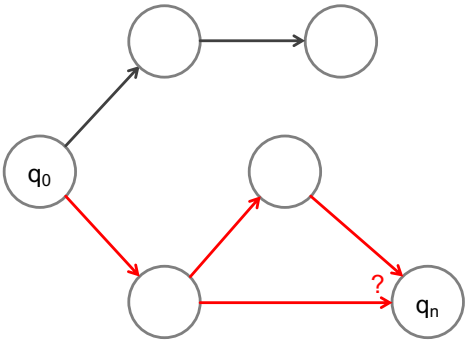
Die für die Rekonstruktion erforderliche Kenntnis des Systems (das Expertenwissen) nennen Gladyshev und Patel [GP04] explizit als Anforderung für die Rekonstruktion. Nach Gladyshev und Patel [GP04] ist das Expertenwissen dann der vollständig modellierte endliche Automat. Auch in [Dew12] ist die Kenntnis der Funktionalität des Systems als Voraussetzung für die Prüfung von Hypothesen implizit über die Kenntnis aller Zustände des endlichen Automaten gegeben. Carrier und Spafford [CS04] erwäh-



(a) Pfade in einem Zustandsautomaten



(b) Zu rekonstruierender Pfad im Zustandsautomaten



(c) Alternative Pfade im Zustandsautomaten

Abbildung 2.3 – Rekonstruktion anhand der Pfade eines Zustandsautomaten (nach [Dew12, S. 71f])

nen zusätzlich, dass die Kenntnis des Systems und der darüber abgebildeten Befehle analog zu den bekannten physikalischen Gesetzen in der physischen Welt zu sehen ist. Die individuellen Befehlssätze von z.B. Betriebssystemen oder Anwendungssoftware bilden demnach auch eine zusätzliche Quelle von Spuren, da diese individuell für jeden Computer sein können [CS04]. Die Rekonstruktion von Aktionen beantwortet nach Carrier und Spafford [CS04] bzw. Carrier [Car09] dann die Fragen wieso ein Objekt gewisse Eigenschaften aufweist, woher diese kommen könnten und wann diese erstellt wurden. Da in der Praxis aber nicht alle Aktionen des Computers aufgezeichnet werden, müssen Schlussfolgerungen auf Basis der oben bereits erläuterten Prüfung von Hypothesen gezogen werden [CS06].

Die Arbeitsweise der forensischen Prinzipien bzw. einer hypothesenbasierten digitalen forensischen Untersuchung wird im Folgenden anhand eines Beispiels verdeutlicht. Das Beispiel basiert auf dem in [DF12] veröffentlichten Beispiel des Besuchs einer Webseite B durch Computer A. Die Nullhypothese der Untersuchung ist daher: H_0: Computer A besuchte Webseite B.

Identifikation

Im ersten Schritt müssen relevante digitale Spuren identifiziert werden. Als Ausgangspunkt der Untersuchung steht die Festplatte von Computer A zur Verfügung. Durch sein Expertenwissen kann ein Ermittler die Hypothese verfeinern und auf der nächsten Ebene die Hypothese $H_{0,0}$: Computer A besuchte Webseite B mit Browser C aufwerfen. Dahinter steckt die Vermutung, dass die Webseite über die Nutzung eines bestimmten Browsers C aufgerufen wurde. Browser C kann ein beliebiger Browser sein. Typischerweise speichert ein Browser die Inhalte der besuchten Webseiten in einem Cache auf der Festplatte. Der Ermittler identifiziert also z.B. die Dateien, die den Cache von C auf der Festplatte ausmachen und klassifiziert diese Spuren als Cache des installierten Browsers C.

Individualisierung

Nachdem der Ermittler festgestellt hat, dass von Browser C ein Cache existiert, nutzt er eine Methodik zur Abstraktion der Spuren, in der Regel in Form eines Werkzeugs, um den Cache auszuwerten. Dabei sieht er sich insbesondere den Dateiinhalt sowie Eigenschaften der einzelnen Einträge im Cache wie z.B. das Erstellungsdatum oder die Größe an, um die individuellen Eigenschaften der Dateien im Vergleich zu den Inhalten von Webseite B zu identifizieren.

Assoziation

Wenn genügend individuelle Eigenschaften identifiziert wurden, z.B. HTML-Dateien, Mediendateien wie Bilder oder Videos und Spuren aus dem Dateiinhalt wie z.B. der Benutzername oder Personen auf den gefundenen Bildern, die in dieser Kombination oder gänzlich nur auf Webseite B vorkommen, kann der Ermittler auf einen Kontakt

zwischen Computer A und Webseite B schließen, die Hypothesen annehmen und dadurch die entsprechende Assoziation herstellen.

Durch dieses Beispiel wird nochmals deutlich, dass die Prinzipien forensischer Wissenschaften auch bei digitalen forensischen Untersuchungen ihre Gültigkeit besitzen. Weiter zeigt das Beispiel auch die Anwendung von Hypothesentests bei digitalen forensischen Untersuchungen. Ein Problem von digitalen Spuren ist allerdings, dass diese normalerweise lediglich Indizien sind. Eine direkte Zuordnung der Spuren zu einer Person ist daher in der Regel schwierig [Cas11, S. 26]. Auch im Fall von sehr guten digitalen Spuren, z.B. durch das Auffinden eines Benutzernamens in den auf der Festplatte von Computer A gefundenen Dateien der Webseite B aus dem obigen Beispiel wäre es schwierig, den Besuch der Webseite rein durch digitale Beweise einer Person zuzuordnen, insbesondere da Authentifizierungsmaßnahmen, wenn überhaupt welche existieren, umgangen werden können [AN95],[Cas11, S. 26].

Nachdem sich dieser Abschnitt ausführlich mit den Grundprinzipien der digitalen Forensik beschäftigt hat und Assoziationen und die Rekonstruktion von Ereignissen auf Basis von Hypothesentests als die in den forensischen Wissenschaften etablierte Vorgehensweise identifiziert wurden, wird im Folgenden konkreter auf digitale Spuren und deren Eigenschaften eingegangen.

2.3 Digitale Spuren

Digitale Spuren sind der Untersuchungsgegenstand von digitalen forensischen Untersuchungen, da digitale forensische Untersuchungen, wie in Abschnitt 2.1 bereits festgestellt auf digitale Beweismittel bzw. Spuren beschränkt sind [BFGK09]. Unter einer digitalen Spur kann man sich viele Dinge vorstellen, z.B. einzelne Bits, eine Reihe von Dateien, verschiedene Dokumente wie PDF-Dateien, Word-Dateien, E-Mails, Bilder oder auch Videos. Diese Liste könnte stetig fortgeführt und ergänzt werden. Aus diesem Grund werden digitale Spuren in dieser Arbeit allgemein nach Casey [Cas11, S. 7] definiert:

> Digitale Spuren sind alle Daten, die durch die Benutzung von Computern gespeichert oder übertragen werden und die die Theorie über einen Tathergang unterstützen oder ablehnen, oder die ein kritisches Element wie ein Motiv oder Alibi betreffen. [Cas11, S. 7]

Diese allgemeine Definition stellt digitale Spuren in den Kontext eines Verbrechens. Ohne einen Bezug zu einem Verbrechen spricht man demnach nicht von einer digitalen Spur. Dies entspricht auch der Argumentation von Inman und Rudin [IR02], die, wie im vorherigen Abschnitt 2.2 bereits ausführlich dargelegt, die Entstehung von Spuren (Transfer von Materie oder Mustern) und damit auch die Spuren selbst explizit in den Kontext eines Verbrechens stellen.

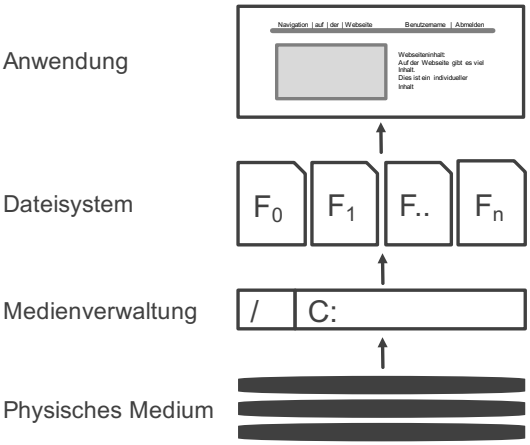


Abbildung 2.4 – Abstraktionsebenen für eine HTML-Datei (nach [Car03])

Die Definition von Casey [Cas11] umfasst alle eingangs genannten Beispiele für digitale Spuren. Es ist aber dennoch ein Unterschied hinsichtlich des betrachteten Abstraktionsniveaus zu beobachten. Digitale Spuren sind zunächst ebenfalls physische Spuren, da sie in physischer Form vorliegen, z.B. als Magnetisierung der Festplattenoberfläche oder als Lichtwellen im Glasfaserkabel [Dew12, S. 38],[DEPG+14, S. 156]. Durch die Interpretation dieser physischen Spuren erfolgt der Übergang zur digitalen Forensik [Dew12, S. 38]. Die digitalen Spuren können dann auf unterschiedlichen Abstraktionsniveaus betrachtet werden, z.B. als Menge an Bits, als Buchstaben auf dem Bildschirm, als E-Mailnachricht, usw. [Car03],[Cas11, S. 25],[Dew12, S. 38]. Die Transformation der physischen Spuren auf ein für eine Untersuchung sinnvolles Abstraktionsniveau ist allerdings nicht trivial und kann auch selbst Fehler enthalten [Pal01],[Car03]. Abbildung 2.4 zeigt exemplarisch die Abstraktionsebenen bei der Interpretation einer HTML-Datei. Carrier beschreibt in [Car03] die verschiedenen in Abbildung 2.4 dargestellten Abstraktionsschritte:
Auf der untersten Ebene befindet sich demnach die Ebene des physischen Mediums. Darin wird das individuelle Speicherformat des physischen Mediums in ein allgemeineres Format mit Sektoren, LBA und CHS Adressierung transformiert. Die darauf aufbauende Ebene Medienmanagement übersetzt die vom physischen Medium bereitgestellten transformierten Daten in Partitionen. Darauf aufbauend nutzt das Dateisystem die Partitionen und abstrahiert deren Inhalt zu einzelnen Dateien. Auf der Anwendungsebene werden die Daten schließlich in die von einer Anwendung benötigte Form transformiert. Für eine HTML-Datei passiert dies z.B. durch die Transformation der Rohdaten aus dem Dateisystem in eine ASCII und HTML-Datei.

Neben ihrer nur durch Abstraktion möglichen Interpretation haben digitale Spuren auch weitere Eigenschaften, die besonders bei ihrer Sicherung und forensischen Verarbeitung zu beachten sind. Diese Eigenschaften sowie Maßnahmen zur Sicherung der Eigenschaften digitaler Spuren werden nun in den folgenden Unterabschnitten 2.3.1-2.3.5 detailliert betrachtet.

2.3.1 Flüchtigkeit digitaler Spuren

Da die digitalen Spuren lediglich eine Interpretation physischer Spuren darstellen, sind auch die digitalen Spuren aufgrund der Speicherung in physischen Medien und der dadurch bedingten physikalischen und chemischen Prozesse einer gewissen Flüchtigkeit unterworfen. Generell lassen sich drei Arten der Flüchtigkeit unterscheiden: persistente, semi-persistente und flüchtige Spuren [Dew12, S. 39f].

Persistente Spuren sind auch ohne Stromzufuhr des Mediums auf dem sie gespeichert sind für einen großen Zeitraum erhalten [Dew12, S. 39]. Beispiele für solche digitale Spuren sind: Daten auf Festplatten, Daten auf optischen Medien wie Blu-rays, CDs oder DVDs, oder Daten auf Flash-basierten Medien wie USB-Sticks oder Solid-State-Disks [Ass07],[Dew12, S. 39].

Semi-persistente Spuren bleiben nur mit ständiger Stromzufuhr des Speichermediums dauerhaft bestehen [Dew12, S. 39]. Bei einer Unterbrechung der Stromzufuhr bleiben die Spuren, wenn überhaupt, nur eine kurze Zeit erhalten [Dew12, S. 39]. Das typische Beispiel semi-persistenter digitaler Spuren sind die Daten im Hauptspeicher (RAM) eines Rechners [Dew12, S. 39f].

Flüchtige Spuren sind Spuren die selbst im laufenden Betrieb und unter ständiger Stromzufuhr nur temporär auf den Medien erhalten bleiben [Dew12, S. 40]. Beispiele für diese Spuren sind die Daten auf einem Netzwerkkabel oder Daten in den Prozessorregistern [Dew12, S. 40].

Die Flüchtigkeit der digitalen Spuren bestimmt maßgeblich das Vorgehen bei ihrer Sicherung und Verarbeitung [BK02, Wil12],[Dew12, S. 39f]. Je nach ihrer Flüchtigkeit können die Spuren auch lange nach der Tat (persistente Spuren) noch gesichert werden oder müssen bereits im noch laufenden Betrieb nach (semi-persistente Spuren) oder gleich bei ihrer Entstehung bzw. ihrer Verarbeitung (flüchtige Spuren) gesichert und auf persistente Medien übertragen werden [Dew12, S. 39f],[Wil12]. Werden digitale Spuren nicht adäquat oder gar nicht gesichert, kann auch die Analyse durch die Flüchtigkeit digitaler Spuren beeinträchtigt werden, z.B. wenn flüchtige Spuren nicht gesichert und durch das Fehlen dieser Spuren das Assoziieren und die Rekonstruktion des Tathergangs nicht mehr lückenlos möglich sind [BK02, Wil12].

2.3.2 Manipulierbarkeit digitaler Spuren

Digitale Spuren sind, wie auch physische Spuren, manipulierbar. Nach Inman und Rudin [IR02] führt jede Handlung zu einem Transfer, d.h. auch die Manipulation ist eine Handlung, die entweder zum Transfer von Materie, Mustern oder Beidem führt. Dieser Transfer ist allerdings, anders als bei physischen Spuren, bei digitalen Spuren in den meisten Fällen sehr viel schwerer oder gar nicht als solcher zu erkennen [Pal01],[Cas11, S. 26],[Dew12, S. 41]. Ein perfektes Verbrechen ist in der digitalen Welt theoretisch möglich [BFGK09, FG15]. Allerdings ist es sehr schwer keine Spuren zu hinterlassen, da Kopien von Daten ggf. an einem, dem Täter unbekannten Ort abgelegt sein können [Cas11, S. 26]. Weiter können die Daten unter Umständen wiederhergestellt und Veränderungen durch den Vergleich der digitalen Spuren mit Kopien der Daten auf anderen Medien entdeckt werden [Cas11, S. 26]. Zudem könnten Manipulationen oder das Fehlen von digitalen Spuren durch kryptographische Sicherungsmaßnahmen erkannt werden [Cas11, S. 26]. Dennoch ist es alleine aufgrund der Möglichkeiten, digitale Spuren einfach und ohne offensichtliche Spuren zu hinterlassen manipulieren zu können wichtig, digitale Spuren insbesondere bei der Sicherung und Verarbeitung entsprechend abzusichern [Cas11, S. 26].

Gerade Fehler bei der Sicherung können dazu führen, dass digitale Spuren entwertet werden [Wil12]. Dies ist insbesondere bei semi-persistenten und flüchtigen Spuren der Fall, da diese im laufenden Betrieb und unter Hinnahme der Veränderung des laufenden Systems gesichert werden müssen [Wil12].

2.3.3 Sicherung der Authentizität

Die Sicherung der Authentizität von digitalen Spuren muss kontinuierlich ab dem Zeitpunkt der Sicherung der Spuren durchgeführt werden. Initial muss dazu festgestellt werden, ob die Spuren tatsächlich von einem bestimmten Rechner kommen [Cas11, S. 21]. Dazu untersucht man den Rechner auf entsprechende Hinweise. Bei der Untersuchung des Webseitenbeispiels aus dem vorherigen Abschnitt 2.2 müsste man z.B. prüfen, ob die gefundenen Dateien des Browsercaches auch zum installierten Browser passen oder ob der installierte Browser gar keine solchen Cachedateien erzeugt. Daneben muss auch die Beweiskraft der digitalen Spuren ermittelt werden [Cas11, S. 21].

Zur Wahrung der Authentizität im Verlauf der weiteren Verarbeitung der digitalen Spuren ist es zudem notwendig, die Beweismittelkette zu pflegen und aufrecht zu erhalten [Cas11, S. 21f]. Jede Person, die mit den Spuren in Kontakt kommt, muss entsprechend nachweisen können, dass die Spuren nicht verändert oder ausgetauscht wurden und dass tatsächlich die in Frage stehenden digitalen Spuren genutzt wurden [Cas11, S. 21f]. Andernfalls könnte man vor Gericht argumentieren, dass die Spuren falsch gehandhabt, ausgetauscht oder verändert wurden, was im schlimmsten Fall dazu führt, dass die digitalen Spuren entwertet werden und nutzlos sind [Cas11, S. 21f].

Tabelle 2.1 – Kategorien der Sicherheit digitaler Spuren (nach [Cas11, S. 70],[DF11, S. 41])

Kategorie	Beschreibung/Indikatoren	Einstufung
C0	Die Spuren widersprechen bekannten Fakten.	inkorrekt
C1	Die Spuren sind mehr als fraglich.	sehr unwahrscheinlich
C2	Es gibt nur eine Spurenquelle und diese ist nicht gegen Manipulationen geschützt.	unwahrscheinlich
C3	Die Spurenquelle(n) ist schwieriger zu Manipulieren, aber es existieren zu wenig Spuren um eine Schlussfolgerung zu unterstützen oder es finden sich ungeklärte Inkonsistenzen in den verfügbaren Spuren.	möglich
C4	(a) Die Spuren sind gegen Manipulationen geschützt oder (b) die Spuren sind nicht gegen Manipulationen geschützt, aber es existieren mehrere unabhängige Spurenquellen mit übereinstimmenden digitalen Spuren.	wahrscheinlich
C5	Übereinstimmung von Spuren aus mehreren unabhängigen und gegen Manipulationen geschützten Spurenquellen. Kleine Unstimmigkeiten sind vorhanden, z.B. temporäre Fehler und Datenverluste.	sehr wahrscheinlich
C6	Die Spuren sind manipulationssicher oder haben eine hohe statistische Signifikanz.	sicher

2.3.4 Sicherung der Integrität

Die Sicherung der Integrität digitaler Spuren ist entscheidend für die spätere Verwertung digitaler Spuren. Die wichtigste Aufgabe der Sicherung der Integrität ist der Nachweis, dass Spuren nicht verändert oder anderweitig manipuliert wurden [Pal01],[Cas11, S. 22]. Dazu wird in der Regel bei der Sicherung von digitalen Spuren ein Fingerabdruck in Form eines Hash-Wertes der gesicherten Spuren generiert und dieser Hash-Wert selbst gegen Manipulationen geschützt, z.B. durch ein digitales Signaturverfahren [Pal01],[Cas11, S. 22]. Später kann dann jederzeit ein Hash-Wert der digitalen Spuren generiert und mit dem Hash-Wert, der bei der Sicherung der Spuren generiert wurde, verglichen werden [Cas11, S. 22].

2.3.5 Kategorien der Sicherheit digitaler Spuren

Da es für die Fehler- bzw. Irrtumswahrscheinlichkeit bei der Transformation digitaler Spuren sowie allgemein für die Aussagekraft digitaler Daten noch zu wenig Forschung und allgemein verfügbare und geprüfte Erfahrungswerte gibt [Pal01], schlägt Casey [Cas11] sieben qualitative Kategorien der Sicherheit digitaler Spuren vor. Die Kategorien können insbesondere dazu verwendet werden, die Aussagekraft der digitalen Spuren und damit die Wahrscheinlichkeit der einzelnen aufgeworfenen Hypothesen zu ermitteln. Insbesondere soll damit die Wahrscheinlichkeit, dass kein Kontakt im Sinne eines

Transfers von Mustern stattfand, obwohl dieser festgestellt wurde, ausgedrückt werden [Dew12, S. 57]. Die sieben qualitativen Kategorien nach Casey [Cas11] sind in der Tabelle 2.1 aufgelistet. Für die Praxis sind insbesondere die Stufen C0 sowie C4 bis C6 relevant [Dew12, S. 59].

2.4 Digitale Spuren von Aktionen im System

Nachdem die Definition digitaler Spuren sowie ihre allgemeinen Eigenschaften betrachtet wurden, werden nun speziell Aktionen im System sowie die bei der Ausführung von Aktionen entstehenden Spuren als zentraler Untersuchungs- bzw. Rekonstruktionsgegenstand digitaler forensischer Untersuchungen detailliert betrachtet. Dieser Abschnitt baut dazu im Wesentlichen auf den Erkenntnissen zur Rekonstruktion von Aktionen in digitalen Systemen von Dewald [Dew12, Dew15] auf, da Dewald [Dew12], anders als Gladyshev und Patel [GP04], neben dem allgemeinen Rekonstruktionsproblem auch zwei schwächere und für die Praxis relevantere Formen des Rekonstruktionsproblems definiert und untersucht [Dew12, S. 153]. Sowohl Dewald [Dew12] als auch Gladyshev und Patel [GP04] nutzen einen endlichen Automaten, um ein digitales System in Form eines Modells zu beschreiben. Dewald [Dew12] benutzt im speziellen Dijkstras Guarded Commands [Dij75], da der Formalismus bekannt und gut untersucht ist und damit auch Nebenläufigkeit modelliert werden kann, wodurch sich die Notation sehr gut für die Modellierung realer Computersysteme eignet [Dew12, S. 72].

Im Folgenden werden nun die für diese Arbeit in den folgenden Kapiteln wichtigen Erkenntnisse aus [Dew12] bzw. [Dew15] vorgestellt. Im nächsten Abschnitt wird dazu kurz das Modell des Systems beschrieben, das den Überlegungen von Dewald [Dew12] zugrunde liegt und in den anschließenden Abschnitten auf die verschiedenen Arten von digitalen Spuren von Aktionen sowie auf die Möglichkeiten zu deren Rekonstruktion nach [Dew12] bzw. [Dew15] eingegangen.

2.4.1 Systemmodell

Abbildung 2.5 zeigt ein einfaches Modell eines digitalen Systems S. Das System besteht demnach aus Zuständen, Zustandsübergängen, Variablen, dem Wertebereich der Variablen, Aktionen, Programmen, Pfaden und den Zuordnungen bzw. Beziehungen zwischen den einzelnen Systemkomponenten. Im Folgenden werden nun die einzelnen Systembestandteile genauer erläutert.

Der Zustand eines Systems wird in Form einer Menge an Variablen (V) ausgedrückt. Variablen können Dateisystemobjekte, Festplattenblöcke, Hauptspeicherregionen oder auch Attribute dieser Objekte wie z.B. den Zeitstempel der letzten Änderung einer Datei repräsentieren. Die Art der Werte, die eine Variable speichern kann, wird für jede Variable über eine Domäne (D) festgelegt. In realen Computersystemen ist die Domäne aller Variablen z.B. $D = \{0,1\}$. [Dew12, S. 73]

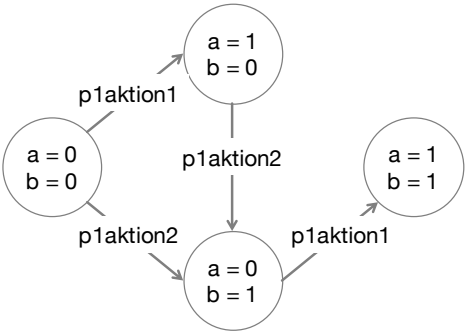


Abbildung 2.5 – Zustandsübergänge eines Programms (nach [Dew12, S. 93])

Ein konkreter Zustand q entspricht der Belegung aller $v \in V$ mit konkreten Werten. Zustände werden als Mengen von Variablen-Wert-Paaren ausgedrückt. Q bezeichnet die Menge aller hinsichtlich V möglichen Zustände. Die initiale Belegung der Variablen wird Initialzustand q_0 mit $q_0 \in Q$ und die initiale Belegung einer einzelnen Variable $v \in V$ Initialwert genannt. Für das Beispiel in Abbildung 2.5 ist $Q = \{\{a = 0, b = 0\}, \{a = 0, b = 1\}, \{a = 1, b = 0\}, \{a = 1, b = 1\}\}$. [Dew12, S. 73]

Um den Wert von Variablen zu ändern, laufen im System Aktivitäten bzw. Programme ab. Programme wiederum bestehen aus einer Menge von Aktionen Σ. Wenn eine einzelne Aktion σ einer Variable einen Wert zuweist, so wird dies über $[v = d] \in \sigma$ ausgedrückt. Die Menge aller Variablen, denen σ einen Wert zuweist, wird mit $vars(\sigma)$ bezeichnet. [Dew12, S. 73f]

$\langle\{a = 0, b = 0\}\rangle,$
$\langle\{a = 0, b = 0\}, p1aktion1, \{a = 1, b = 0\}\rangle,$
$\langle\{a = 0, b = 0\}, p1aktion2, \{a = 0, b = 1\}\rangle,$
$\langle\{a = 0, b = 0\}, p1aktion1\{a = 1, b = 0\}, p1aktion2, \{a = 0, b = 1\}\rangle,$
$\langle\{a = 0, b = 0\}, p1aktion2\{a = 0, b = 1\}, p1aktion1, \{a = 1, b = 1\}\rangle$

Abbildung 2.6 – Ausgewählte Pfade des Programms aus Abbildung 2.5

Zusammengefasst definiert $S = (V, \Sigma, q_0)$ ein System. Werden nun einzelne Aktionen ausgeführt, so wird die alternierende Sequenz aus Zuständen und Aktionen als Pfad α von S bezeichnet. A bezeichnet die Menge aller Pfade α von S. Abbildung 2.6 zeigt eine ausgewählte Menge von Pfaden des Beispiels aus Abbildung 2.5. Die Menge aller Pfade α die in einem gegebenen Zustand $q \in Q$ enden, wird mit $\mathcal{A}(q)$ bezeichnet, wobei für alle $q \in Q$ gilt: $\mathcal{A}(q) \subseteq A$. Falls $\mathcal{A}(q) = \varnothing$, so ist q nicht erreichbar und das System kann ohne äußere Einflüsse oder Manipulationen nie in diesem Zustand q vorgefunden werden. [Dew12, S. 75f]

Die Zusammenfassung von Sequenzen beliebig vieler Aktionen zu einer semanti-

schen Entität wird als Operation bezeichnet. Gerade in realen Computersystemen umfassen selbst nach Außen für einen Betrachter einfach wirkende Operationen wie das Löschen einer E-Mail eine Vielzahl von einzelnen Aktionen, z.B. auf der Ebene des Betriebssystems oder der Hardware [Dew12, S. 77]. In dieser Arbeit wird im Folgenden der Begriff Ereignis als Synonym für Aktionen verwendet.

2.4.2 Rekonstruktion von Aktionen im System

Um nun Assoziationen wie in Abschnitt 2.2 dargestellt feststellen zu können, müssen die Pfade, die ein System S in einen bestimmten Zustand q geführt haben könnten, rekonstruiert werden. Dieses Problem wird auch als allgemeines Rekonstruktionsproblem bezeichnet. Das Problem ist definiert als:

> „Sei $S = (V, \Sigma, q_0)$ ein System. Das allgemeine Rekonstruktionsproblem [..] für S und einen Zustand q ist die Rekonstruktion aller Pfade α des Systems, die in Zustand q führen. Gesucht ist also die Menge $\mathcal{A}(q)$." [Dew12, S. 79f]

In Abschnitt 2.2 wurde bereits angemerkt, dass das komplette reale System in das Modell überführt werden muss, um das allgemeine Rekonstruktionsproblem lösen zu können. Da es in der Praxis aber notwendigerweise nicht nötig ist, alle Pfade zu rekonstruieren, wirft Dewald [Dew12] das spezifische Rekonstruktionsproblem sowie das spezifische Gruppenrekonstruktionsproblem auf und untersucht deren Lösbarkeit. Der Vorteil dieser schwächeren Problemstellungen ist, dass man lokal, d.h. ohne Kenntnis des gesamten Automaten, Rückschlüsse auf das Stattfinden von Aktionen schließen kann [Dew12, S. 153f].

Mithilfe des spezifischen Rekonstruktionsproblems hat Dewald [Dew12] untersucht, inwieweit sich Rückschlüsse auf das Stattfinden genau einer Aktion σ in der Vergangenheit ziehen lassen. Dazu muss man zwischen drei Fällen unterscheiden (nach [Dew12, S. 80]):

1. Um q zu erreichen hat σ definitiv stattgefunden ($\forall \alpha \in \mathcal{A}(q) : \sigma \in \alpha$).
2. Um q zu erreichen hat σ definitiv nicht stattgefunden ($\forall \alpha \in \mathcal{A}(q) : \sigma \notin \alpha$).
3. Um q zu erreichen hat σ möglicherweise stattgefunden ($\exists \alpha, \alpha' \in \mathcal{A}(q) : (\sigma \in \alpha) \wedge (\sigma \notin \alpha')$).

Das spezifische Rekonstruktionsproblem ist definiert als:

> „Sei $S = (V, \Sigma, q_0)$ ein System. Das Spezifische Rekonstruktionsproblem [..] für S und einen Zustand q und eine konkrete Aktion $\sigma \in \Sigma$ definieren wir als die Entscheidung, ob σ definitiv stattgefunden hat oder definitiv nicht stattgefunden hat, um Zustand q zu erreichen. Falls σ in die dritte

Kategorie fällt, bezeichnen wir das [spezifische Rekonstruktionsproblem] als nicht lösbar.“ [Dew12, S. 80]

Anstelle einer einzelnen Aktion σ kann es auch ausreichend sein, eine Aussage hinsichtlich des Auftretens einer Aktion aus einer Menge Σ' an Aktionen zu treffen. Dewald [Dew12] spricht dabei vom spezifischen Gruppen-Rekonstruktionsproblem. Auch für dieses Problem lassen sich drei Fälle unterscheiden (nach [Dew12, S. 81]):

1. Mindestens eine Aktion aus Σ' hat definitiv stattgefunden, um q zu erreichen $(\forall \alpha \in \mathcal{A}(q) : \exists \sigma \in \Sigma' : \sigma \in \alpha)$.
2. Es hat definitiv keine Aktion aus Σ' stattgefunden, um q zu erreichen $(\forall \alpha \in \mathcal{A}(q) : \forall \sigma \in \Sigma' : \sigma \notin \alpha)$.
3. Eine oder mehrere Aktionen aus Σ' haben möglicherweise stattgefunden, um q zu erreichen $(\exists \alpha, \alpha' \in \mathcal{A}(q) : \exists \sigma, \sigma' \in \Sigma' : (\sigma \in \alpha) \wedge (\sigma' \notin \alpha'))$.

Das spezifische Gruppenrekonstruktionsproblem ist definiert als:

„Das Spezifische Gruppenrekonstruktionsproblem [..] für

- ein System S (mit seiner Menge von Aktionen Σ, der Menge von Variablen V und dem Initialzustand q_0),
- einen Zustand q und
- eine konkrete Menge von Aktionen $\Sigma' \subseteq \Sigma$

[ist] definier[t] [..] als die Entscheidung, ob Σ' in die erste oder zweite Kategorie fällt. Falls Σ' in die dritte Kategorie fällt, [ist] das [spezifische Gruppenrekonstruktionsproblem] [..] nicht lösbar.“ [Dew12, S. 82]

Das spezifische Gruppenrekonstruktionsproblem ist insbesondere dann interessant, wenn der dritte Fall des spezifischen Rekonstruktionsproblems eintritt und dieses nicht lösbar ist. Unter gewissen Umständen kann dann nämlich über die Lösung des spezifischen Gruppenrekonstruktionsproblems dennoch eine Aussage getroffen werden. [Dew12, S. 82]

Nachdem in diesem Abschnitt die Grenzen bei der Rekonstruktion von Pfaden und Vorzuständen eines Systems diskutiert wurden, gehen die folgenden Abschnitte konkreter auf die aus einer Aktion resultierenden digitalen Spuren bzw. nicht resultierenden Spuren ein, da sie nach Dewald [Dew12, S. 83] die Grundlage für die Lösung der obigen Probleme darstellen.

2.4.3 Spuren

Die Schlussfolgerungen bzw. Assoziationen bei digitalen forensischen Untersuchungen basieren im Wesentlichen auf der Lösung bzw. Lösbarkeit der im vorherigen

Abschnitt 2.4.2 aufgeworfenen Problemstellungen. In Abschnitt 2.2 wurde bereits erwähnt, dass die Kenntnis des Systems, sprich das Expertenwissen essentiell für das Ziehen von Schlüssen bei digitalen forensischen Untersuchungen ist. Für die Rekonstruktion der aufgetretenen Ereignisse bzw. Aktionen und das Schließen auf vorherige Systemzustände ist daher die Kenntnis der von einer Aktion hervorgerufenen Spuren entscheidend. Digitale Spuren wurden dazu bereits in Abschnitt 2.3 allgemein definiert. Die Spurenmenge einer Aktion σ im Speziellen ist definiert als:

> Die Spurenmenge E einer Aktion σ des Systems $S = (V, \Sigma, q_0)$ ist die Menge aller Teilmengen von Wertzuweisungen zu Variablen V deren enthaltene Zuweisungen von σ ausgeführt werden. Weiter ist die Menge E unter Teilmengen abgeschlossen. [Dew12, S. 83f]

Die Spurenmenge bzw. Spuren einer Aktion σ werden formal mit der Potenzmenge $\mathcal{P}$ bestimmter Variablen-Wert-Paare formuliert. Eine Spur $e \in E(\sigma)$ einer Aktion σ kann in Zustand q beobachtet werden, wenn der e entsprechende boolesche Ausdruck in q wahr ist. [Dew12, S. 84]

Für die Aktion *p1aktion1* des Beispiels aus Abbildung 2.5 ist $E(p1aktion1) = \{\{a = 1\}, \varnothing\}$ und für die Aktion *p1aktion2* ist $E(p1aktion2) = \{\{a = 0, b = 1\}, \{a = 0\}, \{b = 1\}, \varnothing\}$. Vergleicht man nun die Spuren der Aktion *p1aktion1* mit denen der Aktion *p1aktion2*, so ist erkennbar, dass es eine Überschneidung der Spurenmengen $E(p1aktion1)$ und $E(p1aktion2)$ gibt. Um nun also exakt auf eine Aktion schließen zu können, ist es erforderlich, den Begriff der Spur weiter zu verfeinern. Dewald [Dew12] führt dazu den Begriff der charakteristischen Spur bzw. Spurenmenge ein. Charakteristische Spuren CE sind alle Spuren einer Aktion $\sigma \in \Sigma$, die nicht durch eine der verbliebenen Aktionen $\Sigma' \in \Sigma$ mit $\sigma \notin \Sigma'$ hervorgerufen werden oder Teil des Initialzustandes sind [Dew12, S. 86]. Exakter sind charakteristische Spuren nach [Dew12, S. 86] definiert als:

$$CE(\sigma, \Sigma') = E(\sigma) \setminus (\mathcal{P}(ME(\Sigma') \cup ZE)) \tag{2.1}$$

ZE definiert dabei die Variablen-Wert-Paare des Initialzustands als $ZE = \{[v = d] | [v = d] \in q_0\}$. ME definiert die sogenannten kombinierten Spuren einer Menge von Aktionen Σ als Vereinigung aller Spuren aller Aktionen in Σ [Dew12, S. 86]. Es gilt (nach [Dew12, S. 86]):

$$ME(\Sigma) = \bigcup_{\sigma \in \Sigma} \bigcup_{e \in E(\sigma)} e \tag{2.2}$$

Wird nicht nur eine Aktion σ untersucht, sondern eine Menge von Aktionen Σ, so kann man unter Umständen gemeinsame charakteristische Spuren CCE beobachten. Gemeinsame charakteristische Spuren einer Menge von Aktionen Σ' bezüglich einer anderen Menge von Aktionen Σ'' sind definiert „als die Vereinigung der charakteristi-

schen Spuren aller Aktionen $\sigma' \in \Sigma'$ bezüglich Σ''“ [Dew12, S. 88]. Formal gilt (nach [Dew12, S. 88]):

$$CCE(\Sigma', \Sigma'') = \bigcup_{\sigma' \in \Sigma'} CE(\sigma', \Sigma'') \tag{2.3}$$

Die beiden Mengen von Aktionen Σ' bzw. Σ'' sind Teilmengen einer Menge von Aktionen Σ aus dem System $S = (V, \Sigma, q_0)$, also $\Sigma' \subseteq \Sigma$ bzw. $\Sigma'' \subseteq \Sigma$ [Dew12, S. 88].

2.4.4 Kontraspuren

Während Spuren bzw. charakteristische Spuren explizit auf die vorherige Ausführung einer bestimmten Aktion σ im System hindeuten, gibt es auch Spuren, durch die die vorherige Ausführung bestimmter Aktionen ausgeschlossen werden kann. Diese Spuren nennt man Kontraspuren. [Dew12, S. 90]

Die Kontraspurenmenge XE einer Aktion σ des Systems $S = (V, \Sigma, q_0)$ ist diejenige Menge von Teilmengen von Variablen $v \in V$ zusammen mit der Zuweisung von Werten $d \in D$ zu diesen Variablen, denen σ einen Wert zuweist. Dabei sind den $v \in V$ in der Menge der Kontraspuren andere Werte zugewiesen als die Werte, die den $v \in V$ durch σ zugewiesen werden [Dew12, S. 91]. Die Menge ist zudem unter Teilmengen abgeschlossen. Formal gilt (nach [Dew12, S. 91]):

$$XE(\sigma) = \mathcal{P}\Big(\bigcup_{[v=d] | \exists d' \neq d : [v=d'] \in \sigma} \{[v = d]\} \Big) \tag{2.4}$$

Kontraspuren alleine sind aber nicht generell ausreichend, um die Ausführung einer bestimmten Aktion σ auszuschließen [Dew12, S. 92f]. Wie auch für Spuren gibt es bei den Kontraspuren aussagekräftigere charakteristische Kontraspuren CXE, die nicht durch die Ausführung einer anderen Aktion entstehen können [Dew12, S. 93]. Nach [Dew12, S. 93] gilt:

$$CXE(\sigma, \Sigma') = XE(\sigma) \backslash \mathcal{P}(ME(\Sigma')) \tag{2.5}$$

Um das Auftreten einer Menge von Aktionen, die die selbe Menge an Kontraspuren und dementsprechend keine charakteristischen Kontraspuren besitzen, auszuschließen, gibt es zudem die gemeinsamen charakteristischen Kontraspuren $CCXE$ [Dew12, S. 94, 96]. „Gemeinsame charakteristische Konstraspuren sind diejenigen charakteristischen Konstraspuren, die alle Aktionen [einer] Menge gemeinsam haben.“ [Dew12, S. 94] Formal gilt nach [Dew12, S. 94]:

$$CCXE(\Sigma', \Sigma'') = \bigcap_{\sigma' \in \Sigma'} CXE(\sigma', \Sigma'') \tag{2.6}$$

Wenn sich die Aktionen $\sigma' \in \Sigma'$ hinsichtlich ihrer Kontraspuren nicht unterscheiden lassen, kann man dennoch das Auftreten aller Aktionen der Menge Σ' aufgrund der

gemeinsamen charakteristischen Kontraspuren dieser Aktionen ausschließen [Dew12, S. 96].

2.4.5 Differential Forensic Analysis

Da reale Computersysteme aufgrund ihrer Komplexität nach heutigem Stand nicht komplett als endliche Automaten modelliert werden können [GP04],[DF12, S. 153], wird zur Erstellung einer Wissensbasis, die das Ziehen von Schlüssen bzw. das Prüfen von Hypothesen erlaubt, bereits seit langem intuitiv eine alternative Methodik in manchen Teilbereichen der digitalen Forensik verwendet [GNY12]. Garfinkel et al. [GNY12] beschreiben diese Methodik formal und bezeichnen sie als Differential Forensic Analysis (DFA). Die DFA ist im wesentlichen eine Methodik um die Spurenmenge einer Operation Σ' im Sinne einer Reihe von Aktionen σ bzw. Ereignissen in einem realen Computersystem $S = (V, \Sigma, q_0)$ zu bestimmen.

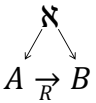


Abbildung 2.7 – Modell der Differential Forensic Analysis (nach [GNY12])

Abbildung 2.7 zeigt das generelle Modell hinter der DFA. Aus einem gemeinsamen Ursprung $\aleph$ entstehen zwei Images A und B. Die Ereignisse bzw. die einzelnen Aktionen, die das Image A in das Image B überführen, werden über die Funktion R beschrieben. In der Terminologie des Modells aus Abschnitt 2.4.1 ist sowohl A als auch B ein bestimmter Zustand q eines Systems $S = (V, \Sigma, q_0)$. R beschreibt dementsprechend eine Menge an Aktionen Σ', die das System vom Zustand q_A in den Zustand q_B überführen. Über die Erkenntnisse aus einer DFA lässt sich damit das spezifische Gruppen-Rekonstruktionsproblem für eine Menge an Aktionen Σ' beantworten, d.h. im Falle einer digitalen forensischen Untersuchung können auf Basis der Erkenntnisse aus einer DFA die spezifischen Spuren einer Menge von Aktionen Σ' identifiziert werden.

Die DFA wird und wurde bereits sehr lange in der digitalen Forensik eingesetzt, z.B. um auf das Verhalten von Malware mittels Reverse Engineering Methodiken zu schließen oder um Veränderungen in Netzwerkströmen von Unternehmen aufzudecken. Dabei werden immer mindestens zwei digitale Objekte, d.h. Images im Sinne von Zuständen verglichen. Das Ziel ist stets die Identifikation von Eigenschaften, oder speziell für die digitale Forensik, von charakteristischen Spuren. Die DFA verallgemeinert all diese Ansätze und bietet eine einheitliche Basis für verschiedene Analyseszenarien. [GNY12]

Zur konkreten Durchführung einer DFA werden zunächst von einem gemeinsamen Ursprung wie z.B. $\aleph$ in Abbildung 2.7 zwei Images erstellt. In Abbildung 2.7 sind die beiden Images durch A und B dargestellt. Anschließend wird das Delta $(B - A)$ mithilfe

einer Unterscheidungsstrategie ermittelt. Die Unterscheidungsstrategie ist eine konkrete Methodik, um die Unterschiede zwischen A und B zu ermitteln. Je nach Art und Beschaffenheit der beiden Images, z.B. Arbeitsspeicherabbilder, Festplattenabbilder oder auch zwei Dateien, muss eine entsprechende Unterscheidungsstrategie gewählt und die Unterschiede ermittelt werden [GNY12]. Für eine Datei A kann z.B. mittels des Tools `diff` der zeilenweise Unterschied zur Datei B ermittelt werden [GNY12]. Mithilfe der Unterschiede könnte man dann einen Patch entwickeln, durch dessen Anwendung A zu B überführt werden würde [GNY12]. Die Unterschiede sind jedoch sehr viel interessanter für die digitale Forensik, da mit deren Hilfe Rückschlüsse auf den vorherigen Zustand der Datei B und die wahrscheinlich abgelaufene Operation möglich sind. Durch eine DFA kann zudem das normale Verhalten eines Systems aufgezeichnet werden. Im Falle einer digitalen forensischen Untersuchung können diese Ergebnisse dann mit dem gesicherten Image verglichen und die Unterschiede sichtbar gemacht werden [GNY12].

Die Durchführung einer DFA zur Aufzeichnung des normalen Systemverhaltens und die anschließende Nutzung dieser Erkenntnisse wird z.B. von Flusche [Flu01] beschrieben. Wenngleich in [Flu01] noch nicht von einer DFA gesprochen wird, so kann die von Flusche [Flu01] durchgeführte Analyse dennoch als DFA bezeichnet werden. Konkret geht es in [Flu01] um einen Fall, bei dem nachgewiesen werden musste, dass Dokumente von Disketten und der Festplatte eines Laptops tatsächlich weitergegeben wurden. Flusche [Flu01] hat zur Durchführung der DFA ein zum sichergestellten Equipment identisches Setup verwendet und die Druckprozedur so oft wiederholt, bis er mit hoher Sicherheit die Aussage treffen konnte, dass durch das Drucken und den Wechsel des zu verwendeten Druckers jeweils eine Datei auf der Festplatte des Laptops in der gleichen Weise verändert wird [Flu01]. Das Ergebnis der DFA hat beim dem in [Flu01] beschriebenen Fall dazu geführt, dass über die digitalen Spuren vom sichergestellten Gerät bewiesen werden konnte, dass ein nicht zur Organisation gehörender Drucker verwendet wurde, um geheime Dokumente auszudrucken und weiterzugeben.

Der in [Flu01] beschriebene Fall sowie die obigen Ausführungen zeigen, dass die DFA eine strukturierte, nachvollziehbare und wissenschaftliche Methodik darstellt, durch die sich eine gemeinsame Wissensbasis über die Funktionsweise von Systemen und die dabei entstehenden digitalen Spuren entwickeln kann. Das bislang in der Breite fehlende gemeinsame Verständnis des *normalen* Systemverhaltens ist nach Cohen [Coh10] einer der Hauptgründe für die falsche Interpretation von digitalen Spuren, da aktuell nur wenige Experten die unter normalen Umständen vorhandenen digitalen Spuren kennen und das Fehlen von digitalen Spuren bemerken und ggf. auch erklären können [Coh10].

2.5 Zusammenfassung

In diesem Kapitel wurden zunächst die Grundprinzipien der digitalen Forensik sowie der forensischen Wissenschaften im Allgemeinen in den Abschnitten 2.1 und 2.2 diskutiert. Anschließend wurde die digitale Spur, ihre Entstehung und ihre Eigenschaften in den Abschnitten 2.3 und 2.4 näher beleuchtet. Abbildung 2.8 zeigt zusammenfassend die Beziehungen zwischen digitalen Spuren, Aktionen im System und der Wissensbasis der digitalen Forensik anhand eines UML-Diagramms.

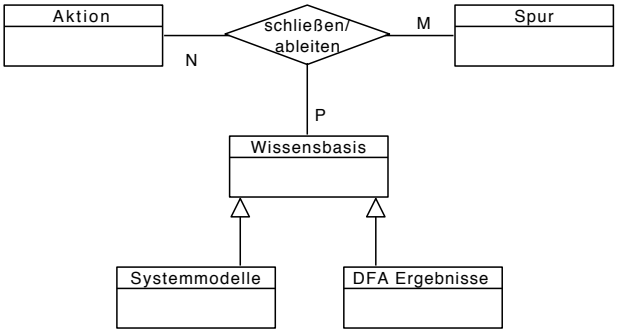


Abbildung 2.8 – Digitale Spuren und die Wissensbasis

Das Schließen oder die Assoziation, dass in einem System S eine bestimmte Aktion ausgeführt wurde, wird, wie in den Abschnitten 2.1 - 2.4 festgestellt, über die vorhandene Wissensbasis in der digitalen Forensik begründet. Die Wissensbasis besteht demnach aus Modellen, die ein System homomorph abbilden, z.B. in Form eines Modells des endlichen Automaten wie in Abschnitt 2.4 beschrieben. Weiter enthält die Wissensbasis auch Erkenntnisse aus der strukturierten Beobachtung des Systemverhaltens bei der Ausführung bestimmter Operationen wie unter Abschnitt 2.4.5 beschrieben. Die Beziehung zwischen der Aktion, der digitalen Spur und der Wissensbasis ist demnach essentiell, um eine Schlussfolgerung bzw. Assoziation wissenschaftlich zu begründen.

Neben den theoretischen Grundlagen der digitalen Forensik wurden in Abschnitt 2.3 auch die praktischen Probleme und Gefahren für die Rechtssicherheit digitaler Spuren angesprochen. Insbesondere die leichte und nahezu spurlose Manipulierbarkeit digitaler Spuren stellen ein großes Problem für die digitale Forensik in der Praxis dar, wodurch mit den digitalen Spuren sehr sorgsam umgegangen werden muss.

KAPITEL 3

Informationssysteme und Prozesse

Dieses Kapitel geht auf Informationssysteme (IS) als „soziotechnische Systeme[, bestehend] aus Menschen (personellen Aufgabenträgern), Informations- und Kommunikationstechnik (maschinellen Aufgabenträgern) und Organisation (Funktionen, Geschäftsprozessen, Strukturen und Management) sowie den Beziehungen zwischen diesen drei Objekttypen“ [ÖBF+10] ein, indem im folgenden Abschnitt 3.1 der Aufbau von Informationssystemen und die Rolle der Anwendungssysteme geklärt wird. Im Anschluss daran wird im Abschnitt 3.2 auf Geschäftsprozesse eingegangen, da diese eine wesentliche Rolle bei der Gestaltung von Informationssystemen in Unternehmen einnehmen [Wes12, S. 4], wodurch ihnen auch eine zentrale Rolle in der, in Kapitel 6 detailliert vorgestellten Unternehmensforensik, zukommt.

3.1 Informations- und Anwendungssysteme

„[Unter] einem Informationssystem [wird] ein System verstanden, das Informationen verarbeitet, d.h. erfasst, überträgt, transformiert, speichert und bereitstellt“ [FS13, S. 3]. Im folgenden Abschnitt 3.1.1 werden nun zunächst die generellen Eigenschaften sowie der Aufbau von Informationssystemen diskutiert. In Abschnitt 3.1.2 werden dann die unterschiedlichen Klassen der Anwendungssysteme (AWS) vorgestellt.

3.1.1 Aufbau und Eigenschaften von Informationssystemen

Ein Informationssystem besteht, wie in Abbildung 3.1 ersichtlich aus der Aufgabenträger- und der Aufgabenebene. In der Aufgabenebene sind die Informationsverarbeitungsaufgaben $(A_1, A_2, .., A_n)$, die über eine Informationsbeziehung miteinander verbunden sind, enthalten. Auf der Ebene der Aufgabenträger gibt es entweder maschinelle Aufgaben-

träger ($R_1, R_2, .., R_n$) oder personelle Aufgabenträger ($P_1, P_2, .., P_n$). Die Aufgabenträger sind wiederum über Kommunikationsbeziehungen bzw. Kommunikationssysteme miteinander verbunden. Zwischen der Aufgaben- und Aufgabenträgerebene gibt es schließlich Zuordnungen, d.h. den betrieblichen Aufgaben ($A_1, A_2, .., A_n$) sind jeweils entsprechende Aufgabenträger zugeordnet, die diese Aufgaben durchführen. [FS13, S. 4f]

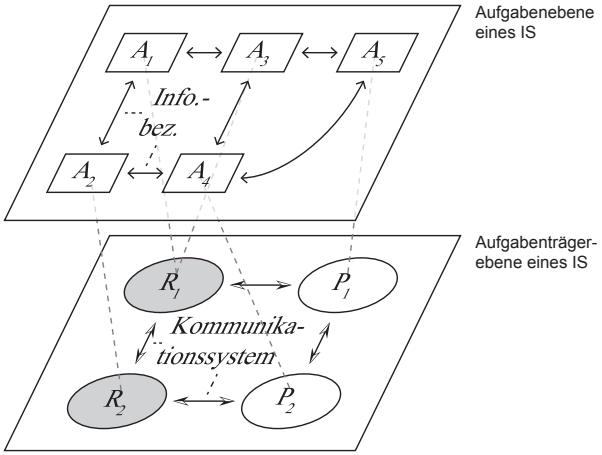


Abbildung 3.1 – Aufgabenebene und Aufgabenträgerebene eines Informationssystems (nach [FS13, S. 4])

Die maschinellen Aufgabenträger stellen dabei die Anwendungssysteme dar [FS13, S. 448]. Diese beinhalten die Kommunikationsschnittstellen sowie die IT-Infrastruktur und lassen sich, wie in Abbildung 3.2 dargestellt, in die drei aufeinander aufbauenden Ebenen Hardwaresysteme, Systemsoftware und Anwendungssoftware unterteilen [FS13, S. 5, 448]. Weiter beinhalten die Anwendungssysteme aus Sicht der Systemtheorie wiederum Programme, Rechner und Kommunikationssysteme [FS13, S. 13].

Eine andere Sicht auf ein Informationssystem wird in Abbildung 3.3 dargestellt. Nach Laudon et al. [LLS06] ist ein Informationssystem „[ein] System, das für die Zwecke eines Teils eines bestimmten Unternehmens geschaffen bzw. in diesem Betrieb eingesetzt wird. Ein Informationssystem enthält die dafür notwendige Anwendungssoftware und Daten und ist in die Organisations-, Personal- und Technikstrukturen des Unternehmens eingebettet“ [LLS06, S. 31]. Der Aufbau folgt nach Laudon et al. [LLS06] dem in Abbildung 3.3 dargestelltem Schema. Laudon et al. [LLS06] unterscheiden zwischen dem Anwendungssystem und dem Informationssystem, wobei ein Anwendungssystem aus Anwendungssoftware (den Programmen) für ein konkretes Anwendungsgebiet im Unternehmen, der IT-Infrastruktur, auf der die Anwendungssoftware läuft, sowie den Daten (z.B. Dateien, Datenbanken, verteilte Datenbanken, etc.), die von der

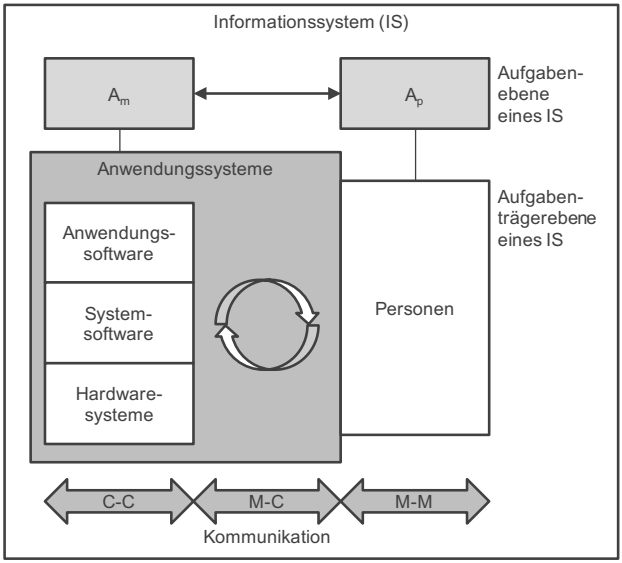


Abbildung 3.2 – Informationsbeziehungen und Kommunikationssysteme im Informationssystem (nach [FS13, S. 5])

Anwendungssoftware genutzt werden, besteht [LLS06, S. 31f]. Nach Laudon et al. [LLS06] werden Anwendungssysteme für eine Klasse bzw. einen Typ von Unternehmen entwickelt und kommen in einem oder mehreren Unternehmen zur Erfüllung eines Unternehmenszwecks zum Einsatz. In einem Unternehmen werden zudem mehrere verschiedene Anwendungssysteme verwendet. Anwendungssysteme sind in der Regel Teil des Informationssystems des Unternehmens und stellen den technisch realisierten Teil (Hardware, Software, Daten) des Systems dar [LLS06, S. 31].

Ein Informationssystem wird wie das Anwendungssystem ebenfalls für ein betriebliches Aufgabengebiet geschaffen. Das Informationssystem betrachtet aber neben einem Anwendungssystem auch die Organisationsstrukturen, in denen das System eingebettet ist bzw. eingebettet werden soll, sowie die damit arbeitenden Menschen. Im Gegensatz zum Anwendungssystem ist ein Informationssystem immer ein individuelles, an die speziellen organisatorischen und personellen Rahmenbedingungen des jeweiligen Unternehmens, angepasstes System. [LLS06, S. 31f]

Sowohl in [LLS06] als auch in [FS13] werden noch eine Reihe anderer Definitionen von Informationssystemen genannt. Diese Arbeit folgt der Definition sowie der Sichtweise von Ferstl und Sinz [FS13]. Die Informationssysteme dienen demnach entweder der Lenkung von betrieblichen Prozessen oder der Erstellung von Dienstleistungen in Form von Informationen [FS13, S. 12]. Weiter nehmen die im Informationssystem enthaltenen Anwendungssysteme Aufgaben, die über die Prozesse des Unternehmens definiert

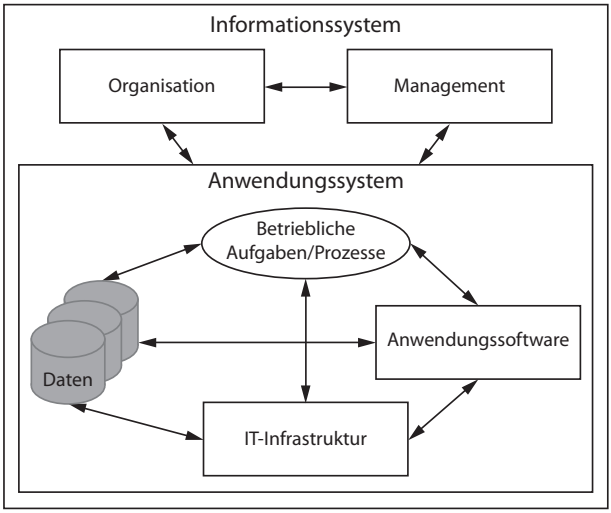


Abbildung 3.3 – Zusammenhang zwischen Informations- und Anwendungssystem (nach [LLS06, S. 32])

sind, wahr und führen diese als maschinelle Aufgabenträger aus [FS13, S. 4f]. Die aus dieser Aufgabenverarbeitung sowie die aus der Kommunikation mit den personellen Aufgabenträgern resultierenden digitalen Daten sind der zentrale Untersuchungsgegenstand der Unternehmensforensik, da, wie bereits in Abschnitt 2.1 im vorherigen Kapitel 2 festgestellt wurde, die digitale Forensik auf digitale Spuren beschränkt ist.

3.1.2 Anwendungssystemklassen

Ein AWS besteht, wie in Abbildung 3.2 dargestellt aus mehreren unterschiedlichen, aufeinander aufbauenden Schichten. Van der Aalst et al. [vtW03] haben ein ähnliches Modell, allerdings aus einem anderen Betrachtungswinkel entwickelt. Das in Abbildung 3.4 dargestellte Modell zeigt die verschiedenen Klassen von AWS. In der Mitte befindet sich demnach das Betriebssystem. Die zweite Ebene besteht aus generischen Anwendungen, die in einer großen Bandbreite von Unternehmen zum Einsatz kommen können. Weiter können diese auch im Unternehmen selbst in verschiedenen Bereichen eingesetzt werden. Beispiele für solche Systeme aus der zweiten Ebene sind Datenbanksysteme, Texteditoren oder Tabellenkalkulationsprogramme. Die dritte Schicht besteht aus den domänenspezifischen Anwendungen, die nur in spezifischen Unternehmen bzw. nur in bestimmten Abteilungen im Unternehmen eingesetzt werden. Beispiele dafür sind Entscheidungsunterstützungssysteme zur Planung von Fahrzeugrouten, Callcentersoftware oder Anwendungen zur Personalverwaltung. Die vierte Ebene besteht aus maßgeschneiderten, individuellen Anwendungen. Diese sind dann spezifisch für ein

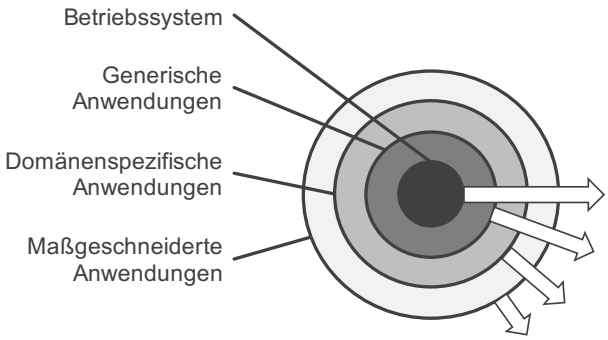


Abbildung 3.4 – Verschiedene Klassen von Anwendungssystemen (nach [vtW03])

Unternehmen entwickelt. [vtW03]

Die verschiedenen Schichten aus Abbildung 3.4 werden dabei im Verlauf der Zeit immer mächtiger und decken dann auch die Funktionalitäten der jeweils äußeren Schicht mit ab [vtW03]. Aktuelle Datenbanksysteme aus der zweiten Schicht bilden mittlerweile z.B. auch Funktionen ab, die vorher nur in individuellen Unternehmensanwendungen enthalten waren [vtW03]. Aus diesem Grund besteht heute die Herausforderung bei der Gestaltung von AWS weniger im Programmieren neuer Software als im Orchestrieren und Integrieren bestehender Softwareartefakte aus den unterschiedlichen Schichten [vtW03]. Durch die daraus resultierende hohe Anzahl an unterschiedlichen Applikationen, der zur Orchestrierung benötigten Schnittstellen, dem hohen Automatisierungsgrad der Prozesse innerhalb von Unternehmen sowie durch das Ineinandergreifen von Prozessen aus verschiedenen Unternehmen, sind die heute gängigen Anwendungssystemarchitekturen daher sehr komplex [HSW04],[RWR06, S. 6ff, 11],[ASM+12, S. 5ff],[FS13, S. 447]. Mittlerweile konzentrieren sich die Systemarchitekten und Ingenieure deshalb auf die Gestaltung der AWS mittels einer prozessorientierten Denk- und Sichtweise [vtW03].

3.2 Anwendungssysteme, Daten und Prozesse

Die prozessorientierte Denk- und Sichtweise wird in vielen Bereichen von Unternehmen verwendet und gewinnt durch die wettbewerbsbedingte Notwendigkeit einer flexiblen und effizienten Unternehmensgestaltung zunehmend an Attraktivität [Kör95],[BRU00],[BK12, S. 4f],[Har15, S. 37ff]. Durch die Spezifikation eines Prozesses wird festgelegt, welche Aufgaben, von wem, wann, wo, unter welchen Umständen und mit welchen Informationen durchgeführt werden sollen [CKO92],[Ham15, S. 8]. „Ein Prozess ist die inhaltlich abgeschlossene, zeitliche und sachlogische Folge von Aktivitäten, die zur Bearbeitung eines betriebswirtschaftlich relevanten Objektes notwendig

sind“ [BK12, S. 6]. Ohne festgelegte Prozesse gäbe es nur unkoordinierte individuelle Aktivitäten und organisatorisches Chaos [Ham15, S. 8]. Alle Aufgaben sind über Prozesse organisiert, wenngleich dies für eher kreative Aktivitäten oder Entwicklungsaufgaben nicht direkt offensichtlich sein mag [Ham15, S. 11]. Auf organisatorischer Ebene sind Geschäftsprozesse gar essentiell, um zu verstehen, wie eine Organisation funktioniert [Rec10],[Wes12, S. 4]. Geschäftsprozesse sind spezielle Prozesse, die der Erfüllung der obersten Ziele der Unternehmung (Geschäftsziele) dienen und das zentrale Geschäftsfeld beschreiben [BK12, S. 6f].

Im folgenden Abschnitt 3.2.1 werden nun zunächst die Beziehungen zwischen den Prozessen, den AWS sowie der Gestaltung von AWS betrachtet. In Abschnitt 3.2.2 wird dann abschließend die Modellierung von Prozessen vorgestellt und diskutiert.

3.2.1 Prozesse und Anwendungssysteme

Neben der Beschreibung des zentralen Geschäftsfelds einer Unternehmung spielen Geschäftsprozesse auch eine wichtige Rolle bei der Gestaltung und Realisierung von AWS [Kör95],[Wes12, S. 4]. Das Themenfeld Enterprise Application Integration (EAI) beschäftigt sich konkret mit einer solchen prozessorientierten Integration der Aufgaben des Unternehmens und der AWS [AS06],[FS13, S. 260]. Ein weiteres Schlagwort in diesem Bereich ist die sogenannte Unternehmensarchitektur, oder auch Enterprise Architecture (EA) genannt. „[Eine] Unternehmensarchitektur subsumiert das Zusammenwirken organisatorischer, technischer und psychosozialer Aspekte bei der Planung und Entwicklung betrieblicher soziotechnischer Informationssysteme [und] geht explizit von bereits existierende[n] Elementen aus [..]“ [AS06].

Außerhalb der IT konnten sich bislang aber weder die Methoden aus dem Bereich der EAI noch das Verwalten und Entwickeln einer EA mittels der Methoden aus dem sogenannten Enterprise Architecture Management (EAM) durchsetzen [AS06],[RR15, S. 82]. Geschäftsprozesse konnten sich dagegen als gemeinsame Sprache zwischen der Unternehmensführung und den IT-Führungskräften etablieren [vtW03],[AS04],[vSR+14],[Har15, S. 74]. IT-Führungskräfte können hierdurch neue Initiativen anhand der dadurch möglichen Verbesserungen an spezifischen Prozessen erklären [Har15, S. 53]. Weiter ist gerade „[..] die Prozessorientierung [eine] Voraussetzung für die Nutzung technologischer Potentiale“ [BK12, S. 12],[vSR+14].

Um neben einem gemeinsamen Verständnis der Aktivitäten des Unternehmens auch einen Wert für die Gestaltung und Implementierung von AWS zu haben, müssen bei der Prozessmodellierung für die Geschäftsprozesse detaillierte Attribute sowie Referenzen zu anderen relevanten Informationsmodellen wie Datenmodellen gepflegt werden [BRU00, SOSF04],[RSD12, S. 57]. Für einen Geschäftsprozess gibt es zudem klar definierte Ein- und Ausgabedaten [Dav93, S. 5],[BRU00, STA15]. Die Modellierung von Daten und Datenflüssen wird aber bei der Geschäftsprozessmodellierung bislang vernachlässigt [SZS04, CG09]. Dabei sind Prozessmodelle je nach Anwendungszweck

unterschiedlich detailliert [CKO92, BRU00]. Zur Gestaltung und Realisierung von AWS eignen sich besonders die Prozessmodelle, welche für den Zweck der Softwareauswahl, dem modellbasierten Customizing, der Softwareentwicklung, dem Workflow Management oder der Simulation modelliert wurden [RSD12, S. 56ff]. Diese enthalten dann auch die notwendigen Attribute, Parameter oder Beziehungen zu Datenmodellen und können dadurch ggf. direkt in Softwarecode überführt werden [RSD12, S. 57].

Neben dem Detaillierungsgrad der Prozessmodelle gibt es zudem eine Unterscheidung der Modelle hinsichtlich des Bezugs zur Realwelt. Man unterscheidet zwischen Istmodellen, Sollmodellen und Referenzmodellen. Istmodelle dokumentieren die Sachverhalte der Realwelt in ihrem aktuellen Zustand. Ein Sollmodell stellt den zukünftig gewünschten Zustand eines Sachverhaltes in der Realwelt dar und Referenzmodelle abstrahieren konkrete Sachverhalte, um eine anerkannte Lösung für eine allgemeine Problemstellung bereit zu stellen. [HMN15, S. 102f]

Zusammenfassend kann man feststellen, dass Prozesse als Mediator zwischen der Unternehmensorganisation und der IT dienen. AWS werden heute zur Unterstützung und Ausführung von Prozessen eingesetzt und die Beziehungen zwischen den AWS und den Aufgaben des Unternehmens über Prozesse festgehalten. Die Modellierung von Prozessen ist zwar oft wenig detailliert und enthält nur in seltenen Fällen genügend Informationen zur direkten Umsetzung eines Prozessmodells mithilfe von AWS. Für die digitale Forensik in Unternehmen bleibt jedoch festzuhalten, dass die Prozesse das Funktionieren des Unternehmens beschreiben und in Form von (Ist)Prozessen dokumentieren.

3.2.2 Modellierung von Prozessen

Wenngleich unterschiedliche Perspektiven und Modellierungssprachen zur Modellierung von Prozessmodellen vorhanden sind, so gilt die Business Process Modeling Notation (BPMN) [Obj11] heute als de-facto Standard für die Prozessmodellierung [KLW09, Rec10, HW14, JLT14, AK15]. Ein Ziel bei der Entwicklung von BPMN war eine einfach verständliche Notation für alle Anwendergruppen, von den Geschäftsprozessentwicklern in der Unternehmensführung bis hin zu den technischen Entwicklern, bereit zu stellen [Obj11]. Es gibt drei unterschiedliche Diagrammtypen in BPMN, wobei das Geschäftsprozessdiagramm (*Business Process Diagram*) der wichtigste Diagrammtyp ist [AK15]. Die Elemente der Modellierungssprache lassen sich in vier Gruppen einteilen: *Flow Objects*, *Connecting Objects*, *Swimlanes* und *Artifacts* [AK15]. Daten können in BPMN mithilfe von sogenannten *Data Objects* modelliert werden, wobei *Data Objects* sowohl digitale Informationen als auch physische Objekte wie Dokumente oder Produkte bedeuten können [Wes12, S. 230]. Mithilfe von *Data Objects*, im Folgenden Datenobjekte oder Datenelemente genannt, lassen sich zudem aktivitätsspezifische Inputs und Outputs modellieren [RSD12, S. 73]. Weiter gibt es das *Data Store* Element, im Folgenden auch Datenspeicher genannt, welches ein AWS repräsentieren kann, aber

auch physische *Speicher* wie z.B. ein Lagerhaus [Wes12, S. 231].

Während bestimmte Elemente zur Modellierung und Einbindung der mit dem Prozess verarbeiteten Daten vorhanden sind, „[..] lassen die in BPMN verfügbaren Bausteine zur Beschreibung von Daten keine redundanzfreie Modellierung eines Datenschemas zu und isolieren die Datenflüsse von den Sequenzflüssen." [FS13, S. 193]. Daten werden nur über ihren Namen im Prozessmodell repräsentiert [Wes12, S. 209]. Ihre interne Struktur kann aber nicht über die Sprachelemente von BPMN definiert werden [Wes12, S. 209].

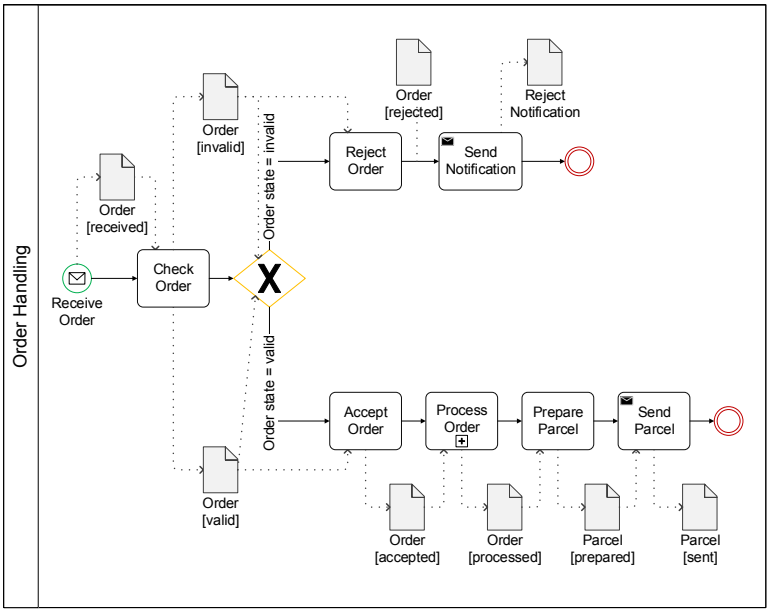


Abbildung 3.5 – Prozessdiagramm mit Datenobjekten (nach [Wes12, S. 231])

Abbildung 3.5 zeigt abschließend beispielhaft einen BPMN Prozess, bei dem Datenobjekte mit modelliert sind. Während die interne Struktur der Datenelemente, z.B. in Form von Entity Realtionship Diagrammen, nicht über BPMN ausgedrückt werden kann, so ist es dennoch möglich z.B. den Status der Datenobjekte und zum Teil auch den Datenfluss zwischen Aktivitäten mit zu modellieren. Der Status wird in eckigen Klammern als Teil des Bezeichners des jeweiligen Datenobjektes vermerkt. Das Datenobjekt *Order [processed]* aus dem Prozessmodell in Abbildung 3.5 zeigt dementsprechend, dass das Datenobjekt *Order* im Status *processed* von der Aktivität *Process Order* erzeugt und von der Aktivität *Prepare Parcel* in diesem Status benötigt wird. Der Datenfluss zwischen zwei Aktivitäten kann ebenfalls modelliert werden, wie

zwischen den beiden Aktivitäten *Reject Order* und *Send Notification* im Prozessmodell in Abbildung 3.5. Auch kann eine Aktivität je nach Verarbeitungsergebnis unterschiedliche Outputs erzeugen, wie bei *Check Order* über die beiden Datenobjekte *Order [valid]* und *Order [invalid]* angedeutet. [Wes12, S. 231ff]

Das kleine Beispiel in Abbildung 3.5 demonstriert, dass Prozessmodelle und Prozessbeschreibungen tatsächlich eine große Menge an Information hinsichtlich des genauen Funktionierens eines Unternehmens enthalten. Inwieweit diese Informationen bei digitalen forensischen Untersuchungen in Unternehmen Verwendung finden können, wird in den Kapiteln 6 und 7 weiter vertieft.

Teil II

Digitale Forensik in Unternehmen

KAPITEL 4

Forensic Readiness und Unternehmensforensik im Überblick

Nachdem sich der vorherige Teil der Arbeit mit den Grundlagen zur digitalen Forensik und zu AWS beschäftigt hat, wird in diesem Kapitel auf die in der Literatur vorhandenen und konkret für Unternehmen entwickelten Maßnahmen und Methoden zur Durchführung und zur Vorbereitung auf digitale forensische Untersuchungen eingegangen. Im folgenden Abschnitt 4.1 werden dazu zunächst Arbeiten zum Thema digitale Forensik in Unternehmen vorgestellt und diskutiert. Im Abschnitt 4.2 werden dann explizit vorbereitende Maßnahmen aus dem Themengebiet *Forensic Readiness*, auch *Digital Forensic Readiness* genannt, näher beleuchtet.

4.1 Status Quo der digitalen Forensik in Unternehmen

Um eine digital forensische Untersuchung durchzuführen, sind insbesondere Methoden und Tools zur Durchführung einer Untersuchung und zum Erstellen von Assoziationen im Sinne der Definition aus Abschnitt 2.2 nötig. Der Status Quo im Bereich der Unternehmensforensik wurde daher im Rahmen einer strukturierten Literaturrecherche analysiert. Die Analyse basiert auf den Daten aus der Literatursuche von Ostermeier [Ost16]. Die Analyse selbst wurde allerdings auf Basis der am Ende des folgenden Abschnitts 4.1.1 vorgestellten Auswahl- und Analysemethodik neu durchgeführt.

4.1.1 Methodik, Datenbanken und Auswahlkriterien

Zur Durchführung der strukturierten Literaturrecherche wurden die in Tabelle 4.1 aufgeführten Suchbegriffe verwendet. Um eine möglichst breite Sicht auf das Themengebiet

Tabelle 4.1 – Suchbegriffe für die Literaturrecherche zum Thema *Enterprise Forensics*

Term 1	Term 2
Enterprise	Forensics
Corporation	Cyber Forensics
Business	Computer Forensics
Company	Digital Forensics
Industry	Incident Response
Venture	Forensic investigation

Tabelle 4.2 – Datenbanken für die Literaturrecherche zum Thema *Enterprise Forensics*

Datenbank	URI (http)	Suchtermformulierung
ACM	dl.acm.org	Advanced Search; Select items from the ACM Guide to Computing Literature where ANY FIELD MATCHES ALL of the following words or phrases: [Term 1] [Term 2]
IEEE	computer.org	Advanced Search; [Term 1] AND [Term 2]; Appearing in Full Text
Springer Link	link.springer.com	[Term 1] "[Term 2]"
Science Direct	sciencedirect.com	Advanced Search; [Term 1] "[Term 2]"
AISel	aisel.aisnet.org	Advanced Search; All Fields; [Term 1] [Term 2]
JDFSL	ojs.jdfsl.org	[Term 1] [Term 2]

zu erhalten, wurden dabei sowohl für Term 1 als auch für Term 2 die verschiedenen bekannten Synonyme verwendet. Mit Term 1 wurde die Unternehmensseite und mit Term 2 die digitale Forensik abgedeckt. Jeder Term 1 wurde zur Suche mit jedem Term 2 kombiniert, sodass am Ende 36 Suchterme wie *Business Forensics* oder *Enterprise Computer Forensics* entstanden sind.

Neben der breiten Auswahl von Suchtermen wurde auch eine große Bandbreite an online Literaturdatenbanken ausgewählt. Darunter sind die Science Direct/Elsevier Datenbank, in der auch die Artikel des Digital Investigation Journals sowie die Proceedings des DFRWS EU und USA enthalten sind, oder die Springer Link Datenbank mit den Proceedings der jährlich stattfindenden IFIP WG 11.9 International Conference on Digital Forensics. Es wurde aber z.B. auch die AISeL Datenbank ausgewählt, um die Literatur aus der Wirtschaftsinformatik oder der Prozessmodellierung mit in die Suche einzubeziehen. Ein abschließender Überblick über alle ausgewählten Datenbanken wird in Tabelle 4.2 gegeben. Tabelle 4.2 enthält zudem genaue Angaben zur Verwendung der 36 Suchtermkombinationen mit der jeweiligen Suchfunktion der jeweiligen Datenbank.

Die Literaturrecherche wurde im Januar 2016 durchgeführt. Da nahezu alle wissenschaftlichen Publikationen im Bereich der digitalen Forensik sofort oder dann in einem zweiten Schritt in englischer Sprache veröffentlicht werden, wurden nur englischsprachige Suchergebnisse berücksichtigt. Für den Zeitpunkt der Veröffentlichung

sowie das Forschungsfeld wurden keine Einschränkungen gemacht. Aufgrund der teilweise über 3.000 Ergebnisse pro Suchterm wurde ein Abbruchkriterium eingeführt: Es mussten mindestens 500 Ergebnisse durchsucht werden. Nach Erreichen des 500. Suchergebnisses wurde die Suche abgebrochen, wenn das letzte relevante Ergebnis mindestens 100 Suchtreffer weiter vorne gefunden wurde. Wenn das Ergebnis 489 z.B. die letzte relevante Publikation war, dann wurde die Suche noch mindestens bis zum 589. Ergebnis fortgesetzt, wenn zwischenzeitlich kein neues Ergebnis gefunden wurde. War das Ergebnis 576 eine weitere relevante Publikation, wäre die Suche bis mindestens Ergebnis Nr. 676 fortgesetzt worden. Bei allen relevanten Publikationen wurde zudem das Literaturverzeichnis auf weitere relevante Publikationen untersucht (Rückwärtssuche).

Die Auswahl der relevanten Publikationen selbst war in mehrere Phasen unterteilt. Zuerst wurden die Ergebnisse auf Basis des Titels aussortiert. Wenn es nicht möglich war eine Entscheidung auf Basis des Titels zu treffen, wurde der Abstract untersucht. Wenn auch das nicht zu einem eindeutigen Ergebnis geführt hat, wurde der gesamte Text der Publikation analysiert und eine Entscheidung getroffen. Die Analyse und Auswahl der Publikationen wurde ohne Zuhilfenahme von Analyseprogrammen, Algorithmen oder ähnlichem rein manuell durchgeführt.

Zur Unterscheidung und Auswahl von relevanten Publikationen wurden folgende Kriterien angelegt:

1. Die Publikation musste entweder ein Paper, ein Journalartikel, ein Buchkapitel oder ein Buch sein. Präsentationen oder Whitepaper wurden generell aussortiert.

2. Der wesentliche Beitrag der Publikationen musste in Unternehmen oder für spezielle Unternehmenssparten nutzbar oder dafür gedacht sein.

3. Publikationen, die lediglich *Forensic Readiness* oder andere vorbereitende Schritte adressieren, wurden ausgeschlossen, da die Literaturrecherche ihren Fokus explizit auf Methoden, Techniken oder Tools zur Durchführung von Untersuchungen oder zum Ziehen von Assoziationen hatte.

4.1.2 Ergebnis der Literaturrecherche

Nach der Durchführung der Literaturrecherche und der Auswahl der Publikationen, wie im vorherigen Abschnitt 4.1.1 beschrieben, konnten 24 relevante Publikationen identifiziert werden. Tabelle 4.3 gibt einen detaillierten Überblick in Zahlen über alle Ergebnisse, die ausgewerteten Ergebnisse sowie die tatsächlich relevanten Ergebnisse und das Ergebnis der Rückwärtssuche. Jede Zahl entspricht der Summe aus den 36 Einzelsummen pro Suchterm. Die Spalte *Ergebnisse* listet die Summe aller gefundenen Publikationen pro Datenbank auf. Zur Bildung der Summe wurden die von der Datenbank pro Suchterm ausgegebene Zahl der Treffer aufsummiert. Die Spalte *Ausgewertete Ergebnisse* listet die tatsächlich ausgewerteten Ergebnisse pro Datenbank

Tabelle 4.3 – Ergebnis der Literaturrecherche zum Thema *Enterprise Forensics* (Summe der Ergebnisse über alle Suchterme)

Datenbank	Ergebnisse	Ausgewertete Ergebnisse	Relevante Ergebnisse
ACM	444	444	3
IEEE	2.994	2.418	4
Springer Link	55.097	3.142	7
Science Direct	24.139	14.033	7
AISeL	3.131	3.131	0
JDFSL	69	69	1
Rückwärtssuche	-	-	2

auf und die Spalte *Relevante Ergebnisse* enthält die Anzahl an tatsächlich relevanten Publikationen pro Datenbank. Die Zahlen in der Spalte *Relevante Ergebnisse* wurden bereits um Duplikate bereinigt.

Nach der finalen Auswahl wurden die gefundenen relevanten Publikationen detailliert untersucht. In den folgenden Abschnitten 4.1.2.1 – 4.1.2.3 wird jede Publikation sowie deren wesentlicher Beitrag kurz vorgestellt. Die Publikationen wurden zudem auf Basis des jeweiligen wesentlichen Beitrags in die drei Gruppen *Untersuchungsprozess*, *Rechtliche Anforderungen* und *Technische Lösungen* eingruppiert.

4.1.2.1 Untersuchungsprozess

Die größte Gruppe der gefundenen und relevanten Publikationen kann beschrieben werden als Bericht darüber, wie eine digitale forensische Untersuchung in Unternehmen durchgeführt werden soll und was es zu beachten gilt. Der wesentliche Inhalt dieser Publikationen ist daher meist eine Art Prozessmodell für digitale forensische Untersuchungen. Für eine detailliertere Einordnung der jeweils betrachteten Untersuchungsschritte wurden die allgemeinen Prozessschritte für digitale forensische Untersuchungen nach Casey [Cas11] verwendet. Diese sind: *Vorbereitung*, *Erhebung/Identifizierung*, *Sicherung*, *Überprüfung und Analyse* und *Präsentation* [Cas11, S. 189f].

Die insgesamt älteste Publikation, die im Rahmen dieser Recherche identifiziert wurde, kann auch in dieser ersten Gruppe *Untersuchungsprozess* eingruppiert werden. Sie wurde von Tipton verfasst und 1993 veröffentlicht [Tip93]. Tipton [Tip93] beschreibt einen Prozess, wie eine Untersuchung um ein Computerverbrechen durchgeführt werden kann. Er beschreibt dabei im Wesentlichen welche und wie (physische) Spuren sowie Informationen aus Befragungen von Beteiligten, z.B. Mitarbeitern, genutzt werden können, um das Verbrechen aufzuklären.

Auch May [May02] gibt, ähnlich den Ausführungen von Tipton [Tip93], Anweisungen, wie eine digitale forensische Untersuchung in einer betrieblichen Umgebung durchgeführt werden kann. Im Gegensatz zum Artikel von Tipton [Tip93] beschreibt May [May02] die Schwierigkeiten und Stolpersteine, die sich z.B. durch festgelegte

Prozesse zur Vorfallsbehandlung ergeben und die Ergebnisse einer digitalen forensischen Untersuchung beeinträchtigen können.

Der Artikel von Wolfe [Wol04] betrachtet nur wenige Punkte bezüglich der Vorbereitung auf digitale forensische Untersuchungen und zur Sicherung digitaler Spuren. Der Artikel beinhaltet allerdings kein vollständiges Prozessmodell oder eine vollständige Beschreibung wie eine digitale forensische Untersuchung durchgeführt werden kann.

Auch Wang und Yang [WY05] beschreiben in ihrem Paper, ähnlich wie Wolfe [Wol04] nur einige wenige Anforderungen und Schritte zur Durchführung digitaler forensischer Untersuchungen in Unternehmen. Sie fordern zudem, dass sich Unternehmen auf digitale forensische Untersuchungen vorbereiten [WY05].

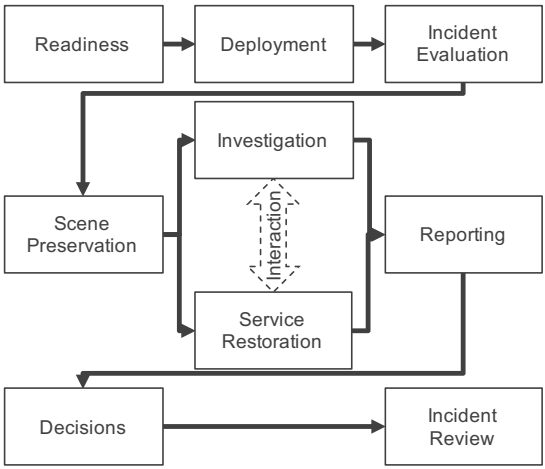


Abbildung 4.1 – Vorgehensmodell für digitale forensische Untersuchungen in Unternehmen (nach [FI06])

Forrester und Irwin [FI06] stellen das in Abbildung 4.1 dargestellte Prozessmodell für digitale forensische Untersuchungen vor. Das hauptsächliche Ziel dieses Modells ist es, eine Entscheidung zwischen einer schnellen Wiederherstellung der Dienste des Unternehmens und einer ordnungsgemäßen digitalen Spurensammlung zu vermeiden, da diese oft in Konflikt zueinander stehen. Zur Lösung des Konfliktes führen sie, wie in Abbildung 4.1 dargestellt eine explizite parallele Ausführung der forensischen Untersuchung im Schritt *Investigation* sowie der Systemwiederherstellung im Schritt *Service Restoration* ein [FI06]. Dadurch kann Forrester und Irwin [FI06] zufolge nach einer initialen Spurensicherung im Schritt *Scene Preservation* direkt mit der Wiederherstellung der Dienste begonnen werden, ohne dass die Aussagekraft der Untersuchung gefährdet ist.

Ähnlich wie Tipton [Tip93] und May [May02] skizzieren auch Haggerty und Taylor [HT06] Prozessschritte für die Durchführung einer digitalen forensischen Untersuchung

in einer betrieblichen Umgebung. Zudem unterstreichen sie die Notwendigkeit für Unternehmen, sich auf digitale forensische Untersuchungen vorzubereiten.

Solms et al. [SLRG06] stellen ein Governance Rahmenwerk für die digitale Forensik in Unternehmen vor. Hierfür definieren sie auf abstrakter Ebene sogenannte Kontrollziele, die dann in 66 detailliertere Kontrollziele verfeinert werden. Das Rahmenwerk soll als Basis zur Implementierung einer digitalen forensischen Governance in Unternehmen dienen. Die Kontrollziele sind dabei sehr detailliert und beschreiben die Hauptziele eines jeden Prozessschrittes einer digitalen forensischen Untersuchung.

Ähnlich zu Standards aus dem IT-Sicherheitsmanagement wie ISO 27001 [ISO13] schlagen Grobler et al. [GLv10b] ein Managementrahmenwerk für die digitale Forensik vor. Dazu beschreiben sie proaktive, reaktive und aktive Maßnahmen für die Vorbereitung auf eine und die Durchführung einer digitalen forensischen Untersuchung. Im Rahmen des Rahmenwerks wird auch ein Prozessmodell vorgestellt, das den Untersuchungsprozess beschreibt.

Leibolt [Lei10] diskutiert die Komplexität betrieblicher Umgebungen und die sich daraus ergebenden Auswirkungen auf digitale forensische Untersuchungen. Dazu beschreibt er wichtige Schritte für eine Untersuchung, weist auf essentielle Punkte für jeden Schritt hin und gibt Beispiele. Weiter nutzt er zur Verdeutlichung seiner Argumentation eine Fallstudie eines erfundenen Vorfalls. Daneben diskutiert er kurz zukünftige Entwicklungen auf dem Gebiet der digitalen Forensik in Unternehmen.

Ähnlich wie die kurzen Publikationen von Wolfe [Wol04] und Wang und Yang [WY05] stellen auch Naqvi et al. [NDP10] eine Liste mit Prozessschritten zur Durchführung einer digitalen forensischen Untersuchung vor. Die Prozessschritte sind bei Naqvi et al. [NDP10] explizit an kleine und mittlere Unternehmen adressiert. Allerdings werden die Schritte nur kurz erklärt. Eine detaillierte Erläuterung der einzelnen Schritte ist in [NDP10] nicht enthalten.

Sims [Sim10] beschreibt die Sicherung von (digitalen) Spuren entlang eines Prozesses für die Identifikation eines Innentäters. Die Publikation ist sehr auf diesen Fall beschränkt, da sie im Wesentlichen nur die Erkennung und Untersuchung von unberechtigter Datenweitergabe durch Innentäter betrachtet.

Blackwell [Bla11] stellt ein Rahmenwerk zur Erfassung und Klassifizierung eines Vorfalls in all seinen Dimensionen und nicht nur auf technischer Ebene vor. Dazu benutzt er das Zachmann Rahmenwerk sowie die Howard-Longstaff Taxonomie und kombiniert diese für sein Rahmenwerk zur Klassifikation von Vorfällen. Das Rahmenwerk soll im Wesentlichen einem Ermittler dabei helfen, alle Auswirkungen eines Vorfalls zu verstehen und ihn dann bei der forensischen Untersuchung unterstützen. Eine erweiterte und leicht im Fokus geänderte Version des Papers [Bla11] wurde erneut von Blackwell [Bla12] veröffentlicht. Die neuere Version [Bla12] beinhaltet eine Evaluation und Demonstration des erweiterten Rahmenwerks zur systematischen Klassifikation und Analyse von Insiderattacken. Zur Evaluation nutzt Blackwell [Bla12] eine Fallstudie.

4.1.2.2 Rechtliche Anforderungen

Die kleinste Gruppe von Publikationen stammt von ein und derselben Autorengruppe und beschäftigt sich mit rechtlichen Anforderungen und Einschränkungen von digitalen forensischen Untersuchungen im betrieblichen Umfeld. Taylor et al. [THG07] skizzieren rechtliche Herausforderungen für die digitale Forensik in Unternehmen, die sich aus der Rechtsprechung und den Gesetzen im vereinigten Königreich ergeben.

Ähnlich wie in [THG07] stellen Taylor et al. in [THG09] rechtliche Anforderungen, die sich ebenfalls aus der Rechtsprechung und den Gesetzen im vereinigten Königreich ergeben, für den speziellen Fall der Untersuchung von E-Mails im Unternehmen vor. Zudem weisen sie auf einige Maßnahmen hin, um mit den rechtlichen Anforderungen umzugehen.

4.1.2.3 Technische Lösungen

Die letzte Gruppe von relevanten Publikationen kann beschrieben werden als technische Lösungen für digitale forensische Untersuchungen in Unternehmen. In diesem Kontext stellen Baek et al. [BKSL08] eine Infrastruktur sowie Maßnahmen zur Erkennung von Informationslecks in Organisationen vor. Die vorgestellten Maßnahmen sind alle auf einem sehr abstrakten Niveau. Die wesentlichen Beiträge sind der Vorschlag einer Totalüberwachung, um Innentäter, die Informationen weitergeben, zu finden und dass, wenn das Informationsleck identifiziert wurde, Spuren gesammelt werden sollen.

Accorsi et al. [AWS11] stellen eine Methode zur Analyse von Geschäftsprozesslogs vor. Ziel dieser Methodik ist das Aufdecken unberechtigter Informationsflüsse durch die Richtlinien, wie z.B. das Aufgabentrennungsprinzip, verletzt werden. Die Methode wird vollständig vorgestellt, inkl. einer Formalisierung der Methodik. Zur praktischen Umsetzung nutzen Accorsi et al. [AWS11] Techniken zum Traversieren von Graphen. Dazu präsentieren sie zudem einen Algorithmus sowie ein kleines Beispiel.

Carlton und Matsumoto [CM11] diskutieren Speichertechnologien für Unternehmen, sowie deren Auswirkungen für die digitale Spurensicherung. Auf Basis einer unstrukturierten Recherche schlagen sie LUN Schnappschüsse als Lösung für die forensische Datenakquise aus Speicherlösungen für Unternehmen vor.

Cohen et al. [CBC11] stellen GRR Rapid Response (GRR) vor. GRR ist ein Werkzeug zur Durchführung von digitalen forensischen Untersuchungen in Unternehmen. Nachdem sie die in Abbildung 4.2 dargestellte Architektur von GRR sowie einige andere Details der Implementierung, wie die Nutzung von Sleuthkit, einer bekannten Open-Source Bibliothek zum Zugriff auf Daten auf der Clientseite beschrieben haben, wird die Anwendbarkeit und der Nutzen von GRR anhand einiger Fallstudien demonstriert und evaluiert. Wie in Abbildung 4.2 erkennbar, wurde GRR für hohe Last und große global verteilte Infrastrukturen designt [CBC11]. In einem weiteren, späteren Artikel [MC13] werden dann von Moser und Cohen hauptsächlich praktische Aspekte, die sich durch den Betrieb von GRR in den großen Umgebungen ergeben, erläutert. Dazu werden die

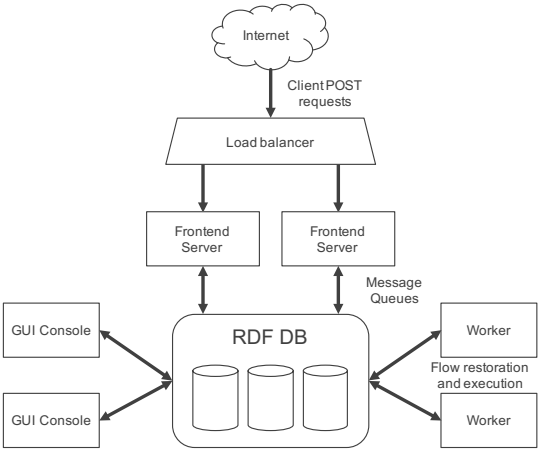


Abbildung 4.2 – GRR Architektur (nach [CBC11])

Möglichkeiten von GRR in ausgewählten realitätsnahen Szenarien demonstriert und die sich dadurch ergebende Limitation diskutiert.

Eine spezielle Methodik, um mit Datenbankservern in digitalen forensischen Untersuchungen umzugehen, wird von Son et al. [SLJ+11] vorgestellt. Sie beschreiben dazu Werkzeuge und besondere Aspekte für jeden Schritt einer Untersuchung, hauptsächlich um Datenbankserver zu finden und die Daten von diesen Systemen zu sichern. Die Funktionsfähigkeit der vorgestellten Schritte wird dann anhand eines Szenarios mit einem Microsoft SQL Server demonstriert.

Ähnlich wie Son et al. [SLJ+11] schlagen auch Flores et al. [FAS12] eine im Wesentlichen technische Methode zur Sammlung, Analyse und zur Präsentation digitaler Spuren von Datenbanken vor. Im Gegensatz zur Methodik von Son et al. [SLJ+11] ist die Methodik von Flores et al. [FAS12] fast ausschließlich rein technischer Natur und zudem auf Fälle von Geldwäsche in Finanzinstitutionen beschränkt.

Schrittwieser et al. [SKW12] diskutieren die digitale forensische Untersuchung von Dokumenten, die durch ein Enterprise Rights Management System geschützt sind. Zudem demonstrieren sie, wie Dokumente von zwei konkreten Enterprise Rights Management Systemen untersucht werden können und zeigen die Unterschiede bei der Untersuchung der beiden Systeme auf. Die Unterschiede ergeben sich im Wesentlichen durch die verschiedene Softwarearchitektur der beiden Implementierungen.

Das sehr spezielle Thema der digitalen forensischen Untersuchung von Industriesteuerungen wird von Sohl et al. [SFH+15] adressiert. Sohl et al. [SFH+15] stellen dabei Unterschiede zu einer regulären digitalen forensischen Untersuchung heraus, die sich vor allem durch die Architektur der Steuerungssysteme sowie der eingesetzten Komponenten ergeben. Zudem diskutieren sie die Nutzung von Werkzeugen und die

Verfügbarkeit und Sicherung von digitalen Spuren von diesen Systemen. Der wesentliche Beitrag ist, dass spezielle Werkzeuge erforderlich sind, die mit der speziellen Umgebung und Architektur der Industriesteuerungen umgehen können.

4.1.3 Status Quo der Unternehmensforensik in der Literatur

Tabelle 4.4 – Zusammenfassung und Evaluation der Publikationen zum Thema *Enterprise Forensics*

		Artefakt								
		Untersuchungsprozess								
	Jahr	Vorbereitung	Identifikation	Sicherung	Analyse	Präsentation	Rechtliche Anforderungen	Technische Lösungen	Evaluation	Digitale Forensik
[Tip93]	1993	◑	◔	◔	○	◔			○	◔
[May02]	2002	◑	◔	◔	◔	◔			○	◔
[Wol04]	2004	◔		◔					○	◔
[WY05]	2005	◑		◔	◔	◔			○	◔
[FI06]	2006	◑	◑	◑	◑	◑			◔	◔
[HT06]	2006	◑	◑	◑	◑	◑			○	◔
[SLRG06]	2006	◕	◕	◕	◕	◕			○	○
[THG07]	2007						◑		○	◔
[BKSL08]	2008							◑	○	◔
[THG09]	2009						◕		○	◔
[GLv10b]	2010	◕	◕	◕	◕	◕			○	◑
[Lei10]	2010	◕	◕	◕	◕	◔			◑	◑
[NDP10]	2010	◔	◔	◔	◔	◔			○	◔
[Sim10]	2010	◔	◔	◔	◔				○	◔
[AWS11]	2011				●			●	○	◕
[Bla11]	2011	◑	◑		◕				◔	◔
[CM11]	2011			◑				◕	○	◔
[CBC11]	2011							●	●	◑
[SLJ+11]	2011	◔	◑	◑	◔			◑	◑	◔
[Bla12]	2012	◑	◑		◑				◑	◔
[FAS12]	2012							●	◔	◑
[SKW12]	2012							◕	◕	◑
[MC13]	2013							●	●	◑
[SFH+15]	2015							◑	◑	◑

Das Ergebnis der Literaturrecherche erlaubt tiefe Einblicke in die unterschiedlichen Facetten der digitalen Forensik in Unternehmen. Die gefundenen Publikationen konn-

ten in drei Gruppen eingeteilt werden. Diese sind: *Untersuchungsprozess*, *Rechtliche Anforderungen* und *Technische Lösungen*. Tabelle 4.4 fasst die Ergebnisse der Evaluation und des Vergleichs der Arbeiten aus dem vorherigen Abschnitt 4.1.2 zusammen und gibt einen abschließenden Überblick. Zur Bewertung der Beitrage der jeweiligen Publikationen wurden Harvey Balls verwendet. Damit wurden die in den jeweiligen Publikationen vorgestellten Methoden, Techniken und Werkzeuge bewertet. Abschließend wurde noch die Adressierung des Themas digitale Forensik als forensische Wissenschaft durch die jeweilige Publikation im Sinne der Ausführungen aus Abschnitt 2.2 analysiert und eingeordnet. Die Ergebnisse dieser Analyse sind in der Spalte *Digitale Forensik* in Tabelle 4.4 dargestellt.

Die Bedeutung des jeweiligen Harvey Balls ergibt sich durch folgendes Schema: Ein leerer Harvey Ball bedeutet, dass der entsprechende Punkt nur kurz erwähnt wurde. Ein viertel voller Harvey Ball heißt, dass der Punkt genannt und ggf. kurz in einem Satz bis zu einem Absatz erläutert wurde. Der halb volle Harvey Ball zeigt, dass ein Aspekt länger beschrieben wurde und ein dreiviertel Harvey Ball, dass der Punkt länger beschrieben und zudem die Herleitung oder ein Beispiel mit erläutert wurden. Ein voller Harvey Ball bedeutet, dass das Kriterium vollumfänglich adressiert wurde. Zellen ohne Harvey Ball zeigen, dass der jeweilige Aspekt gar keine Erwähnung findet.

Da die meisten Arbeiten, die im Rahmen dieser strukturierten Literaturrecherche gefunden wurden, keine vollumfängliche Evaluation als Teil einer rigorosen wissenschaftlichen Vorgehensweise enthalten, ist dieses Kriterium sehr häufig mit einem leeren Harvey Ball in der Spalte *Evaluation* versehen. Weiter haben viele der Arbeiten lediglich jeweils kleine Teile der Prozessschritte oder andere Aspekte beleuchtet. Viele Publikationen sind eher unstrukturierte Berichte von Praktikern, die eine Aufzählung von Aspekten, die es bei der Untersuchung zu beachten gibt, enthalten. Darüber hinaus sind diese Berichte oftmals nicht theoretisch fundiert, was sich ebenfalls anhand der Bewertung in der Spalte *Evaluation* niedergeschlagen hat.

4.2 Forensic Readiness

Die *Forensic Readiness* beschäftigt sich mit Methoden und Maßnahmen zur Vorbereitung von Organisationen auf digitale forensische Untersuchungen. Der Begriff wurde von Tan in [Tan01] eingeführt. Weiter definiert Tan [Tan01] die beiden wesentlichen Ziele der *Forensic Readiness*:

1. Verbesserung der Fähigkeiten einer Umgebung, belastbare bzw. forensisch sichere digitale Spuren zu sammeln.

2. Verringerung der Kosten einer forensischen Untersuchung im Rahmen einer Vorfallsbehandlung.

Um diese Ziele zu erreichen, schlägt Tan [Tan01] verschiedene Maßnahmen vor. Auch andere Autoren wie Yasinsac und Manzano [YM01], Rowlingson [Row04] oder Barske

Tabelle 4.5 – Datenbanken für die Literaturrecherche zum Thema *Forensic Readiness*

Datenbank	URI (http)	Suchtermformulierung
ACM	dl.acm.org	Advanced Search; Select items from the ACM Guide to Computing Literature where ANY FIELD MATCHES ALL of the following words or phrases: Forensic Readiness
IEEE	computer.org	Advanced Search; Forensic AND Readiness; Appearing in Full Text
Springer Link	link.springer.com	Forensic Readiness
Science Direct	sciencedirect.com	Advanced Search; Forensic Readiness
AISeL	aisel.aisnet.org	Advanced Search; All Fields; Forensic Readiness
JDFSL	ojs.jdfsl.org	Forensic Readiness

et al. [BSJ10] schlagen in ihren Arbeiten jeweils Maßnahmen zur Implementierung von *Forensic Readiness* vor. Für diesen Abschnitt wurden die in der Literatur vorhandenen Maßnahmen gesammelt und ein Katalog mit Maßnahmen zur Etablierung von *Forensic Readiness* auf Basis der Literaturrecherche erstellt. Im folgenden Abschnitt 4.2.1 werden die Methodik, die Auswahlkriterien, die durchsuchten Datenbanken sowie die Suchtermformulierung für diese Literaturrecherche beschrieben. Im anschließenden Abschnitt 4.2.2 werden die gefundenen Arbeiten jeweils einzeln vorgestellt. Maßnahmen zur Implementierung von *Forensic Readiness* auf Basis der Literaturrecherche werden schließlich in Abschnitt 4.2.3 beschrieben.

4.2.1 Methodik, Datenbanken und Auswahlkriterien

Da das Themengebiet *Forensic Readiness* bzw. *Digital Forensic Readiness* sehr charakteristisch ist, wurde als Suchterm lediglich *Forensic Readiness* verwendet. Analog zur Literaturrecherche aus dem vorherigen Abschnitt 4.1 sollte aber auch hier eine möglichst breite und vollständige Sicht auf die wissenschaftliche Literatur zum Thema *Forensic Readiness* geworfen werden. Daher wurde ebenfalls die selbe große Bandbreite an online Literaturdatenbanken wie unter Abschnitt 4.1.1 ausgewählt. Ein Überblick über alle Datenbanken sowie genaue Angaben zur Formulierung des Suchterms mit der jeweiligen Suchfunktion pro Datenbank werden in Tabelle 4.5 gegeben.

Da nahezu alle wissenschaftlichen Publikationen im Bereich der digitalen Forensik sofort oder dann in einem zweiten Schritt in englischer Sprache veröffentlicht werden, wurden nur englischsprachige Suchergebnisse berücksichtigt. Für den Zeitpunkt der Veröffentlichung sowie das Forschungsfeld wurden keine Einschränkungen gemacht. Bei allen relevanten Publikationen wurde zudem das Literaturverzeichnis auf weitere relevante Publikationen untersucht (Rückwärtssuche).

Die Auswahl der relevanten Publikationen selbst war in mehrere Phasen unterteilt. Zuerst wurden die Ergebnisse auf Basis des Titels aussortiert. Wenn es nicht möglich war eine Entscheidung auf Basis des Titels zu treffen, wurde der Abstract untersucht.

Wenn auch das nicht zu einem eindeutigen Ergebnis geführt hat, wurde der gesamte Text der Publikation analysiert und eine Entscheidung getroffen. Die Analyse und Auswahl der Publikationen wurde wie bei der Literaturrecherche aus dem vorherigen Abschnitt 4.1 ohne Zuhilfenahme von Analyseprogrammen, Algorithmen oder ähnlichem rein manuell durchgeführt.

Zur Unterscheidung und Auswahl von relevanten Publikationen wurden folgende Kriterien verwendet:

1. Die Publikation ist entweder ein Paper, ein Journalartikel oder ein Buchkapitel. Präsentationen oder Whitepaper wurden sofort aussortiert.

2. Die Arbeit ist dem Themengebiet *Forensic Readiness* bzw. *Digital Forensic Readiness* zuzuordnen.

3. Die Arbeit beschreibt Methoden oder Maßnahmen zur Implementierung von *Forensic Readiness* in Unternehmen oder Organisationen. Arbeiten, die spezielle Implementierungen von *Forensic Readiness* z.B. für den Linux Kernel [LL14] oder W-Lan Netzwerke [NV09] beschreiben, wurden aussortiert.

4.2.2 Ergebnis der Literaturrecherche

Tabelle 4.6 – Ergebnis der Literaturrecherche zum Thema *Forensic Readiness*

Datenbank	Ergebnisse	Relevante Ergebnisse
ACM	49	5
IEEE	78	4
Springer Link	1.151	6
Science Direct	1.027	5
AISeL	48	0
JDFSL	2	0
Rückwärtssuche	-	7

Die Literaturrecherche wurde im März 2016 durchgeführt und es konnten ohne Duplikate insgesamt 23 Arbeiten identifiziert werden. Tabelle 4.6 zeigt die Ergebnisse der Suche pro Datenbank sowie die jeweils relevanten Publikationen.

Die hohe Zahl an Suchergebnissen im Vergleich zu den ausgewählten Arbeiten bei Springer Link und Science Direct ist darauf zurückzuführen, dass es keine Einschränkung hinsichtlich des Forschungsgebietes gegeben hat. Dementsprechend sind in der Anzahl der Ergebnisse auch Treffer aus anderen Wissenschaften wie der Psychologie, der Medizin, der Rechtswissenschaft oder den Sozialwissenschaften enthalten. Bei der Suche in Science Direct konnten aufgrund einer technischen Limitierung der Datenbank die letzten 27 der 1.027 Treffer nicht mehr durchsucht werden. Aus diesem Grund wurde die Suche in einem zweiten Durchlauf verfeinert und auf das Gebiet *Computer*

Science eingegrenzt, um zu überprüfen, ob wenigstens alle Publikationen aus diesem Gebiet ausgewählt wurden. Es konnte unter den 238 Suchtreffern aber keine weitere Arbeit identifiziert werden.

Im folgenden Abschnitt 4.2.2.1 werden die identifizierten Arbeiten im Überblick dargestellt und die Ergebnisse zusammengefasst. Im anschließenden Abschnitt 4.2.2.2 werden die Arbeiten dann jeweils einzeln vorgestellt.

4.2.2.1 Status Quo der Forensic Readiness in der Literatur

Die in den ausgewählten Arbeiten vorgestellten Maßnahmen zur Implementierung von *Forensic Readiness* wurden zusammengefasst und entsprechend den drei Dimensionen *technisch*, *organisatorisch* und *personell* zugeordnet. Tabelle 4.7 stellt alle Arbeiten in chronologischer Reihenfolge dar. Analog zu den Ergebnissen aus dem vorherigen Abschnitt 4.1 zeigt Tabelle 4.7 die in der jeweiligen Arbeit angesprochenen bzw. beschriebenen Maßnahmen mithilfe eines Harvey Balls an. Wenn kein Harvey Ball vorhanden ist, so bedeutet dies, dass die jeweilige Maßnahme nicht erwähnt wurde. Ein leerer Harvey Ball zeigt, dass die zugehörige Maßnahme erwähnt, aber nicht näher beschrieben wurde. Ein viertel Harvey Ball bedeutet, dass die Maßnahme kurz beschrieben wurde. Wurde die Maßnahme ausführlich erklärt, so ist dies mit einem halb vollen Harvey Ball dargestellt. Ein dreiviertel Harvey Ball heißt, dass die Maßnahme ausführlich erläutert und erste Hinweise zur konkreten Implementierung gegeben werden. Ein voller Harvey Ball bedeutet, dass die Maßnahme in der jeweiligen Arbeit ausführlich und mit konkreten Anweisungen zur Implementierung erläutert wird.

Tabelle 4.7 enthält zudem die Spalte *Evaluation*. Analog zur Literaturrecherche im Abschnitt 4.1 wurde auch hier ein wissenschaftliches Vorgehen und die verwendete Methodik mit in die Recherche einbezogen. Wie in der Spalte *Evaluation* in Tabelle 4.7 durch den leeren Harvey Ball für die meisten Arbeiten ersichtlich, wurde oft keine wissenschaftliche Methode verwendet. Häufig handelt es sich, wie auch schon bei den Arbeiten zur digitalen Forensik in Unternehmen aus Abschnitt 4.1 um unstrukturierte Arbeiten mit *Wünschen* zur *Forensic Readiness*. Nur in wenigen Arbeiten ist eine Evaluation der Maßnahmen enthalten, wie z.B. in [EAML15] in Form von Experteninterviews.

4.2.2.2 Forensic Readiness Literaturüberblick

Tan [Tan01] definiert zunächst die *Forensic Readiness* sowie deren Ziele. Demnach beschäftigt sich die *Forensic Readiness* mit der Vorbereitung auf digitale forensische Untersuchungen. Durch eine Vorbereitung werden besser verwertbare und wertvollere Spuren im Sinne der forensischen Sicherheit sowie die Senkung der Kosten für digitale forensische Untersuchungen erwartet [Tan01]. Anschließend beschreibt er Log Mechanismen und deren Implementierung sehr ausführlich. Zudem stellt er Techniken zur digitalen Spurensicherung für verschiedene Systeme sowie Maßnahmen zur Handhabung

Tabelle 4.7 – Zusammenfassung und Evaluation der Publikationen zum Thema *Forensic Readiness*

		technisch				organisatorisch						personell		
	Jahr	Log Management	Absicherung von Spuren	Identitätsmanagement	Digitale Spurensicherung	Identifikation kritischer Systeme	Regeln zur Spurenhandhabung	Vorgehensmodell	Datenschutzregelungen	Systemdokumentation	Unternehmenskommunikation	Response Team	Schulungen	Evaluation
[Tan01]	2001	●	◔				◔							○
[YM01]	2001	◕	◔	◑				◑	◔	◔		◑	◑	○
[WWW03]	2003	◔					◔	◔			◑	◔		○
[Row04]	2004	◕	◔	◔		◕	◑	◔		◕	◔	◕	◔	○
[BC05]	2005	◔			◔	○	◔	◔				◔	◔	◑
[Cas05]	2005	◔				◔					◔		◔	◔
[SLRG06]	2006	◔		◔	◔	◔	◔					◑	◔	○
[EPFT07]	2007					◔	◔						◔	○
[GL07]	2007	◔	◔	◔		◔	○	◔				◔	◔	○
[TEPF07]	2007					◔								○
[RV09]	2009	◔				◔		◔		◔		◔	◔	○
[BSJ10]	2010	◔			◑	◔			◔				◔	○
[GLv10a]	2010	◔			◑		◔	◔				◔	◑	○
[GLv10b]	2010	◔			◔		◔	◔				◔	◔	○
[PIP10]	2010	○				○	○					○	○	○
[PK10]	2010		◔										◔	○
[AWJT11]	2011	○												●
[MGL11]	2011					◔	◔	○					○	◔
[NLZ+12]	2012	○			◔	◔	◔	◔				◔	◔	○
[Ker13]	2013				◔		◔	◔	◔			◔	◔	◕
[RV13]	2013	◑	◑			◔	○	◑		◔		◑	◔	●
[VV13]	2013	◑	◑		◔	◑	◑	◔		◔			◔	◔
[EAML15]	2015	◔	◔	◔	◑		◔	◔				◔	◑	●

von digitalen Spuren vor. Dabei geht er sowohl auf die physische Handhabung von Spurenträgern als auch auf digitale Spurensicherungsmaßnahmen ein.

Yasinsac und Manzano [YM01] definieren ebenfalls verschiedene Richtlinien, die Unternehmen etablieren sollen, um im Falle einer digitalen forensischen Untersuchung entsprechend handeln zu können. Yasinsac und Manzano [YM01] gehen dabei auf personelle, technische wie auch organisatorische Maßnahmen ein und fordern z.B. die Einrichtung eines Response Teams sowie die Etablierung einer Vorgehensweise für

Untersuchungen. Weiter werden auch technische Maßnahmen wie das Logging oder die Notwendigkeit eines Identitätsmanagements angesprochen, um anonyme und nicht explizit autorisierte Handlungen im System auszuschließen [YM01].

In [WWW03] werden Maßnahmen, die zum Erfolg einer forensischen Untersuchung beitragen, auf einer sehr abstrakten Ebene beschrieben. Das Ziel von Wolfe-Wilson und Wolfe [WWW03] ist es, Handlungsanweisungen für die Leitungsebene in Unternehmen bereit zu stellen und die Auswirkung von digitalen forensischen Untersuchungen auf die Sicherheitsstrategie und -richtlinien zu beleuchten.

Im Vergleich zu den vorherigen Arbeiten beschreibt Rowlingson [Row04] mit seinen zehn Schritten zur *Forensic Readiness* sehr ausführlich was ein Unternehmen tun muss, um auf digitale forensische Untersuchungen vorbereitet zu sein. Neben den bereits in den vorherigen Arbeiten genannten Maßnahmen geht er dabei vor allem auf die gezielte Auswahl und Vorbereitung bestimmter Systeme ein. Das Risiko und die potentiellen Auswirkungen von maliziösen Handlungen in den Systemen auf den Geschäftsbetrieb stellen dabei die beiden wesentlichen Kriterien zur Identifikation solcher kritischer Systeme, von denen potentiell digitale Spuren benötigt werden, dar [Row04]. Rowlingson [Row04] gibt auch Anweisungen hinsichtlich der Entscheidung wann eine digitale forensische Untersuchung gestartet werden soll. Außerdem wird nach einer Untersuchung ein explizites *Lernen* der Organisation aus einem Fall gefordert [Row04].

Größtenteils auf Basis von [Row04] nennen Beebe und Clark [BC05] anhand eines Rahmenwerkes für einen Untersuchungsprozess verschiedene vorbereitende Maßnahmen. Außerdem geht die Arbeit auf die Nutzung bzw. konkrete Implementierungen der vorbereitenden Maßnahmen im Rahmen von zwei Fallstudien ein.

Anhand der Erkenntnisse aus der Untersuchung eines konkreten Falles präsentiert Casey in [Cas05] verschiedene Maßnahmen zur Vorbereitung auf digitale forensische Untersuchungen. Dabei spricht er jeweils die Maßnahme kurz an und beschreibt dann wie diese die Aufklärung des konkreten Falles positiv beeinflussen hätte können.

Solms et al. [SLRG06] stellen im Kontext eines Rahmenwerks zur Steuerung der digitalen Forensik Maßnahmen bzw. Kontrollziele für die Vorbereitung auf digitale forensische Untersuchungen vor. Die Kontrollziele zur Vorbereitung auf forensische Untersuchungen sind aber im Wesentlichen eine Zusammenfassung der in [Row04] vorgeschlagenen Maßnahmen.

Endicott-Popovsky et al. [EPFT07] zeigen, geleitet von der sogenannten 4R Strategie, verschiedene Phasen zur Erreichung von *Forensic Readiness* in Netzwerken auf. Bei der 4R Strategie handelt es sich um eine Erweiterung der drei Strategien *Resistance*, *Recognition* und *Recovery*, zur Absicherung eines Netzwerks um die *Redress* Strategie. Die *Redress* Strategie soll dabei im Wesentlichen die Täter rechtssicher identifizieren. Zur Implementierung von *Forensic Readiness* präsentieren Endicott-Popovsky et al. [EPFT07] des Weiteren verschiedene Modelle.

Forensic Readiness als Teil des Informationssicherheitsmanagements wird in [GL07]

betrachtet. Grobler und Louwrens [GL07] vergleichen dazu die beiden Themengebiete und stellen dann Maßnahmen zur Etablierung von *Forensic Readiness* vor. Die Maßnahmen basieren wiederum größtenteils auf den von Rowlingson [Row04] vorgestellten zehn Schritten.

In [TEPF07] stellen Taylor et al. die Einführung von *Forensic Readiness* auf Basis von Sicherheitsrichtlinien vor. Dabei soll zur Vorbereitung auf forensische Untersuchungen spezifiziert werden, welche forensischen Fähigkeiten ein System haben muss, um potentiell eintretende Ereignisse und die dadurch entstehenden relevanten Spuren handhaben bzw. sichern zu können [TEPF07].

Speziell für Fälle bei denen der Datenschutz verletzt wurde, stellen Reddy und Venter [RV09] Maßnahmen zur Implementierung von *Forensic Readiness* vor. Dabei diskutieren sie sowohl technische wie nicht-technische Maßnahmen, die für diese speziellen Fälle relevant sind. Eine zentrale Rolle spielen dabei die Geschäftsprozesse, die mit diesen Daten operieren. Maßnahmen wie das Logging sollten an den Geschäftsprozessen ausgerichtet und die, die Prozesse ausführenden Anwendungssysteme dementsprechend überwacht werden [RV09].

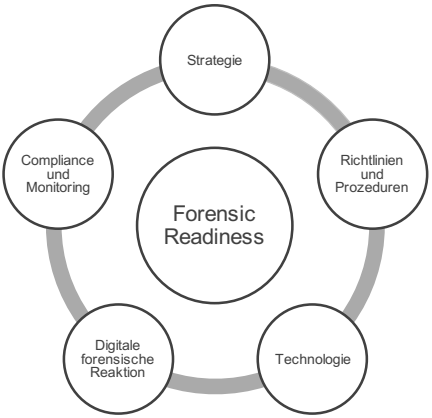


Abbildung 4.3 – *Forensic Readiness* Bereiche (nach [BSJ10])

Mit dem Fokus auf kleine und mittlere Unternehmen stellen Barske et al. [BSJ10] Maßnahmen zur Implementierung von *Forensic Readiness* vor. Dabei bedienen sich Barske et al. [BSJ10] größtenteils der Maßnahmen und Konzepte aus bereits vorhandenen Werken im Bereich *Forensic Readiness*, wie z.B. [Tan01] oder [Row04] und zeigen diese für den Kontext der kleinen und mittleren Unternehmen auf. Dabei heben sie auch hervor, dass es gerade für kleine Unternehmen wichtig ist, erfolgreich auf Vorfälle reagieren zu können, da sie im Gegensatz zu großen Unternehmen Verluste weniger gut verkraften können [BSJ10]. Weiter gruppieren sie die Maßnahmen aus dem Bereich der *Forensic Readiness* in die in Abbildung 4.3 dargestellten Bereiche ein. Anschließend

beschreiben sie die einzelnen Bereiche detailliert und stellen für jeden Bereich speziell Maßnahmen vor [BSJ10].

Grobler et al. [GLv10a] stellen mit dem sogenannten ProDF Rahmenwerk eine Sammlung an Maßnahmen zur Implementierung von *Forensic Readiness* vor. Dabei legen sie Ziele fest und diskutieren anschließend verschiedene Maßnahmen, um diese Ziele zu erreichen. Die Maßnahmen wiederum sind anhand von Dimensionen, z.B. Prozesse, Menschen oder Technologie, gruppiert [GLv10a].

In [GLv10b] betrachten Grobler et al. das ProDF Rahmenwerk aus [GLv10a] im größeren Kontext eines Gesamtrahmenwerks. Das Gesamtrahmenwerk enthält neben vorbereitenden Maßnahmen aus dem ProDF Rahmenwerk auch reaktive Maßnahmen für forensische Untersuchungen [GLv10b]. Dementsprechend stellt [GLv10b] hinsichtlich der Maßnahmen zur Implementierung von *Forensic Readiness* nur eine verkürzte Version von [GLv10a] dar.

Pangalos et al. [PIP10] motivieren die Implementierung von *Forensic Readiness* und vergleichen das Thema mit verschiedenen anderen Themen, wie dem Auditing oder dem Informationssicherheitsmanagement. Die vorgeschlagenen Maßnahmen zur Implementierung von *Forensic Readiness* sind aber im Wesentlichen eine sehr verkürzte Version der zehn Schritte von Rowlingson [Row04].

Ähnlich wie in [PIP10] motivieren Pangalos und Katos [PK10] die Notwendigkeit von *Forensic Readiness*. Sie diskutieren diesen Aspekt im Rahmen der Erweiterung und Herausforderungen, die über das Informationssicherheitsmanagement hinaus gehen, wobei nur sehr wenige konkrete Maßnahmen zur Erreichung von *Forensic Readiness* vorgestellt werden [PK10].

In [AWJT11] wird eine Literaturrecherche zu den Prozessen in der digitalen Forensik vorgestellt. Das Ergebnis der Literaturrecherche ist, dass lediglich die Arbeit von Grobler et al. [GLv10b] einen proaktiven Prozess enthält. Die Arbeit von Alharbi et al. [AWJT11] enthält daher auch nur eine sehr kleine Zahl an Hinweisen auf die Implementierung von *Forensic Readiness*, wobei diese aus [GLv10b] stammen.

Mouhtaropoulos und Grobler [MGL11] beleuchten verschiedene staatliche und akademische Initiativen zur Etablierung von *Forensic Readiness*. Aufgrund der vielen unterschiedlichen Initiativen fordern sie eine Standardisierung innerhalb des Bereichs *Forensic Readiness* [MGL11]. Zudem haben nach Mouhtaropoulos und Grobler [MGL11] insbesondere Unternehmen noch einen erheblichen Nachholbedarf im Bereich *Forensic Readiness*. Zur Implementierung von *Forensic Readiness* werden allerdings nur wenige abstrakte Empfehlungen gegeben.

Nnoli et al. [NLZ+12] beschreiben ein Governance Rahmenwerk für die digitale Forensik. Dabei verfeinern und erweitern sie die Maßnahmen aus [Row04] und integrieren diese in ihr Governance Rahmenwerk [NLZ+12]. Nnoli et al. [NLZ+12] erhoffen sich durch die Integration von Maßnahmen in ein Lenkungs- und Steuerungsrahmenwerk eine effektivere Umsetzung von *Forensic Readiness* Maßnahmen in Unternehmen, im Gegensatz zur alleinigen Integration von *Forensic Readiness*.

Im Rahmen der Vorstellung eines Reifegradmodells beschreibt Kerrigan [Ker13] verschiedene Maßnahmen zur Implementierung von *Forensic Readiness*. Mithilfe des vorgestellten Reifegradmodells können die digitalen forensischen Fähigkeiten einer Organisation gemessen werden, wobei er betont, dass nicht zwingend die höchste Stufe angestrebt werden sollte, da diese einen erheblichen finanziellen Mehraufwand bedeutet [Ker13].

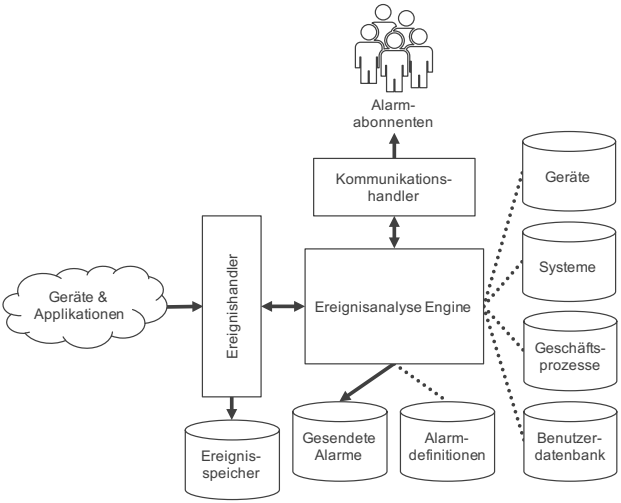


Abbildung 4.4 – Ereignisanalysemodul des *Forensic Readiness* Managementsystems (nach [RV13])

Motiviert von der Komplexität von *Forensic Readiness* Initiativen in großen Unternehmen stellen Reddy und Venter [RV13] ein *Forensic Readiness* Managementsystem vor, um *Forensic Readiness* effektiv managen zu können. Basierend unter anderem auf den oben vorgestellten Arbeiten von Tan [Tan01], Yasinsac und Manzano [YM01] sowie Rowlingson [Row04] definieren Reddy und Venter [RV13] zunächst Anforderungen an das Managementsystem. Diese Anforderungen sind daher zu einem Großteil Maßnahmen zur Erreichung von *Forensic Readiness*. Im Anschluss an die Definition der Anforderungen wird eine darauf aufbauende Softwarearchitektur und ein implementierter Prototyp vorgestellt und evaluiert [RV13]. Abbildung 4.4 zeigt die Komponenten zur Behandlung von Ereignissen. Reddy und Venter [RV13] begründen dabei auch eine Verbindung des Vorfallsmanagements mit den Geschäftsprozessen, da bei einem Vorfall, der einen Geschäftsprozess betrifft, auch der jeweilige verantwortliche Manager mit hinzugezogen werden soll [RV13].

Zur Implementierung von *Forensic Readiness* stellen Valjarevic und Venter [VV13] ein Prozessmodell vor. Die einzelnen Prozessschritte sind dabei in die drei Gruppen Planung, Implementierung und Kontrolle eingeteilt. Im Wesentlichen entsprechen die

von Valjarevic und Venter [VV13] vorgestellten Prozesse und die darin enthaltenen Maßnahmen den Maßnahmen aus den bereits oben vorgestellten Arbeiten [Tan01], [YM01], [WWW03] und [Row04].

Ein sehr ausführliches Rahmenwerk mit Zielen für die Implementierung von *Forensic Readiness* wird von Elyas et al. [EAML15] diskutiert und auf Basis von Experteninterviews evaluiert. Das Rahmenwerk kann zur Implementierung und zur Kontrolle und Verbesserung der *Forensic Readiness* von Unternehmen verwendet werden [EAML15]. Dazu enthält es detaillierte Beschreibungen einzelner Fähigkeiten bzw. Maßnahmen, die zur Erreichung bzw. zum Erhalt der *Forensic Readiness* notwendig sind [EAML15].

4.2.3 Maßnahmen zur Implementierung von Forensic Readiness

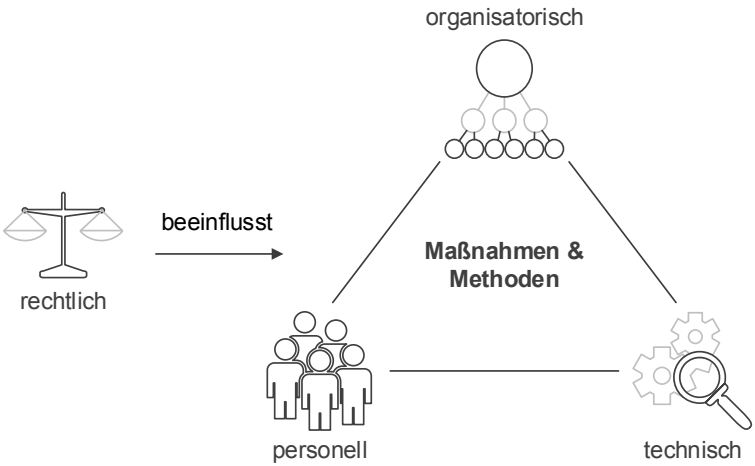


Abbildung 4.5 – Dimensionen der *Forensic Readiness* Maßnahmen

In allen Arbeiten, die im vorherigen Abschnitt 4.2.2.2 vorgestellt wurden sind mehr oder weniger Maßnahmen zur Umsetzung und Kontrolle von *Forensic Readiness* in Unternehmen enthalten. Im Folgenden werden die einzeln vorgestellten Maßnahmen nun zusammengefasst und beschrieben. Die Maßnahmen wurden, anders als in Abbildung 4.3 dargestellt bzw. in [BSJ10] vorgeschlagen, im Sinne der Definition soziotechnischer Systeme [ÖBF+10] anhand der drei Dimensionen *organisatorisch*, *personell* und *technisch* eingruppiert. Abbildung 4.5 zeigt diese drei Dimensionen. Weiter stellt Abbildung 4.5 die bestehenden gegenseitigen Abhängigkeiten zwischen den Maßnahmen der *Forensic Readiness* dar [EAML15]. Die *rechtliche* Dimension ist nicht Teil der Maßnahmen der *Forensic Readiness*, sondern beeinflusst diese, z.B. in Form von Regeln und Gesetzen zur forensisch sicheren Spurensammlung [BSJ10, NLZ+12].

4.2.3.1 Technische Maßnahmen

Die technischen Maßnahmen bezeichnen alle technisch, in Form von Hard- und Software zu implementierenden Maßnahmen.

Log Management

Das Log Management, auch als präventives Sammeln von digitalen Spuren, Monitoring oder Auditing bezeichnet, wird von fast allen Autoren der unter Abschnitt 4.2.2.2 vorgestellten Arbeiten mindestens genannt. Im Rahmen der Vorbereitung auf forensische Untersuchungen sollen dabei insbesondere kritische Ereignisse in den Systemen mitgeschrieben werden, die zum Erkennen eines Verbrechens oder der Täter nützlich sind [YM01, Row04, RV09]. Nützlich bzw. wichtig sind in der Regel Ereignisse wie z.B. die Authentifizierung und Autorisierung von Benutzern, um zu beantworten, wer sich wann wo an- oder abgemeldet hat [YM01].

Die Auswahl der mitzuschneidenden Ereignisse bzw. Systeme für das Logging ist allerdings nötig, da aufgrund von Limitierungen hinsichtlich der Ressourcen, insbesondere von Personen, dem notwendigen Speicherplatz, der Netzwerkbandbreite und der Prozessorleistung, nicht alles mitgeschnitten werden kann [Tan01, WWW03, Row04]. Zur Auswahl kann z.B. eine Kosten-Nutzen Analyse durchgeführt werden, wobei zwischen dem Nutzen der digitalen Spuren und den Kosten um sie zu erheben abgewogen wird [Row04]. Ein limitierender oder fordernder Faktor können aber auch die jeweils anzuwendenden Gesetze sein, da diese z.B. Aufbewahrungsfristen definieren können [Row04].

Tan [Tan01] definiert zudem konkrete Anforderungen an ein Log Management System. So fordert er die zentrale Sammlung der Logs, um bei der Kompromitierung eines einzelnen Systems noch Referenzlogs im zentralen Repository gespeichert zu haben, deren Integrität noch nicht verletzt wurde. Des Weiteren ist ein zentrales System leichter abzusichern. Um die Logs zentral vorzuhalten, ist zudem ein einheitliches Format notwendig und die Uhrzeiten auf den zu loggenden Systemen müssen synchron sein.

Absicherung von digitalen Spuren

Die Einführung und Etablierung von Maßnahmen zur Spurensicherung betrifft zum einen die Schaffung von Möglichkeiten zur manipulationssicheren Aufbewahrung von Spuren und zum anderen die sichere Übertragung von digitalen Spuren [Tan01]. Bei der Übertragung von digitalen Spuren sind diese kryptographisch zu sichern, z.B. über Hashes, und sowohl Empfänger als auch der Sender über digitale Signaturen zu authentisieren [Tan01, VV13]. Im Rahmen der *Forensic Readiness* sind daher solche Methoden entsprechend einzuführen.

Zur Absicherung der Integrität von digitalen Spuren für die Aufbewahrung, können diese ebenfalls mithilfe kryptographischer Maßnahmen gesichert werden [YM01]. Wie auch für die Übertragung können von Zeitstempeldiensten signierte Hashes verwendet

werden [Tan01, Row04, RV13]. Eine weitere Möglichkeit zur technisch sicheren Aufbewahrung sind WORM (write once read many) Medien [Tan01, Row04], die sich nur einmal beschreiben lassen und technisch die Wiederverwendung oder unbemerkte Manipulationen der darauf gesicherten Daten ausschließen. Die Auswahl und Sicherstellung der Benutzbarkeit dieser Dienste oder Medien sind wiederum Teil der *Forensic Readiness*. Sind keine Möglichkeiten oder nicht die Richtigen zur Sicherung der Integrität digitaler Spuren bei einer digitalen forensischen Untersuchung vorhanden, so riskiert man unter Umständen die Zulässigkeit der Spuren und damit seine Position in einem Rechtsstreit [BSJ10].

Identitätsmanagement

Das Identitätsmanagement ist wichtig, um bei einer digitalen forensischen Untersuchung zu bestimmen, wer Zugang zu fragwürdigen Systemen hatte oder für die Entstehung von bestimmten Daten verantwortlich ist [Row04, EAML15]. Dementsprechend ist das Identitätsmanagement und die Einführung sicherer Autorisierungs- und Authentifizierungsverfahren obligatorisch für die Vorbereitung auf digitale forensische Untersuchungen [YM01]. Über das Identitätsmanagement muss sichergestellt werden, dass nur valide Nutzer Zugang zum System haben und keine anonymen Aktivitäten im System möglich sind [YM01].

Wurden im Rahmen der *Forensic Readiness* entsprechend sichere Maßnahmen zur Authentifizierung und Autorisierung implementiert und alle sonstigen anonymen Aktivitäten unterbunden, so kann eine digitale forensische Untersuchung damit beginnen, die Personen zu identifizieren, die aufgrund ihrer Rechte im System Zugang zu den fraglichen Dateien hatten [YM01].

Digitale Spurensicherung

Neben Maßnahmen zur Absicherung der Spuren müssen auch Maßnahmen für die forensische Sicherung digitaler Spuren im Rahmen der *Forensic Readiness* etabliert werden [Row04, BC05, BSJ10, GLv10a]. Hierfür müssen alle Hard- und Softwarekomponenten inkl. der Netzwerkkomponenten auf forensische Untersuchungen und die potentielle Spurenextraktion aus diesen Systemen vorbereitet werden [GLv10a]. Dazu sind in erster Linie technische Möglichkeiten in Form von forensischen Werkzeugen wie GRR oder EnCase erforderlich und müssen entsprechend implementiert werden [BC05, GLv10a, EAML15]. Weiter muss geklärt werden, ob und wie die digitalen Spuren ohne Unterbrechung von Geschäftsprozessen gesammelt oder extrahiert werden können [Row04].

Neben Softwaretools in Form der forensischen Werkzeuge muss unter Umständen auch spezielle Hardware wie Writeblocker angeschafft werden, um ein auf die Unternehmensinfrastruktur angepasstes forensisches Labor auszustatten [GLv10a].

4.2.3.2 Organisatorische Maßnahmen

Unter organisatorischen Maßnahmen werden alle im Rahmen der *Forensic Readiness* zu etablierenden Unternehmensrichtlinien, Prozesse und Handlungsanweisungen zusammengefasst.

Identifikation kritischer Systeme

Ein kritisches System ist ein System, auf dem potentiell ein höheres Risiko für kriminelle Handlungen besteht oder das einen großen Einfluss auf den Geschäftsbetrieb hat [Row04, VV13]. Die Identifikation der kritischen Systeme ist aus mehrerlei Hinsicht notwendig.

Zum einen kann nicht alles und jedes System mitgeloggt werden, wie unter Abschnitt 4.2.3.1 bereits erläutert. Demnach dient die Identifikation als Basis für die Auswahl der in das Log Management einzubindenden Systeme [Row04, RV09]. Darüber hinaus dient die Auswahl aber auch einer besonderen Vorbereitung dieser Systeme auf forensische Untersuchungen und der Priorisierung bei einer digitalen forensischen Untersuchung [Cas05]. So können die wertvollsten digitalen Anlagen bevorzugt behandelt und gesichert werden [Cas05].

Potentielle Fragen für die Identifizierung eines kritischen Systems nach [Row04] sind:

- Wo ist das Geld?
- Welche Systeme sind systemkritisch?
- Wo ist ein hohes Maß an Vertrauen in die mit dem System arbeitenden Personen notwendig?

Zur tatsächlichen Auswahl von kritischen Systemen muss dann eine Risikoanalyse und Einschätzung auf Basis der zu erwartenden Verluste und der bestehenden Angriffsmöglichkeiten, wie z.B. Betrug, Datendiebstahl oder Sabotage durchgeführt werden [TEPF07, NLZ+12, VV13].

Regeln zur Spurenhandhabung

Neben den in Abschnitt 4.2.3.1 vorgestellten technischen Maßnahmen zur Absicherung der digitalen Spuren ist es vor allem für die Beweissicherungskette (continuity of evidence (UK) oder chain of custody (US) [Row04]) wichtig, dass mittels eines Protokolls ab der tatsächlichen Sicherung der digitalen Spuren bis nach dem Gerichtsprozess festgehalten wird, wer wann zu welchem Zweck Zugang zu den digitalen Spuren hatte [Tan01, Row04].

Diese Beweissicherungskette und der eingeschränkte Zugang zu den Spuren muss auch über einen Transport der digitalen Spuren hinweg eingehalten werden, weshalb diese z.B. nur mittels Kurier versandt werden dürfen [Tan01]. Auch bei der Lagerung

digitaler Spuren muss der Zugang entsprechend protokolliert und eingeschränkt werden [Tan01, Row04].

Im Rahmen einer *Forensic Readiness* Initiative müssen daher entsprechende Handlungsanweisungen und Formulare erstellt werden.

Vorgehensmodell

Neben der Spurenhandhabung ist auch ein festgelegtes Vorgehensmodell oder ein Prozess zur Gewährleistung einer strukturierten Durchführung einer digitalen forensischen Untersuchung notwendig [YM01]. Insbesondere, da die digitale forensische Untersuchung im Konflikt mit anderen im Rahmen eines Sicherheitsvorfalls durchzuführenden Aktivitäten wie der Wiederherstellung wichtiger Systeme stehen kann [Row04]. Ein im Rahmen der *Forensic Readiness* eingeführter und getesteter Prozess kann wichtige Spuren vor der Zerstörung durch eine voreilige Wiederherstellung schützen und gleichzeitig die Kosten einer Untersuchung und den Zielkonflikt zwischen der schnellen Wiederherstellung und der rechtssicheren Spurensammlung minimieren [Row04].

Datenschutzregelungen

Der Datenschutz und die Gesetze zum Schutz der Privatsphäre von Angestellten oder anderen im Unternehmen und mit den Systemen des Unternehmens interagierenden Personen können unter Umständen eine digitale forensische Untersuchung einschränken oder gar blockieren [YM01, BSJ10]. Aus diesem Grund sind Richtlinien notwendig und im Rahmen der *Forensic Readiness* einzuführen, um die Privatsphäre der Mitarbeiter entsprechend einzuschränken, damit im Falle einer Untersuchung auf jede notwendige Datei zugegriffen werden darf [YM01, BSJ10].

Systemdokumentation

Die Systemdokumentation ist eine wichtige Quelle, um zu verstehen, wo Spuren entstehen und welche Spuren es geben sollte [YM01, Row04]. Auch kann es von der Systemdokumentation abhängen, ob potentielle Spuren aus speziellen Hard- und Softwaresystemen überhaupt extrahiert und verarbeitet werden können [YM01]. Aus diesem Grund ist eine schriftliche Dokumentation der Systeme für die Etablierung von *Forensic Readiness* notwendig [YM01].

Eine weitere Möglichkeit besteht in der Dokumentation und Zusammenführung der Informationen in einem *Forensic Readiness* Managementsystem wie von Reddy und Venter [RV13] vorgeschlagen. Im Vorfallsmanagementmodul, wie in Abbildung 4.4 dargestellt werden die für eine Untersuchung wichtigen Informationen zusammengeführt und bei der Vorfallsbehandlung entsprechend einbezogen [RV13].

Unternehmenskommunikation

Zur *Forensic Readiness* gehört auch die Festlegung von Richtlinien zur Unternehmenskommunikation und Öffentlichkeitsarbeit. Es ist wichtig, vorab festzulegen wer wann

und wie informiert wird [WWW03]. Informationen müssen sorgsam kommuniziert werden, z.B. an Strafverfolgungsbehörden, Internetprovider oder andere Dritte [Cas05]. Andernfalls können Missverständnisse entstehen, Zeit kann verloren gehen oder es kann zu anderen unvorhergesehenen Konsequenzen führen [Cas05].

4.2.3.3 Personelle Maßnahmen

Unter den personellen Maßnahmen werden alle das Personal des Unternehmens sowie für das Unternehmen arbeitende Personen betreffende Maßnahmen verstanden.

Response Team
Das Response Team, auch CERT (Computer Emergency Response Team) genannt, führt digitale forensische Untersuchungen tatsächlich durch [RV13]. Für die *Forensic Readiness* ist ein solches Team obligatorisch. Es setzt sich in der Regel aus einer breiten Palette an Mitarbeitern zusammen [YM01, Row04]. Typische Mitglieder sind neben Mitarbeitern der IT Mitarbeiter aus der Personalabteilung, der Unternehmenskommunikation, des Vorstands und der Rechtsabteilung [YM01, Row04]. Weiter können die jeweils für die Geschäftsprozesse und Daten verantwortlichen Personen sowie der Werkschutz Teil des Teams sein [Row04].

Das Team soll durch seine Zusammensetzung dazu befähigt werden auch kritische Fragen, wie z.B. ob ein bestimmtes System abgeschaltet werden kann oder welches Vorgehen gewählt werden soll selbst beantworten können [YM01, SLRG06].

Schulungen
Neben der Zusammensetzung des Response Teams ist auch die Schulung der dem Response Team zugeordneten Mitarbeiter notwendig [Cas05, SLRG06, EAML15]. Zusätzlich zur Vorbereitung der Teammitglieder auf ihre potentielle Aufgabe beim Eintreten eines Vorfalls ist es notwendig, Erfahrungen aus vergangenen Vorfällen in das Training und die Schulungsmaßnahmen zu integrieren [RV13].

Schulungsmaßnahmen sollten aber auch alle anderen Mitarbeiter des Unternehmens, die einen PC im Rahmen ihrer Tätigkeit benutzen einschließen, um ein Bewusstsein für digitale forensische Untersuchungen zu entwickeln [YM01, EAML15]. Eine kritische Gruppe sind die Systemadministratoren, da sie klare Handlungsanweisungen erhalten sollen, um Vorfälle erkennen und auf Vorfälle adäquat reagieren zu können, bis das Response Team die Arbeit übernimmt [Cas05].

4.3 Zusammenfassung

Die in diesem Kapitel vorgestellten Problemlösungsstrategien in der Literatur zur digitalen Forensik in Unternehmen bestätigen die bereits in Abschnitt 2.1 enthaltene Aussage, dass wenig wissenschaftliche Literatur in der digitalen Forensik vorhanden ist [YM01, Kes12]. Sowohl im Themenbereich digitale Forensik in Unternehmen wie

auch im speziellen Bereich *Forensic Readiness* zeigen die beiden Ergebnistabellen 4.4 und 4.7 aus den Literaturrecherchen, dass die wissenschaftliche Strenge oft nicht erfüllt wird. Viele der Arbeiten, die durch die strukturierten Literaturrecherchen identifiziert wurden, gleichen mehr Berichten von Praktikern. Dabei wird ein Aspekt nach dem anderen genannt, ohne, dass eine klare Struktur oder eine wissenschaftliche Methodik erkennbar sind. Weiter wurden die vorgestellten Lösungen größtenteils nicht evaluiert, was sich deutlich in der Spalte *Evaluation* der Tabellen 4.4 und 4.7 zeigt.

Neben dem Vergleich und der Bewertung der jeweiligen Arbeiten aus den beiden Literaturrecherchen wurde im vorigen Abschnitt 4.2.3 ein Maßnahmenkatalog zur Implementierung von *Forensic Readiness* in Unternehmen aus den einzelnen Arbeiten, die im Rahmen der Literaturrecherche zur *Forensic Readiness* identifiziert wurden, zusammengetragen. Der Katalog zeigt, dass zumindest über die Arbeiten hinweg größtenteils ein Konsens hinsichtlich der zu implementierenden Maßnahmen im jeweiligen Bereich herrscht. Keine der Arbeiten gibt eine gänzlich neue Richtung vor und viele der Arbeiten greifen z.B. auf die vielzitierten Maßnahmen von Rowlingson [Row04] zurück oder bauen darauf auf. Zudem adressieren die Maßnahmen alle Bereiche der Informationssysteme nach den Definitionen aus Kapitel 3 und enthalten sowohl Maßnahmen für die Menschen, die Informations- und Kommunikationstechnik sowie für organisatorische Aspekte.

KAPITEL 5

Digitale Forensik und Forensic Readiness in der Unternehmenspraxis

Um den tatsächlichen Stand der Nutzung von Methoden aus der digitalen Forensik in der Praxis festzustellen, wurde im Rahmen der Seminararbeit [HDL13] eine Studie durchgeführt. Die Rohdaten wurden anschließend zum Teil neu ausgewertet und in verkürzter Form in [MP14] veröffentlicht. Dieses Kapitel basiert auf der Veröffentlichung [MP14]. Das Kapitel enthält aber über die Ergebnisse aus [MP14] hinaus weitere bislang unveröffentlichte Ergebnisse sowie einen Vergleich mit den in [Qui05] und [Ker13] vorgestellten Ergebnissen ähnlicher Studien.

Im folgenden Abschnitt 5.1 wird das Studiendesign, die Methodik und die Studiendurchführung beschrieben. Abschnitt 5.2 beschreibt das Teilnehmerfeld. In den anschließenden Abschnitten 5.3 - 5.6 werden die Ergebnisse vorgestellt und am Ende zusammengefasst.

5.1 Studiendesign und Durchführung

Das Hauptziel der Studie war es zu klären, ob sich Organisationen tatsächlich bereits aktiv mit dem Thema digitale Forensik und *Forensic Readiness* beschäftigen. Weiter sollte geklärt werden, ob und für welchen Zweck digitale Forensik in Organisationen verwendet wird, wenn es bereits eingesetzt wird und wieso digitale forensische Methoden nicht eingesetzt werden, wenn noch kein Einsatz stattgefunden hat.

Da die digitale Forensik in Organisationen oft mit IT-Sicherheitsvorfällen in Verbindung gebracht wird, sollten auch Beziehungen zum Bereich IT-Sicherheit überprüft werden. Insbesondere die im Rahmen einer Zertifizierung des IT-Sicherheitsmanagements

nach ISO 27001 [ISO13] umgesetzten Maßnahmen gelten als Basisvoraussetzungen für digitale forensische Untersuchungen [Nel06], weshalb hier auch die Details etwaiger Beziehungen genauer mit untersucht werden sollten.

Zusammenfassend wurden folgende Forschungsfragen abgeleitet, die mithilfe der Studie geklärt wurden:

1. Haben sich Organisationen bereits mit der Thematik digitale Forensik beschäftigt und entsprechende Maßnahmen und Ressourcen etabliert?
2. Zu welchem Zweck werden Methoden der digitalen Forensik verwendet?
3. Sehen die Organisationen Beziehungen zum IT-Sicherheitsmanagement?
4. Welche Gründe stehen dem Einsatz von digitaler Forensik in Organisationen entgegen?

Zur Durchführung der Studie wurde ein Fragebogen mit insgesamt 21 Fragen erstellt. Der Fragebogen war sowohl als *Offlineversion* in Papierform verfügbar als auch online mithilfe des Systems SoSci Survey[1] modelliert. Potentielle Teilnehmer wurden entweder per E-Mail eingeladen den Onlinefragebogen auszufüllen oder auf Veranstaltungen mit dem Themenschwerpunkt IT-Sicherheit direkt akquiriert. Insgesamt konnten im Untersuchungszeitraum vom 15.05.2013 bis 24.06.2013 **69 Organisationen** befragt werden.

5.2 Studienteilnehmer

Die Teilnehmer der Studie kommen überwiegend aus Deutschland, was aufgrund der Durchführung der Studie im deutschsprachigen Raum wenig überraschend ist. Von den 69 befragten Organisationen haben daher 65 ihren Hauptsitz in Deutschland. Die verbliebenen vier Organisationen haben ihren Sitz in Frankreich, Japan, der Türkei und in den Vereinigten Staaten.

Abbildung 5.1 zeigt die Größe der Unternehmen gemessen an deren Mitarbeiterzahl und der zugehörigen Branche. 20 Unternehmen haben demnach weniger als 100 Mitarbeiter. Neun Teilnehmer haben zwischen 100 und 500 und sieben zwischen 500 und 1.000 Mitarbeiter. 21 Unternehmen haben 1.000 - 10.000 Mitarbeiter und zwölf Teilnehmer haben mehr als 10.000 Mitarbeiter. Deutlich zu sehen ist in Abbildung 5.1 auch, dass es gelungen ist, Organisationen aus verschiedenen Branchen und mit unterschiedlicher Größe zu akquirieren.

Wie in Abbildung 5.2 ersichtlich, haben manche Unternehmen die Frage nach ihrem Umsatz nicht beantwortet oder konnten dies nicht beantworten, da es sich z.B. um eine staatliche Einrichtung ohne Umsatz handelt. Daher wird im Folgenden und bei allen

[1] https://www.soscisurvey.de/

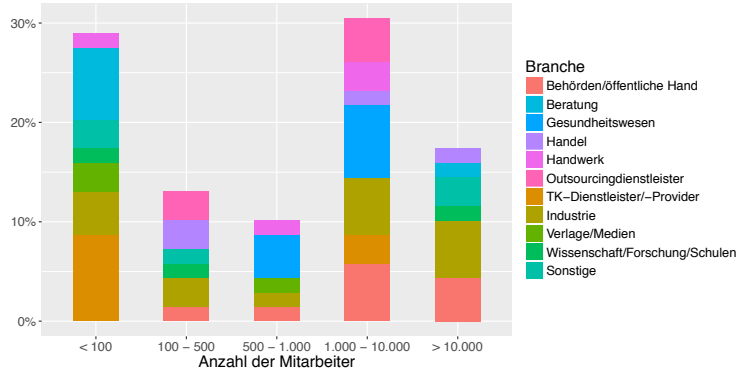


Abbildung 5.1 – Teilnehmer nach Anzahl der Mitarbeiter und Branche

Hypothesentests als Kennzahl für die Unternehmensgröße immer die Anzahl der Mitarbeiter verwendet. Bei allen Hypothesentests gilt zudem eine Irrtumswahrscheinlichkeit von $\alpha = 0{,}05$. Das Hypothesenpaar ist dabei definiert als:

$\mathbf{H}_0$ Die Merkmale sind unabhängig.

$\mathbf{H}_1$ Die Merkmale sind abhängig.

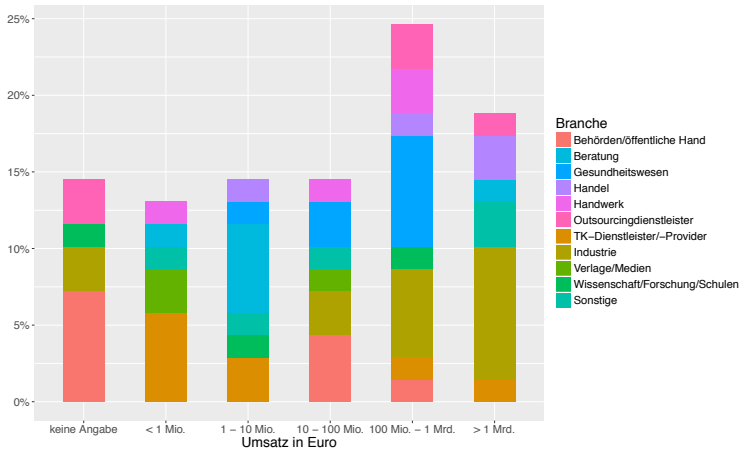


Abbildung 5.2 – Teilnehmer nach Umsatz und Branche

Die Unternehmen nach Umsatz sind in Abbildung 5.2 dargestellt. Wenngleich der Umsatz bei den Hypothesentests nicht als Kennzahl verwendet wird, so wird doch ein

detaillierteres Bild der Studienteilnehmer erkennbar. Von den 69 Teilnehmern haben zehn die Frage nach ihrem Umsatz nicht beantwortet. Neun Unternehmen haben einen Umsatz von unter einer Million €. Einen Umsatz von 1 bis 10 Millionen sowie von 10 bis 100 Millionen € haben jeweils zehn Unternehmen. 17 Teilnehmer haben einen Umsatz von 100 Millionen bis zu einer Milliarde € und 13 Unternehmen haben einen Umsatz von mehr als einer Milliarde €. Die Branchenzugehörigkeit der Unternehmen ist, wie bereits bei der Gruppierung nach der Anzahl der Mitarbeiter in Abbildung 5.1, auch über die Umsatzkategorien, wie in Abbildung 5.2 dargestellt, gut verteilt.

5.3 Ergebnisse

Da die digitale Forensik oft mit der IT-Sicherheit in Verbindung gebracht wird, wurde das jährliche Budget für IT-Sicherheit abgefragt. Abbildung 5.3 stellt die Ergebnisse im Vergleich zur Mitarbeiterzahl dar. Der in Abbildung 5.3 zusätzlich zu beobachtende Zusammenhang zwischen der Mitarbeiterzahl und den Ausgaben für IT-Sicherheit ist auch statistisch nachweisbar. Dabei sind die Ausgaben für IT-Sicherheit höher, je größer ein Unternehmen ist (Spearmans Rangkorrelationskoeffizient (r_s) = 0,82). Weiter ist der Zusammenhang auch statistisch signifikant bei einem p-Wert von 0,00. Zwischen der Branche und den Ausgaben für IT-Sicherheit beträgt der Kontingenzkoeffizient (K) 0,77, jedoch muss aufgrund eines p-Wertes von 0,20 ein statistischer Zusammenhang abgelehnt werden.

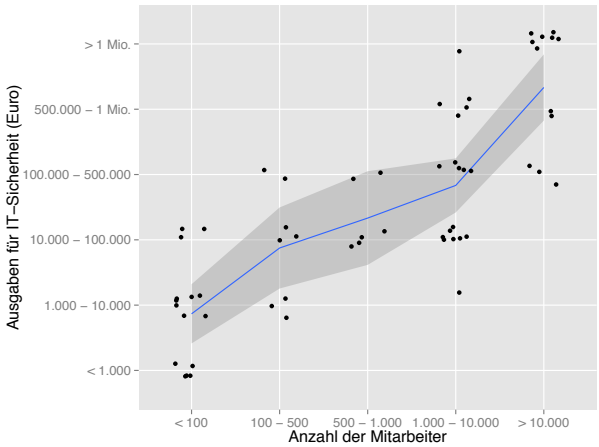


Abbildung 5.3 – Anzahl der Mitarbeiter in Relation zu den Ausgaben für IT-Sicherheit

Die zentrale Frage nach der Implementierung bzw. Verwendung von digitaler Forensik sollte zum einen über die Frage nach der bewussten Implementierung von

Maßnahmen aus der *Forensic Readiness* beantwortet werden und zum anderen über die Frage, ob im Unternehmen bereits digitale forensische Untersuchungen durchgeführt wurden bzw. dies zukünftig geplant ist. Abbildung 5.4 zeigt die Antworten auf die beiden Fragen in einer kombinierten Darstellung. Die Balken zeigen jeweils den Prozentsatz der Antworten auf die Frage nach der Implementierung von *Forensic Readiness*. Die Antwort auf die Frage, ob im Unternehmen bereits eine digitale forensische Untersuchung durchgeführt wurde, wird über die Füllung der Balken in Abbildung 5.4 dargestellt. Abhängig von der Antwort auf die erste Frage wurde die Antwort auf die zweite Frage dem entsprechenden Balken zugeordnet. Lediglich 15,93 % der Organisationen haben demnach bereits Maßnahmen aus dem Bereich *Forensic Readiness* implementiert. Davon haben zudem bereits 90,91 % forensische Untersuchungen durchgeführt. 40,60 % der Organisationen planen zukünftig konkrete Maßnahmen der *Forensic Readiness* zu implementieren. In dieser Gruppe haben noch gut die Hälfte der Unternehmen (53,57 %) keine forensische Untersuchung durchgeführt. In 43,47 % der Organisationen spielt das Thema *Forensic Readiness* dagegen überhaupt keine Rolle, wobei hier auch nur 10,00 % in der Vergangenheit bereits eine forensische Untersuchung durchgeführt haben. Insgesamt haben bereits 37,68 % der befragten Organisationen digitale forensische Untersuchungen durchgeführt. In 62,32 % der Organisationen wurden noch keine Untersuchungen durchgeführt und es sind auch keine digitalen forensischen Untersuchungen geplant.

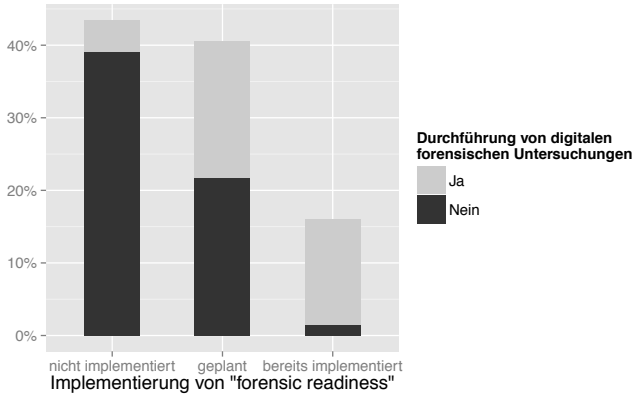
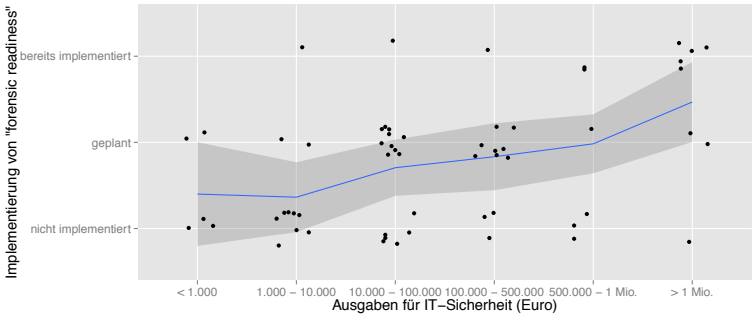
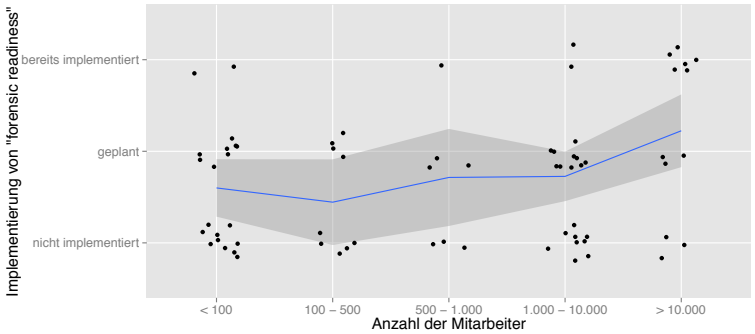


Abbildung 5.4 – Implementierung von *Forensic Readiness* und Durchführung digitaler forensischer Untersuchungen

Betrachtet man Abbildung 5.4 genauer und bezieht die Zahlen aus dem vorherigen Absatz mit ein, so lässt sich eine Korrelation zwischen der Durchführung von Untersuchungen und der Implementierung bzw. Planung von Maßnahmen der *Forensic Readiness* vermuten. Die Korrelation lässt sich mit einem r_s von 0,58 bestätigen und



(a) *Forensic Readiness* und Ausgaben für IT-Sicherheit



(b) *Forensic Readiness* und Unternehmensgröße

Abbildung 5.5 – Ausgaben für IT-Sicherheit bzw. Unternehmensgröße in Relation zur *Forensic Readiness*

ist statistisch signifikant bei einem p-Wert von 0,00.

Eine besondere Abhängigkeit zwischen einer Zertifizierung nach ISO 27001 [ISO13] und der Durchführung digitaler forensischer Untersuchungen kann nicht nachgewiesen werden. Dagegen kann aber hinsichtlich der Implementierung von *Forensic Readiness* eine Korrelation zur Größe einer Organisation als auch zu den IT-Sicherheitsausgaben nachgewiesen werden. Abbildung 5.5(a) zeigt die Ausgaben für IT-Sicherheit in Relation zur Implementierung von *Forensic Readiness*. Die Korrelation ist bei $r_s = 0{,}41$ (p-Wert = 0,00) aber eher schwach. Dasselbe gilt für die Abhängigkeit der *Forensic Readiness* von der Unternehmensgröße, dargestellt in Abbildung 5.5(b). Hier kann lediglich eine sehr schwache aber statistisch signifikante Korrelation von $r_s = 0{,}24$ (p-Wert = 0,02) nachgewiesen werden.

Eine Abhängigkeit des Implementierungsgrades von der Branche muss dagegen jedoch abgelehnt werden (K = 0,63, p-Wert = 0,20). Weiter hat auch die Bedeutung

von IT-Systemen für den Geschäftsbetrieb nur eine sehr geringe (r_s = 0,30, p-Wert: 0,01) Auswirkung auf die Implementierung von Maßnahmen der *Forensic Readiness*. Abbildung 5.6 zeigt dies, wobei für 71,01 % der Unternehmen die Informationssysteme einen essentiellen Stellenwert haben. Aus diesem Grund ist die Korrelation nur sehr schwach, da von den 71,01 % mit essentiellem Stellenwert der IS 79,59 % Unternehmen sind, die lediglich die Einführung von Maßnahmen der *Forensic Readiness* geplant haben oder noch gar keine Maßnahmen implementiert haben. Eine Zertifizierung nach ISO 27001 [ISO13] und die Implementierung bzw. geplante Implementierung von Maßnahmen der *Forensic Readiness* korrelieren mit einem r_s von 0,48 (p-Wert = 0,00) moderat.

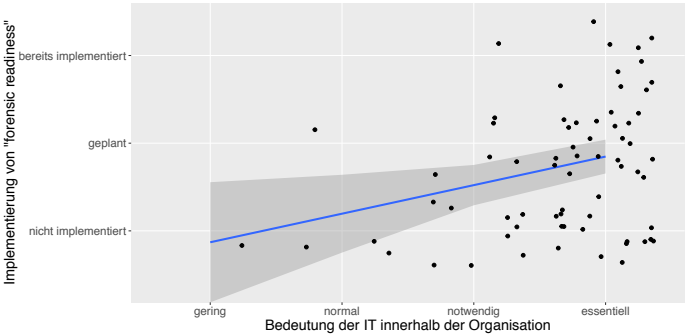


Abbildung 5.6 – Forensic Readiness und Bedeutung der Informationssysteme für die Organisation

Neben den präventiven Maßnahmen der IT-Sicherheit sollte auch geprüft werden, ob die befragten Organisationen tatsächlich bereits Opfer von Computerkriminalität bzw. digitalen Angriffen wurden. Eine Organisation hat bei dieser Frage keine Auskunft erteilt. Von den verbleibenden 68 Organisationen wurden 40,0 % bereits Opfer von Angriffen.

Wurde eine Organisation bereits Opfer eines Angriffs auf ihre IT-Systeme, so könnte man vermuten, dass das Unternehmen sich auf zukünftige Angriffe besser vorbereitet. Ein Zusammenhang zwischen der Implementierung von *Forensic Readiness* und der Opfer von Angriffen kann aber nicht nachgewiesen werden (r_s = 0,13, p-Wert = 0,15). Auch die Ausgaben für die IT-Sicherheit sind bei Organisationen, die bereits angegriffen wurden, nicht zwingend höher als bei den anderen 60 % der noch nicht wissentlich erfolgreich angegriffenen Organisationen (r_s = 0,24, p-Wert = 0,07). Die Gruppe der noch nicht erfolgreich angegriffenen Organisationen wurde zudem befragt, ob die Organisation in naher Zukunft mit einem Angriff rechnet. Dabei gaben 44,0 % der Organisationen an, dass sie nicht mit einem Angriff rechnen und 56,0 % der Organisationen rechnen mit einem Angriff. Die Organisationen, die mit einem Angriff rechnen, bereiten sich jedoch nicht zwingend besser auf digitale forensische

Untersuchungen vor als die Organisationen, die nicht mit einem Angriff rechnen (r_s = 0,19, p-Wert = 0,12).

5.3.1 Einsatz von digitaler Forensik in Organisationen

Der Einsatz von Methoden der digitalen Forensik wird in Abbildung 5.7 dargestellt. Abbildung 5.7 zeigt im Detail zu welchen Zwecken Methoden der digitalen Forensik in Organisationen verwendet werden. Am häufigsten verwenden Organisationen demnach digitale Forensik tatsächlich zur Täteridentifikation nach einem IT-Sicherheitsvorfall, gefolgt von einem expliziten Lernen von einem digitalen Angriff zur Verbesserung der IT-Sicherheit. Darauf folgend wird digitale Forensik zur Untersuchung von Verstößen gegen interne Richtlinien verwendet und danach zur Aufklärung von klassischen Verbrechen. Bei der Häufigkeit von digitalen forensischen Untersuchungen gibt es keinen Zusammenhang zwischen großen Organisationen und häufigeren Untersuchungen (r_s = 0,19, p-Wert = 0,23). Weiter haben Organisationen, die regelmäßig forensische Untersuchungen durchführen nicht zwingend interne personelle Ressourcen, um diese Untersuchungen durchzuführen (r_s = 0,32, p-Wert = 0,20).

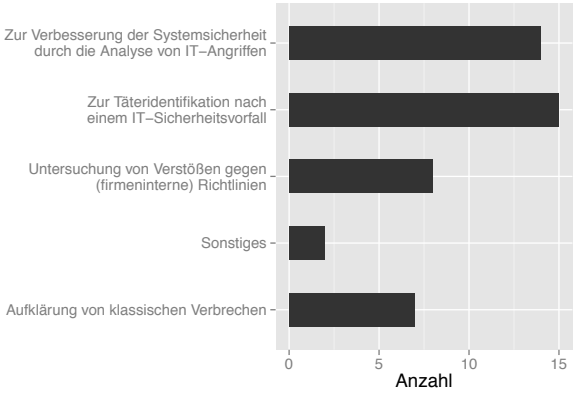


Abbildung 5.7 – Verwendung von digitaler Forensik in Organisationen

Die Höhe der Ausgaben für IT-Sicherheit und die Höhe der Ausgaben für digitale Forensik korrelieren dagegen sehr stark bei einem r_s = 0,87 und einem p-Wert von 0,00. Abbildung 5.8 zeigt diesen Zusammenhang.

5.3.2 Gründe für das Fehlen von digitalen forensischen Maßnahmen in Organisationen

Neben den im vorigen Abschnitt 5.3.1 beschriebenen konkreten Zielen von digitalen forensischen Untersuchungen wurde im Rahmen der Studie auch explizit nachgefragt,

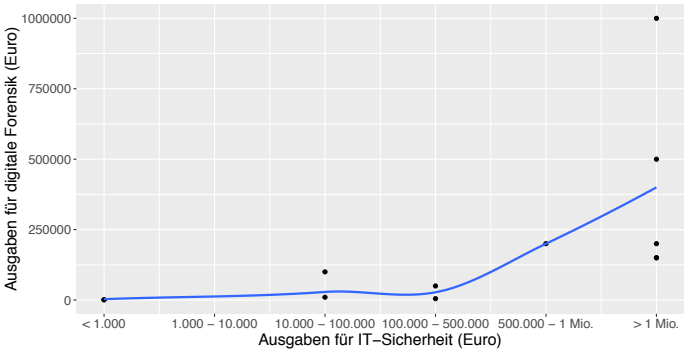


Abbildung 5.8 – Ausgaben für IT-Sicherheit und digitale Forensik

wieso digitale Forensik gerade nicht eingesetzt wird. Abbildung 5.9 zeigt die Antworten auf diese Frage. Demnach wird digitale Forensik insbesondere aufgrund fehlender personeller und/oder finanzieller Mittel nicht eingesetzt, gefolgt von fehlenden Best Practices für digitale forensische Untersuchungen. In 15 Organisationen ist das Thema nicht einmal bekannt und vier Organisationen halten digitale Forensik sogar für nicht geeignet.

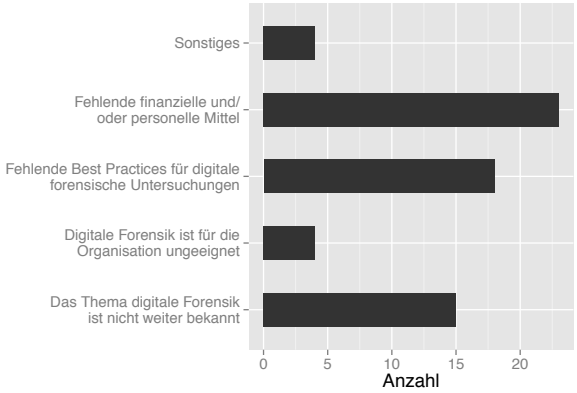


Abbildung 5.9 – Gründe wieso digitale Forensik in Organisationen nicht zum Einsatz kommt

5.4 Bewertung der Ergebnisse

Im Folgenden sollen nun die in Abschnitt 5.1 aufgeworfenen Forschungsfragen mithilfe der Ergebnisse aus dem vorigen Abschnitt 5.3 diskutiert und beantwortet werden.

Frage 1: Haben sich Organisationen bereits mit der Thematik digitale Forensik beschäftigt und entsprechende Maßnahmen und Ressourcen etabliert?
Die Antwort auf diese Frage liefern die Ergebnisse aus der direkten Frage nach der Implementierung von Maßnahmen aus dem Bereich *Forensic Readiness* sowie der Nachfrage hinsichtlich der Durchführung von digitalen forensischen Untersuchungen. Die Antworten zeigen, dass manche, insbesondere große Organisationen sich bereits mit dem Thema auseinandergesetzt haben. Weiter wurden in 37,68 % der befragten Organisationen bereits digitale forensische Untersuchungen durchgeführt. Zusammenfassend lässt sich sagen, dass sich manche Organisationen bereits mit dem Thema digitale Forensik beschäftigt haben. In der Mehrzahl der Organisationen ist jedoch keine Forensikkompetenz vorhanden und das Thema ist eher eine Randerscheinung.

Frage 2: Zu welchem Zweck werden Methoden der digitalen Forensik verwendet?
Forschungsfrage 2 lässt sich erschöpfend über Abbildung 5.7 beantworten. Es zeigt sich, dass digitale Forensik tatsächlich für die Täteridentifikation verwendet wird. Aber auch die Kontrolle und Durchsetzung von internen Richtlinien mittels Methoden der digitalen Forensik zeigt, dass das breite Anwendungsspektrum zumindest in einigen wenigen Organisationen bereits ausgeschöpft wird.

Frage 3: Sehen die Organisationen Beziehungen zum IT-Sicherheitsmanagement?
Verbindungen zwischen der IT-Sicherheit und der digitalen Forensik können über das zur Verfügung stehende Budget für das jeweilige Thema nachgewiesen werden. So ist eine positive Korrelation zwischen der Höhe der Ausgaben für IT-Sicherheit und dem Budget für digitale Forensik nachweisbar. Was die Vorbereitung auf digitale forensische Untersuchungen mittels Methoden aus der *Forensic Readiness* angeht, kann zumindest eine schwache positive Beziehung zu den Ausgaben für IT-Sicherheit festgestellt werden. Auch gibt es eine sehr schwache Korrelation zwischen einer vorhandenen Zertifizierung nach ISO 27001 und der Implementierung von *Forensic Readiness*. Zusammenfassend können durchweg eher schwache bis mittelstarke Beziehungen zwischen den Gebieten nachgewiesen werden.

Frage 4: Welche Gründe stehen dem Einsatz von digitaler Forensik in Organisationen entgegen?

Neben den heute schon genutzten Möglichkeiten der digitalen Forensik hat die Studie insbesondere gezeigt, wieso das Thema digitale Forensik gerade keine Rolle in der Mehrzahl der befragten Organisationen spielt. Abbildung 5.9 beantwortet diese Frage direkt. Neben fehlenden personellen wie auch finanziellen Mitteln sind insbesondere fehlende Best Practices Gründe, wieso die digitale Forensik eine solch geringe Durchdringung erfährt. Auch ist es eher beunruhigend, dass manche Organisationen die digitale Forensik für ungeeignet halten bzw. das Thema noch gar nicht in der Organisation bekannt ist.

5.5 Vergleich der Ergebnisse

Auch Quinn [Qui05] und Kerrigan [Ker13] haben im Rahmen ihrer Arbeiten jeweils Studien zur Vorbereitung von Unternehmen auf digitale forensische Untersuchungen durchgeführt.

Die in [Qui05] vorgestellte Studie hatte ein ähnliches Ziel wie die in diesem Kapitel vorgestellte Studie. Im Wesentlichen ging es darum zu prüfen, ob ein Bewusstsein für das Thema digitale Forensik besteht und inwieweit die Organisationen auf forensische Untersuchungen vorbereitet sind [Qui05]. Für die Studie wurden 750 Manager mit IT-Verantwortung in Neuseeland gezielt angeschrieben. 162 Manager haben schlussendlich an der Studie teilgenommen. Die *Forensic Readiness* hat Quinn [Qui05] besonders an den Fragen nach dem eigenen oder fremden Personal und nach Richtlinien für digitale forensische Untersuchungen festgemacht. Demnach haben 29 % der befragten Unternehmen eigenes oder fremdes Personal zur Durchführung digitaler forensischer Untersuchungen und 15 % haben Richtlinien zur Durchführung von Untersuchungen und zur Handhabung digitaler Spuren [Qui05]. Das Fazit der Studie ist, dass sehr viele Unternehmen nicht ausreichend auf digitale forensische Untersuchungen vorbereitet sind [Qui05].

Wenngleich Kerrigan [Ker13] zur Evaluation seines Reifegradmodells nur zehn Organisationen aus Irland befragt hat, so sind die Ergebnisse seiner Befragung dennoch mit der Studie in [Qui05] sowie der in diesem Kapitel vorgestellten Studie vergleichbar, da sein Reifegradmodell mehr oder minder die *Forensic Readiness* einer Organisation messbar machen soll. Weiter wurde die Studie als Expertenstudie entweder im persönlichen Gespräch oder per Telefon durchgeführt. Im Ergebnis haben 70 % der Organisationen angegeben, keine strukturierten Maßnahmen aus dem Bereich *Forensic Readiness* implementiert zu haben. 30 % haben entweder externe Berater oder eigenes Personal und Mittel für digitale forensische Untersuchungen [Ker13].

Die zumindest in Teilen vergleichbaren Ergebnisse aus den Studien von Quinn [Qui05] und Kerrigan [Ker13] sind zusammen mit den in diesem Kapitel bzw. in [MP14] veröffentlichten Ergebnissen zur *Forensic Readiness* in Abbildung 5.10 gemeinsam dargestellt. Die Tendenz ist dabei immer die Gleiche. Viele Organisationen sind nicht ausreichend auf digitale forensische Untersuchungen vorbereitet. Durch die

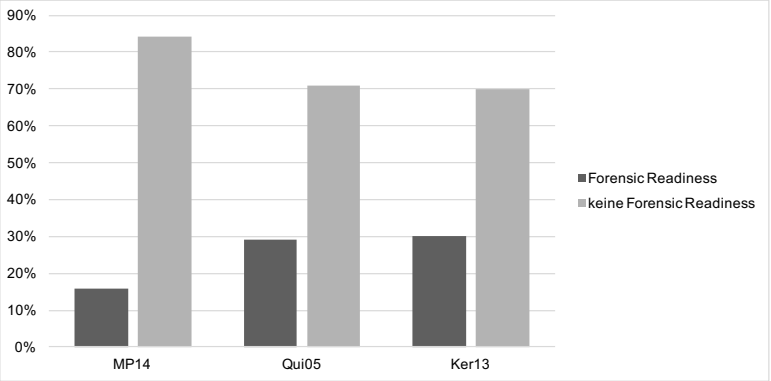


Abbildung 5.10 – Vergleich der Studienergebnisse mit ähnlichen Studien

Gegenüberstellung der Studien zeigt sich auch, dass dies kein Problem ist, das nur auf deutsche Unternehmen zutrifft. Wenngleich die Zahlen zu Unternehmen, die Maßnahmen der *Forensic Readiness* implementiert haben, aus der in diesem Kapitel vorgestellten Studie am niedrigsten erscheinen, so ist dies nur bedingt aussagekräftig, da z.B. für die Studie aus Neuseeland [Qui05] der Wert von 29 % für das Personal verwendet wurde, während der Wert für Richtlinien zur Durchführung von digitalen forensischen Untersuchungen ebenfalls bei vergleichbaren 15 % liegt. Global lässt sich daher der Trend feststellen, dass Unternehmen zu einem Großteil nicht auf digitale forensische Untersuchungen vorbereitet sind.

5.6 Zusammenfassung

Die in diesem Kapitel vorgestellte Studie zeigt, dass digitale forensische Untersuchungen in manchen Organisationen bereits in der vollen Breite im Sinne der zu untersuchenden Fälle genutzt werden, was in Abbildung 5.7 deutlich wird. Viel wichtiger ist jedoch die Erkenntnis, dass insbesondere Best Practices fehlen und auch die notwendigen personellen wie auch finanziellen Mittel zur Einführung und Nutzung von digitaler Forensik anscheinend noch zu hoch sind. Auch ist in vielen Organisationen ein Bewusstsein für die Thematik digitale Forensik nicht vorhanden.

Bestätigt wird die Tendenz aus der Studie in diesem Kapitel durch den Vergleich mit anderen Studien im vorherigen Abschnitt 5.5. Dabei wird nochmals deutlich, dass das Thema *Forensic Readiness* noch keine Durchdringung der Organisationen erfahren hat und viele Unternehmen nur sehr schlecht auf digitale forensische Untersuchungen vorbereitet sind.

Teil III

Unternehmensforensik

KAPITEL 6

Grundlagen der Unternehmensforensik

Auf Basis der Erkenntnisse aus den vorherigen Kapiteln wird nun im folgenden Abschnitt 6.1 die Unternehmensforensik von den bestehenden Problemlösungsstrategien aus der in Kapitel 4 vorgestellten Literatur abgegrenzt und definiert. Anschließend zeigt Abschnitt 6.2 Möglichkeiten zur formalen Definition eines Prozesses auf, auf deren Basis dann eine für die digitale Forensik in Unternehmen erweiterte Prozessdefinition entwickelt wird. Im Anschluss daran wird diese formale Prozessdefinition im Abschnitt 6.3 genutzt, um die Entstehung digitaler Spuren in den AWS aus Sicht der Prozesse zu betrachten. Weiter werden im Abschnitt 6.3 die Definitionen zu digitalen Spuren nach Dewald [Dew12], wie sie in Abschnitt 2.4 beschrieben sind, auf die digitalen Spuren aus Sicht der Prozesse transferiert. Die digitalen Spuren aus Sicht der Prozesse werden in Abschnitt 6.3.3 zudem mit den digitalen Spuren und den Begrifflichkeiten, wie sie in Abschnitt 2.4 vorgestellt wurden verglichen. Abschnitt 6.4 fasst die Ergebnisse dieses Kapitels abschließend zusammen.

6.1 Abgrenzung und Definition der Unternehmensforensik

Die Unternehmensforensik (*Enterprise Forensics*) ist, wie in den vorherigen Kapiteln 4 und 5 dargelegt ein in großen Teilen von Praktikern dominiertes Gebiet. Viele Publikationen beschäftigen sich mit digitalen forensischen Untersuchungen in Unternehmen. Eine konkrete Definition der Unternehmensforensik sowie eine klare Abgrenzung des Forschungsfeldes bleiben aber bislang offen. Auch sind die vorgestellten Arbeiten, wie in Abschnitt 4.3 festgestellt oft keine Arbeiten, denen eine rigorose wissenschaftliche Methodik zugrunde liegt. Dies wird besonders bei näherer Betrachtung der Tabellen 4.4 und 4.7 deutlich, da die Evaluation als wesentlicher Bestandteil einer wissenschaftlichen

Methodik oft fehlt.

Neben dem obigen Aspekt wird eine Abgrenzung der Unternehmensforensik von der regulären, allgemeinen digitalen Forensik zwar vielfach motiviert, schlüssige Gründe finden sich in den Arbeiten allerdings kaum. Oft wird in den in Abschnitt 4.1 aufgezeigten Publikationen von einer höheren Komplexität bei einer digitalen forensischen Untersuchung im Unternehmen gesprochen. Dieses Argument kann aber einer kritischen Betrachtung kaum standhalten, da es auch außerhalb von Unternehmen komplexe digitale forensische Untersuchungen gibt, z.B. bei der Aufdeckung und Untersuchung von bandenmäßiger (Online-)Kriminalität [Cas11, S. 255]. Ein weiterer Hinweis, dass die Komplexität nicht der entscheidende Faktor bei der Unterscheidung zwischen Unternehmensforensik und digitaler Forensik im Allgemeinen darstellt, ist die Tatsache, dass die allgemeinen Prozessschritte für digitale forensische Untersuchungen nach Casey [Cas11, S. 189f] ausreichend sind, um alle in Abschnitt 4.1.2.1 vorgestellten Prozessmodelle entsprechend zu bewerten und einzuteilen. Der Prozess zur Durchführung einer digitalen forensischen Untersuchung im Unternehmen unterscheidet sich also im Grunde nicht vom allgemeinen Prozess zur Durchführung einer digitalen forensischen Untersuchung. Die Komplexität ist daher kein grundsätzlich anwendbares Kriterium, um zwischen digitalen forensischen Untersuchungen in und außerhalb von Unternehmen zu unterscheiden.

Ein anderer Ansatz zur Unterscheidung zwischen digitaler Forensik, ausgeführt von Strafverfolgungsbehörden, Unternehmen oder Militärs wird in [FI06] vorgeschlagen. Forrester und Irwin [FI06] argumentieren, dass es grundsätzlich unterschiedliche Ziele für eine Untersuchung gibt. Bei der Literaturrecherche zur Unternehmensforensik, die in Abschnitt 4.1 beschrieben ist, enthält aber außer der Arbeit von Forrester und Irwin [FI06] keine andere Arbeit eine ähnliche oder die selbe Argumentation. Es besteht daher offenbar kein allgemeiner Konsens, die digitale Forensik auf Basis der ausführenden Entität zu unterscheiden. Die Argumentation ist zudem leicht zu widerlegen, da auch Strafverfolgungsbehörden digitale forensische Untersuchungen in Unternehmen durchführen. Dabei müssen sie ebenfalls je nach Fall zwischen einer schnellen Wiederherstellung der Dienste des Unternehmens und einer fundierten und umfassenden Sicherung digitaler Spuren abwägen.

Die Anforderungen und Grenzen, die sich durch die jeweilige Rechtsprechung und die Gesetze ergeben, werden ebenfalls oft als Unterscheidungskriterium genannt. Sie sind aber lediglich ein limitierender Faktor und gelten vielfach nur für interne Ermittler des Unternehmens oder externe private Ermittler. Daher stellen die rechtlichen Anforderungen und Grenzen keinen echten Unterschied zwischen der Unternehmensforensik und der allgemeinen digitalen Forensik dar.

Dagegen zeigen die in Abschnitt 4.1.2.3 beschriebenen Publikationen neben technischen Lösungen insbesondere auch Hürden für digitale forensische Untersuchungen und für die typischerweise nur in Unternehmen oder Organisationen vorzufindenden AWS auf. Sowohl die AWS selbst als auch die verteilte Natur dieser Systeme im

Unternehmen stellen den Arbeiten aus Abschnitt 4.1.2.3 zufolge eine Herausforderung bei digitalen forensischen Untersuchungen in Unternehmen dar. Aus diesem Grund motivieren einige der in Abschnitt 4.1.2.3 aufgezeigten Arbeiten die Notwendigkeit von spezialisierten Werkzeugen für die digitale Forensik in Unternehmen. Unterstützt wird diese These auch von anderen, nicht im Rahmen der in Abschnitt 4.1 vorgestellten Literaturrecherche identifizierten Arbeiten. Diese kritisieren, dass die digitale Forensik sehr stark auf Basistechnologien wie Dateisysteme, Betriebssysteme oder Mobiltelefone ausgerichtet ist [BRR06, Bee09]. Dabei sind aber auch Verfahren für nicht-Standard Umgebungen interessant [Bee09]. Es ist also klar ein Bedarf für die Entwicklung und Bereitstellung von, auf AWS zugeschnittenen Werkzeugen vorhanden, um auch digitale Spuren aus AWS mit einer entsprechend fundierten und allgemein akzeptierten Methodik im Rahmen einer digitalen forensischen Untersuchung sichern und untersuchen zu können.

Neben den technischen Aspekten, die spezielle Werkzeuge und Methoden für die digitale Forensik in Unternehmen erfordern, zeigt die in Abschnitt 4.1 vorgestellte Literaturrecherche einen weiteren Punkt auf: Einige der Arbeiten fordern vor dem Start einer digitalen forensischen Untersuchung die Umstände des Falles und die Situation im Unternehmen zu ergründen, insbesondere um relevante digitale Spuren im Vorfeld zu identifizieren [Tip93, SLRG06]. Im Wesentlichen geht es dabei um die Klärung der Frage: Wie wird in diesem Unternehmen tatsächlich gearbeitet? Auch in [AWS11] wird diese Frage adressiert: “We firmly believe that by addressing [the business process] level – as opposed to only the infrastructure – one provides complementary indication as to how a[n information] leak comes to happen and which activity and system subject are to be accounted for in case of non-compliance.” [AWS11] Dabei wird in [AWS11] explizit die Nutzung der Informationen aus den Geschäftsprozessen bei digitalen forensischen Untersuchungen gefordert, wenngleich die Arbeit [AWS11] einen sehr begrenzten Fokus hat und nur die Aufdeckung von unberechtigter Informationsweitergabe über die Logs von Prozessen betrachtet. Auch in der in Abschnitt 4.2.2.2 vorgestellten Arbeit von Reddy und Venter [RV13] wurde die Einbeziehung von Geschäftsprozessen bei der Vorfallsbehandlung gefordert.

Die Unternehmensforensik muss allerdings eine allgemeinere und breitere Sichtweise einnehmen. Das zentrale Ziel ist die fundierte Beantwortung der Fragen wie ein Informationssystem aus Sicht der Geschäftsprozesse arbeiten sollte und welche Geschäftsobjekte im Sinne digitaler Spuren in den AWS als maschinelle Aufgabenträger und Teil des Informationssystems während der Ausführung der Prozesse erzeugt werden. Weiter müssen auch die Rolle, die ein bestimmter Computer im Unternehmen hat, die Personen die Zugriff auf den Computer bzw. die fraglichen AWS haben [Tip93] oder die Richtlinien, die während der Ausführung der Prozesse beachtet werden müssen, aufgedeckt werden [AWS11].

Die im vorigen Absatz geforderte prozessorientierte Sichtweise ist in Abbildung 6.1 als Erweiterung der Abbildung 3.1 veranschaulicht. Dabei stellt die Aufgabenebene

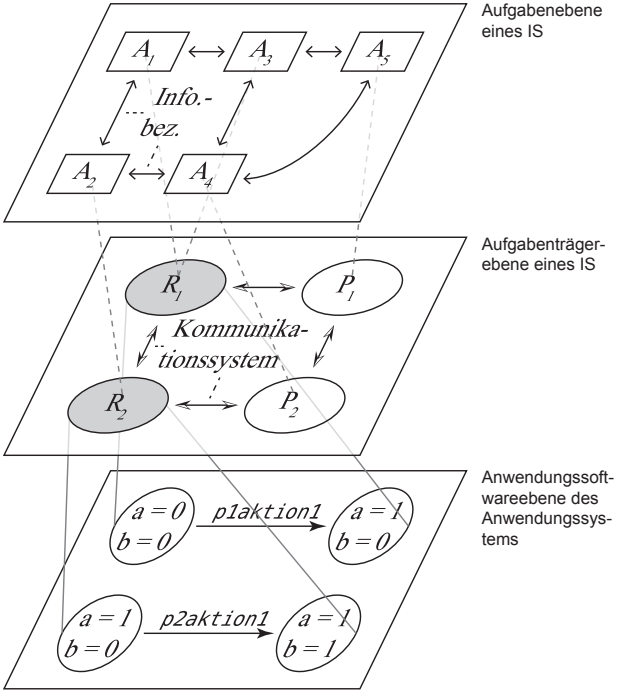


Abbildung 6.1 – Beziehungen zwischen der Aufgaben-, der Aufgabenträger- und der Anwendungssoftwareebene

die einzelnen über Prozesse definierten Aufgaben (Aktivitäten) dar. Diese einzelnen Aufgaben werden mittels der in den Prozessen definierten Beziehungen zu den Aufgabenträgern (personelle Aufgabenträger und Anwendungssysteme) durch diese Aufgabenträger wahrgenommen. Bei der Ausführung von Aktionen entstehen dann im Anwendungssystem auf der untersten Ebene, wiederum über die Prozesse definierte digitale Spuren. Die Spurenentstehung ist in Abbildung 6.1 in Anlehnung an den in Abschnitt 2.4 vorgestellten Formalismus von Dewald [Dew12] als Änderung der Variablen a und b dargestellt.

Ein Beispiel für eine unternehmensforensische Untersuchung ist der sogenannte *Rotterdam computer fraud* Fall [Koo99, S. 26],[Koo10],[Cas11, S. 149]: Ein Verwaltungsbeamter fügte betrügerische Zahlungsanweisungen in ein automatisiertes Zahlungssystem ein. Dadurch ergaunerte er drei Millionen USD. Bei einer digitalen forensischen Untersuchung des Zahlungssystems müssten dem Ermittler die Prozesse, die über das automatisierte Zahlungssystem abgebildet sind und die bei der Ausführung der Prozesse entstehenden digitalen Spuren bekannt sein. Andernfalls wäre es ggf.

nicht möglich zwischen den betrügerischen Zahlungsanweisungen und den regulären Zahlungsanweisungen, die potentiell vor- oder nachgelagerte Prozessschritte haben, zu unterscheiden. Dabei ist es unbedeutend, ob die ermittelnde Person von einer Strafverfolgungsbehörde, vom Militär oder von der Behörde bzw. dem Unternehmen selbst kommt. Entscheidend ist, den *normalen* Betrieb der Systeme und die bei der Prozessausführung entstehenden digitalen Geschäftsobjekte zu kennen. Von einem normalen Betrieb im Unternehmensumfeld wird gesprochen, wenn die Geschäftsprozesse wie geplant ausgeführt werden, andernfalls würde, wie in Abschnitt 3.2 bereits ausführlich dargelegt, Chaos herrschen [Ham15, S. 8].

Zusammengefasst kann also festgestellt werden, dass die Unternehmensforensik als Ziele die Nutzung der Prozesse eines Unternehmens in digitalen forensischen Untersuchungen sowie die Entwicklung und Bereitstellung von Werkzeugen und Methoden zur Untersuchung von AWS hat. Die Unternehmensforensik wird daher wie folgt definiert:

> Die Unternehmensforensik ist eine Teildisziplin der digitalen Forensik, die Methoden und Techniken zur Nutzung von Prozessen bei digitalen forensischen Untersuchungen in Unternehmen entwickelt und bereit stellt. Weiter beschäftigt sich die Unternehmensforensik mit Methoden und Werkzeugen zur Identifikation, Sicherung, Analyse und Präsentation von digitalen Spuren aus den Anwendungssystemen von Unternehmen.

Durch die Nutzung einer prozesszentrierten Sicht wird erwartet, die Entstehung bzw. die Existenz von digitalen Spuren in AWS transparenter und zuverlässiger erklären zu können, als dies mit den herkömmlichen Methoden der digitalen Forensik möglich ist. Dabei betrachtet die Unternehmensforensik Prozesse sowie deren Umsetzung in den AWS des Unternehmens. Die Methoden sollen zudem zur genaueren Bestimmung der Ursache von Spuren (origin of evidence) sowie zur Identifikation weiterer und ergänzender digitaler Spuren genutzt werden können. Durch die Implementierung und Umsetzung der Prozesse mittels IS bzw. AWS müssen jedoch zur konkreten Identifikation, Sicherung, Analyse und Präsentation von digitalen Spuren auch die *tieferen* technischen Schichten der Systeme mit einbezogen werden.

Im nächsten Abschnitt werden nun die Prozesse detailliert betrachtet und eine formale Definition von Prozessen für die Unternehmensforensik entwickelt.

6.2 Formale Definition eines Prozesses

Prozesse bestehen, wie in Abschnitt 3.2 bereits angesprochen aus unterschiedlichen Komponenten und Prozessmodelle sind je nach Anwendungszweck unterschiedlich detailliert [CKO92, BRU00]. Diese Unterschiede finden sich auch in formalen Definitionen von Prozessen wieder, die je nach Intention unterschiedlich fein, im Sinne der im Formalismus enthaltenen Komponenten definiert werden [SWM10, SDMW10, SRWN12, YV14]. In [SDMW10] und in [SRWN12] wird ein Prozessmodell z.B. konkret definiert als

Tupel, bestehend aus einer Menge an Aktivitäten, einer Menge an Gateways sowie einer Menge an Pfaden, die die Aktivitäten und die Gateways zu einem Graphen verbinden. In [SRWN12] ist noch zusätzlich die Art des Gateways im Formalismus definiert. In [SWM10] wird dagegen ein detaillierterer Formalismus verwendet, der neben den Aktivitäten, Gateways und Flussbeziehungen z.B. auch noch die Start- und Endaktivitäten als separate Mengen definiert. In [YV14] wird ebenfalls ein erweiterter Formalismus verwendet, der speziell für BPMN Prozessmodelle entworfen wurde und dementsprechend z.B. auch noch eine Menge an Ereignissen enthält.

6.2.1 Aktivitäten, Gateways und Pfade

Allen in der obigen Einführung zu diesem Abschnitt 6.2 bereits angesprochenen formalen Definitionen gemein ist die Übereinstimmung, dass ein Prozess aus einer Menge von Aktivitäten, einer Menge von Gateways sowie einem festgelegten Ablauf, der die einzelnen Aktivitäten und Gateways mittels Pfaden zu einem Graphen verbindet, besteht [SZS04, SWM10, SDMW10, AWS11, SRWN12, YV14]. Aus diesem Grund wird für die formale Definition eines Prozesses in dieser Arbeit als Basis die Definition aus [SRWN12] genutzt. Ein Prozess ist demnach ein Tupel $P = (A, G, F, t)$ [SRWN12] mit:

Aktivitäten als endliche nichtleere Menge von Aktivitäten $A = \{a_1, a_2, .., a_n\}$.

Gateways als endliche Menge von Gateways $G = \{g_1, g_2, .., g_n\}$.

Knoten als endliche nichtleere Menge von Konten $N = A \cup G$ mit $A \cap G = \{\varnothing\}$.

Pfade $F \subseteq N \times N$ sind die Pfade, sodass (N, F) ein verbundener Graph ist.

Zuordnung $t : G \to \{and, xor\}$, die jedem Gateway einen Typ zuordnet.

6.2.2 Subjekte und Rollen

Da bei unternehmensforensischen Untersuchungen, wie in Abschnitt 6.1 erläutert die Zuordnung der Aufgaben zu den Aufgabenträgern bekannt sein muss und wie in Abschnitt 4.2.3.1 gefordert, das Identitätsmanagement in eine Untersuchung mit einbezogen werden soll, wird das im vorigen Abschnitt 6.2.1 definierte Modell erweitert. Nach [CKO92, BV96] und [FS13, S. 200] sind den einzelnen Aktivitäten des Prozesses Subjekte bzw. Ressourcen zugeordnet. Die Ressourcen entsprechen den maschinellen oder personellen Aufgabenträgern, die eine Aktivität ausführen, z.B. ein Sachbearbeiter, ein E-Mailprogramm, ein Anwendungsprogramm oder ein Datenbanksystem [BV96]. Die Ausführung ist zudem an Rollen geknüpft, die die Zuständigkeiten in Form von Rechten und Pflichten der Ressourcen für Aktivitäten festlegen [CKO92, HH06]. Die Subjekte und die Rollen werden daher definiert als:

Subjekte sind eine endliche nichtleere Menge von Subjekten S in Form von personellen oder maschinellen Aufgabenträgern.

Rollen beschreiben die endliche nichtleere Menge R an Rechten und Pflichten, die den jeweiligen Ressourcen in S auferlegt sind, inkl. etwaiger Einschränkungen.

Die Menge R ist im Detail definiert als Menge an Tupeln $r = (A(r), S(r), RP)$. $A(r) \subseteq A$ bezeichnet eine endliche nichtleere Menge an Aktivitäten, die durch die in $S(r)$ enthaltenen Subjekte ausgeführt werden. $S(r) \subseteq S$ ist eine endliche nichtleere Menge von Subjekten, die der Rolle zugeordnet sind und RP bezeichnet eine endliche Menge an Rechten, Richtlinien und Pflichten bezüglich der Beziehung zwischen $S(r)$ und $A(r)$, wie z.B. der Pflicht für ein $s \in S(r)$ eine bestimmte $a \in A(r)$ in einer bestimmten Zeit auszuführen oder das Aufgabentrennungsprinzip sowie das Vier-Augen-Prinzip, dass die Menge $S(r)$ bezüglich der Ausführung von Aufgaben aus $A(r)$ unter Umständen entsprechend einschränken würde.

6.2.3 Inputs und Outputs

Eine Prozessdefinition enthält zudem Inputs und Outputs [Dav93, S. 5]. Für die Unternehmensforensik sind dabei, wie in Abschnitt 6.1 erläutert, die Teilmengen an digitalen Daten interessant, da sie die von den einzelnen Aktivitäten benötigten oder erzeugten digitalen Daten beschreiben. In [SZS04] und [AWS11] werden speziell für die Analyse von Geschäftsprozessen bzw. Workflows detaillierte Formalismen definiert, die auch Inputs und Outputs bzw. die im Prozess verarbeiteten Datenelemente enthalten. Die digitalen Inputs und Outputs werden nach [AWS11] definiert als $D_i \subseteq D$ bzw. $D_o \subseteq D$.

Jedes Element $d \in D$ ist eine Variablen-Wertzuweisung $d = [v = w]$ im Sinne des in Abschnitt 2.4 beschriebenen Modells von Dewald [Dew12]. Da die Bezeichner d bzw. D bereits für die digitalen Datenelemente und die Menge aller digitalen Daten benutzt wurden, wird anstelle von d bzw. D zur Definition der Domäne im Modell aus Abschnitt 2.4 hier w bzw. W verwendet. Analog zum Modell in Abschnitt 2.4 wird aber ebenfalls für jede der Variablen $v \in V$ festgelegt, welche Art der Werte sie speichern kann. Jede $v \in V$ repräsentiert wiederum einen reellen Speicherort im AWS. Beispiele dafür sind ein Eintrag in einer Datei, eine neue Tabellenzeile in einer Datenbanktabelle, eine Schemadefinition in einer Datenbank, ein Objekt im Sinne einer konkreten Instanz einer Klasse in einer Anwendung oder auch nur die Belegung einer Hauptspeicherregion [Dew12, S. 73]. Eine einzelne Variable $v \in V$ kann sowohl einen Container repräsentieren, der einen bestimmten Wert speichern kann, z.B. eine Tabellenzeile in einer Datenbank, als auch nur ein Attribut eines solchen Containers [Dew12, S. 73]. Die Menge aller potentiell bei der Prozessausführung neu entstehenden Datenelemente $\mathcal{D}$ ist über die Gesamtmenge der möglichen Zustände aller an allen Prozessen beteiligten maschinellen Aufgabenträgern $\mathcal{R}$ festgelegt. Dementsprechend ist $D \subseteq \mathcal{D}$.

Für die einzelnen Aktivitäten des Prozesses gilt, dass $D_i(a) \subseteq D_i$ und $D_o(a) \subseteq D_o$ sind. Weiter wird die Menge $D_i(0) \subseteq D$ analog zum Formalismus in [SZS04] definiert als Menge aller Datenelemente, die außerhalb von P erzeugt werden. $D_i(0)$ enthält daher alle Eingabedaten von P, die bei der Betrachtung von P als Blackbox beobachtet werden könnten. Es gilt $D_i(0) = D_i \setminus (D_i \cap D_o)$. Es wird zudem die Annahme getroffen, dass keine Aktivität $a \in A$ Ausgabedaten erzeugt, die zugleich Teil von $D_i(0)$ sind. Es gilt $\forall D_o(a) \subseteq D_o : D_o(a) \cap D_i(0) = \{\varnothing\}$, da $D_i(0)$ durch $D_i(0) = D_i \setminus (D_i \cap D_o)$ ansonsten nicht vollständig wäre.

Auch die globalen Ausgabedaten von P werden in [SZS04] definiert. In dieser Arbeit wird die endliche Menge an Ausgabedaten analog definiert als $D_o(0)$, wobei $D_o(0) = D_o$. Durch Unterschiede bei der Prozessausführung oder durch die Eliminierung von Ausgabedaten im Laufe der Prozessausführung kann es dazu kommen, dass nicht alle Ausgabedaten am Ende des Prozesses vorhanden sind. Daher kann für jede $v \in V$ auch der Nullwert ($NULL$) definiert werden, um diese Sachverhalte auszudrücken.

6.2.4 Gesamtdefinition

Fasst man die in den Abschnitten 6.2.1 - 6.2.3 beschriebenen Komponenten zusammen, so ist ein Prozess P definiert als $P = (A, G, F, t, D, S, R)$. Neben der Betrachtung eines Prozesses ist für die Unternehmensforensik aber auch die Gesamtheit der Prozesse eines Unternehmens interessant. Die Menge aller Prozesse wird daher abschließend definiert als GP mit $P \in GP$.

Nachdem nun die einzelnen Komponenten von P sowie die Gesamtheit aller Prozesse eines Unternehmens GP ausführlich definiert und beschrieben wurden, wird nun in den folgenden Abschnitten auf die Nutzung von $P = (A, G, F, t, D, S, R)$ und GP in der Unternehmensforensik eingegangen.

6.3 Die digitale Spur in der Unternehmensforensik

Um Prozessmodelle in unternehmensforensischen Untersuchungen nutzen zu können, müssen nun zunächst die Entstehung von digitalen Spuren sowie die Definition von digitalen Spuren in diesem Kontext genauer geklärt werden. Abbildung 6.2 zeigt beispielhaft einen Prozess P in Form eines BPMN Prozessmodells. P beinhaltet insgesamt vier Aktivitäten. Demnach ist $A = \{a_1, a_2, a_3, a_4\}$. Die Eingabedaten sind $D_i = \{i_1\}$ und die Ausgabedaten $D_o = \{o_1, o_2, o_3, o_4\}$. Wird nun der Prozess ausgeführt, so werden entweder a_1, a_2 und a_3 ausgeführt oder a_1 und a_4, da der exklusive Gateway die parallele Ausführung von a_2 und a_3 mit a_4 verhindert. Die Ausgabedaten des Prozesses sind daher entweder $\{o_1, o_2, o_3\}$ oder $\{o_1, o_4\}$. Es stellt sich nun die Frage, wie mit dem Spurenbegriff in diesem Kontext umzugehen ist, da ein Prozessmodell offensichtlich mehrere Möglichkeiten hinsichtlich der bei der Ausführung tatsächlich entstehenden Spuren besitzt.

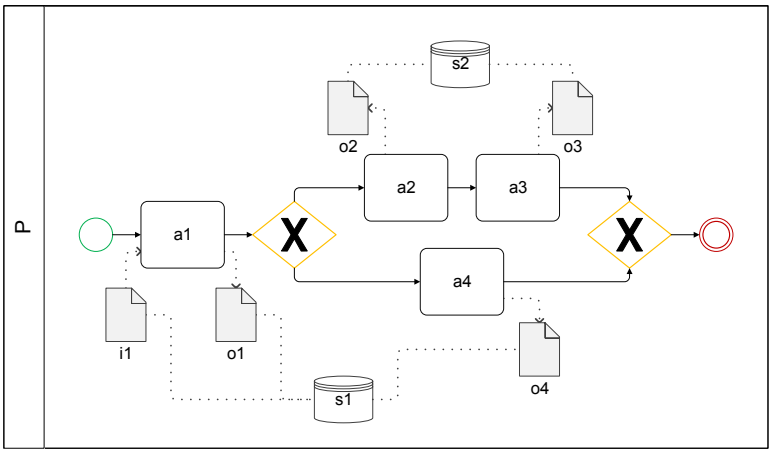


Abbildung 6.2 – Abstrakter Beispielprozess P

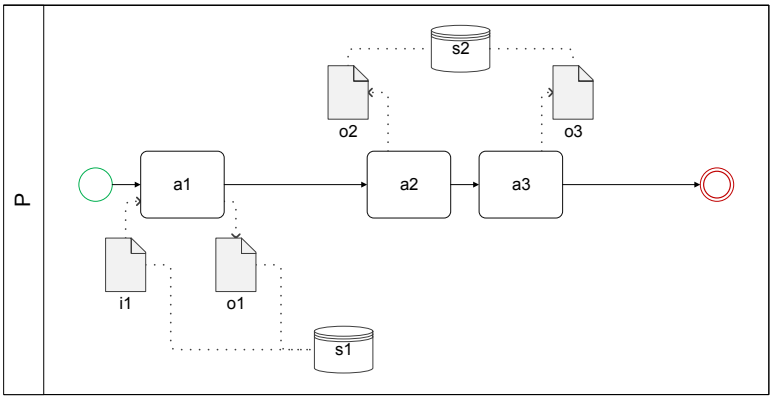
Der folgende Abschnitt 6.3.1 beleuchtet die Frage, was eine digitale Spur im Kontext von Prozessbeschreibungen bedeutet und definiert die Spuren von Prozessen. In Abschnitt 6.3.2 wird dann die teilweise Ausführung des Prozesses bzw. die Spuren einzelner Prozessaktivitäten betrachtet und in Abschnitt 6.3.3 werden die Spuren des Prozesses schließlich mit den Spuren eines Systems aus dem in Abschnitt 2.4 vorgestellten Modell nach Dewald [Dew12] verglichen.

6.3.1 Spuren eines Prozesses

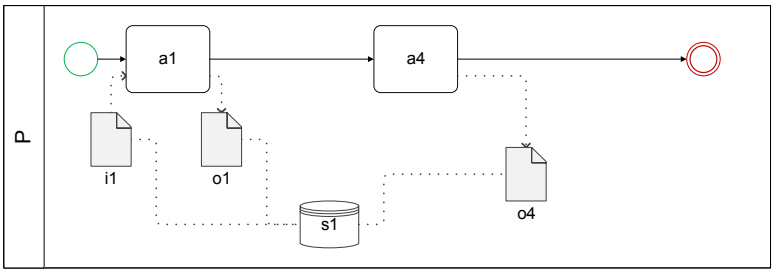
Prozesse bzw. Prozessmodelle legen die Regeln fest, wie ein Prozess in Form einer Instanz ausgeführt werden kann [HMN15, S. 65]. Die tatsächlichen digitalen Spuren entstehen daher durch eine Menge an Prozessinstanzen IN, die durch den Prozess beschrieben sind [SRWN12]. Bedingt durch verschiedene Start- und Endaktivitäten, die exklusiven *xor* Gateways $g \in G$ und die Pfade können in den einzelnen Instanzen eines Prozesses $inst(P) \in IN$ völlig unterschiedliche Aktivitäten ausgeführt werden. Die Unterschiede ergeben sich in der Regel durch Unterschiede bei den Eingabedaten $d \in D_i$, da die einzelnen Aktivitäten $a \in A$ sowie die Gateways $g \in G$ normalerweise ein deterministisches Verhalten aufweisen und deren Abfolge über die Pfade eindeutig geregelt ist.

Durch die Unterschiede bei der Prozessausführung entsteht unter Umständen auch nur ein Teil der Ausgabedaten D_o von P. Abbildung 6.3 verdeutlicht dies. Während durch den Prozessablauf in Abbildung 6.3(a) die Spurenmenge $E(inst(P)) = \{o_1, o_2, o_3\}$ entsteht, entstehen durch den in Abbildung 6.3(b) dargestellten Ablauf die Spuren $E(inst(P)) = \{o_1, o_4\}$. Die Menge der digitalen Spuren eines Prozesses P ist daher definiert als:

Die Menge der digitalen Spuren $E(P)$ eines Prozesses P ist definiert als Menge an Teilmengen $E(inst(P)) \in E(P)$ mit $E(inst(P)) \subseteq D_o$. Jede Teilmenge $E(inst(P)) \in E(P)$ entspricht dabei dem Ergebnis einer über die Eingabedaten, die Gateways und die Pfade festgelegten Sequenz an tatsächlich ausgeführten Aktivitäten $A(inst(P))$ einer Prozessinstanz $inst(P) \in IN$ und der dadurch definierten Menge an digitalen Ausgabedaten $D_o(inst(P))$, die durch die in der Instanz enthaltenen Aktivitäten erstellt werden.



(a)



(b)

Abbildung 6.3 – Mögliche Instanzen des Beispielprozesses P

Wenn bei einer unternehmensforensischen Untersuchung die Menge $E(inst(P))$, bestehend aus Datenelementen $d \in D_o(inst(P))$, sichergestellt wird, so kann deren Entstehung über P erklärt werden. Um von einer Menge $E(inst(P))$ tatsächlich auf P schließen zu können, muss allerdings zudem die Gesamtheit aller Prozesse GP mit $P \in GP$ bekannt sein. Weiter muss für die Feststellung gelten, dass $E(inst(P))$ nicht gleichzeitig von einer anderen Instanz eines anderen Prozesses $P' \in GP$ erstellt wird.

Die Gesamtheit aller durch andere Prozesse $GP' = GP \setminus P$ hervorgerufenen Spuren wird daher zunächst definiert als:

$$ME(GP') = \bigcup_{P \in GP'} \bigcup_{d \in D_o} d \tag{6.1}$$

Dementsprechend werden die charakteristischen Spuren von P bezüglich GP' in Analogie zum Modell aus Abschnitt 2.4 definiert als:

$$CE(P,GP') = \bigcup_{E(inst(P)) \in E(P)} E(inst(P)) \setminus ME(GP') \tag{6.2}$$

Die gemeinsamen charakteristischen Spuren $CCE(GP',GP'')$ einer Menge an Prozessen GP' bezüglich einer anderen Menge an Prozessen GP'', mit $GP' \subseteq GP$ und $GP'' \subseteq GP$, sind analog zum Modell aus Abschnitt 2.4 definiert als Menge aller charakteristischen Spuren, die die Prozesse $P \in GP'$ bezüglich GP'' gemeinsam haben.

Im Modell von Dewald [Dew12] aus Abschnitt 2.4 werden zusätzlich die Kontraspuren definiert. Auch diese lassen sich analog auf die Prozesse übertragen. Dabei sind die Kontraspuren $XE(P)$ eines Prozesses die Variablen $v \in V$, die durch die Datenelemente des Prozesses $P \in GP$ über $d \in D_o$ bestimmt sind. Den Variablen sind aber andere Werte zugewiesen als die, die den Variablen durch die Ausführung von P zugewiesen werden. Weiter entsprechen die charakteristischen Kontraspuren $CXE(P,GP')$ der Menge der Kontraspuren $XE(P)$ ohne die Menge an Variablen-Wertzuweisungen, die durch die Datenelemente anderer Prozesse $P' \in GP'$ mit $GP' = GP \setminus P$ bestimmt sind.

Auch die gemeinsamen charakteristischen Kontraspuren lassen sich übertragen. Dabei sind die gemeinsamen charakteristischen Kontraspuren von GP' all jene charakteristischen Kontraspuren, die alle Prozesse $P \in GP'$ bezüglich der Menge an Prozessesn GP'' gemeinsam haben. Durch die gemeinsamen charakteristischen Kontraspuren $CCXE(GP',GP'')$ einer Menge von Prozessen GP' kann die Ausführung dieser Menge an Prozessen GP', mit $GP' \subseteq GP$ und $GP'' \subseteq GP$, ausgeschlossen werden.

Neben der Betrachtung der Kontraspuren eines gesamten Prozesses können auch Kontraspuren auf Ebene der Instanzen eines Prozesses betrachtet werden. Dabei sind die Kontraspuren einer Instanz $XE(inst(P))$ all jene Variablen $v \in V$, die über die Datenelemente $d \in E(inst(P))$ bestimmt sind, wobei die Werte der Variablen nicht den durch die Datenelemente der Instanz bestimmten Werte entsprechen. Die charakteristischen Kontraspuren $CXE(inst(P),IN')$ entsprechen der Menge der Kontraspuren ohne die Variablen-Wertzuweisungen, die durch die Datenelemente anderer Instanzen $IN' = IN \setminus inst(P)$ des Prozesses definiert sind. Weiter können analog zu den Prozessen unter Umständen auch ganze Instanzmengen IN' des Prozesses durch ihre gemeinsamen charakteristischen Kontraspuren $CCXE(IN',IN'')$ ausgeschlossen werden. Die Menge der gemeinsamen charakteristischen Kontraspuren von IN' ist die Menge der charakteristischen Kontraspuren, die alle in der Menge $IN' \subseteq IN$ enthaltenen Instanzen bezüglich der Menge der Instanzen in $IN'' \subseteq IN$ gemeinsam haben.

6.3.2 Spuren von Teilprozessen und einzelnen Aktivitäten

Die Definition der Spurenmengen von P aus dem vorherigen Abschnitt 6.3.1 trifft implizit die Annahme, dass alle Prozessinstanzen immer bis zum Ende durchlaufen. In der Praxis kann es aber vorkommen, dass Prozesse während einer digitalen forensischen Untersuchung gerade erst ausgeführt werden, in der Vergangenheit abgebrochen oder einfach nicht wie definiert ausgeführt wurden oder Teile der Spuren bereits durch andere Prozesse überschrieben oder entfernt worden sind. In diesen Fällen sind unter Umständen nur mehr bzw. erst Teile der Spuren aus $E(inst(P)) \subseteq E(P)$ nachweisbar. Aus diesem Grund werden nun die Spuren von teilweise ausgeführten Prozessen bzw. einzelnen Aktivitäten genauer betrachtet.

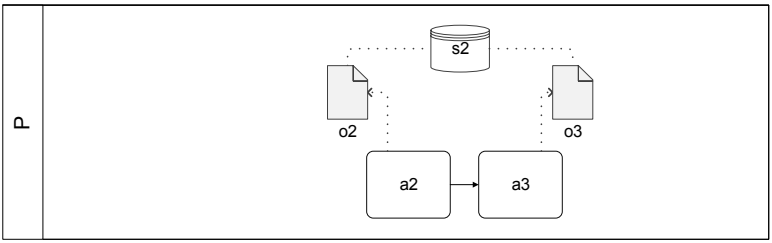


Abbildung 6.4 – Ausschnitt des Beispielprozesses P

Abbildung 6.4 zeigt einen Ausschnitt aus dem in Abbildung 6.2 dargestellten Beispielprozess. Dabei sind in Abbildung 6.4 nur die Aktivitäten a_2 und a_3 enthalten. Wie in Abschnitt 6.2.3 beschrieben, hat jede Aktivität $a \in A$ als Teil einer Prozessdefinition eine festgelegte endliche Menge an Outputs $D_o(a)$. Für a_2 ist diese Menge $D_o(a_2) = \{o_2\}$ und für a_3 ist sie $D_o(a_3) = \{o_3\}$. Nach dem Modell aus Abschnitt 6.2 werden von einer Aktivität keine weiteren digitalen Outputs erzeugt. Für einzelne Aktivitäten $a \in A$ ist die Menge der von ihr erzeugten digitalen Spuren $E(a)$ daher analog zu den Spuren einer Prozessinstanz $E(inst(P))$ definiert als $E(a) = D_o(a)$. Dementsprechend ist $E(a_2) = D_o(a_2) = \{o_2\}$ und $E(a_3) = D_o(a_3) = \{o_3\}$.

Teilweise ausgeführte Prozesse können als Sequenzen von einzelnen Aktivitäten, wie in Abbildung 6.4 dargestellt betrachtet werden. Die gemeinsamen Spuren einer solchen Sequenz an Aktivitäten bzw. einer Menge von $a \in A$ sind dabei die Vereinigung der Spurenmengen der Einzelaktivitäten. Für die Aktivitäten a_2 und a_3 sind die gemeinsamen Spuren daher $ME(\{a_2, a_3\}) = \{o_2, o_3\}$. Allgemein sind die gemeinsamen Spuren einer Menge an Aktivitäten A daher definiert als:

$$ME(A) = \bigcup_{a \in A} \bigcup_{d \in D_o(a)} d \tag{6.3}$$

Um nun bei einer digitalen forensischen Untersuchung auf die Ausführung einzelner Aktivitäten $a \in A$ schließen zu können, muss die Menge an charakteristischen Spuren

von a bezüglich der digitalen Spuren aller anderen Aktivitäten $A' = A \setminus a$ bekannt sein. Die charakteristischen Spuren einer Aktivität a bezüglich A' sind definiert als:

$$CE(a, A') = E(a) \setminus ME(A') \tag{6.4}$$

Abbildung 6.5 zeigt den Prozess P'. Anders als bei P in Abbildung 6.2 hat Aktivität a_4 hier die Spurenmenge $E(a_4) = \{o_2, o_4\}$. Aufgrund der obigen Definition ergibt sich für a_4 bezüglich $A' = \{a_1, a_2, a_3\}$ die charakteristische Menge an Spuren $CE(a_4, A') = \{o_2, o_4\} \setminus \{o_1, o_2, o_3\} = \{o_4\}$. Für a_2 mit $A' = \{a_1, a_3, a_4\}$ ist die Menge der charakteristischen Spuren $CE(a_2, A')$ dagegen $CE(a_2, A') = \{o_2\} \setminus \{o_1, o_2, o_3, o_4\} = \{\varnothing\}$.

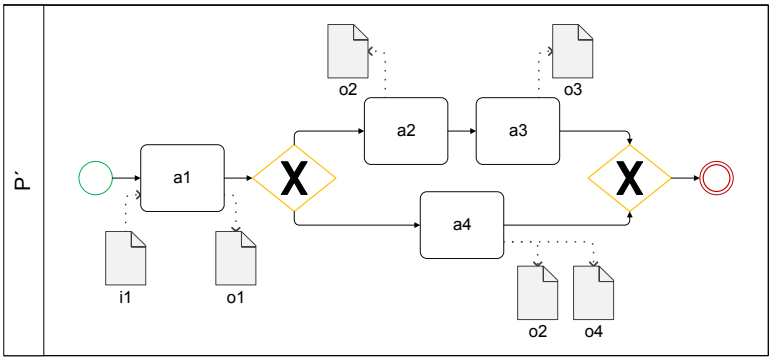


Abbildung 6.5 – Abstrakter Beispielprozess P'

Auch die von Dewald [Dew12] in seinem in Abschnitt 2.4 vorgestellten Modell definierten gemeinsamen charakteristischen Spuren von Aktionen im System S sind auf die Aktivitäten von P übertragbar. Die gemeinsamen charakteristischen Spuren einer Menge von Aktivitäten $A' \subseteq A$ bezüglich einer anderen Menge von Aktivitäten $A'' \subseteq A$ mit $A' \cap A'' = \{\varnothing\}$ sind dementsprechend:

$$CCE(A', A'') = \bigcup_{a \in A'} CE(a, A'') \tag{6.5}$$

Analog zu den digitalen Spuren von Prozessen können auch für die digitalen Spuren von Teilprozessen bzw. von Aktivitäten die Kontraspuren definiert werden. Die Kontraspuren einer Aktivität $a \in A$ sind die Variablen $v \in V$, die durch seine Datenelemente $D_o(a)$ bestimmt sind. Dabei sind den $v \in V$ jedoch andere Werte zugewiesen als die $w \in W$, die den Variablen durch die Erzeugung von $d \in D_o(a)$ bei der Ausführung von a zugewiesen werden.

Die Menge der charakteristischen Kontraspuren $CXE(a, A')$ ist eine um die Variablen-Wertzuweisungen, die über die Datenelemente einer Menge anderer Aktivitäten $A' \subseteq A$ mit $a \notin A'$ bestimmt sind, verkürzte Menge an Kontraspuren. Gibt es für eine Menge an Aktivitäten A' keine charakteristischen Kontraspuren, so kann unter Umständen

durch die gemeinsamen charakteristischen Kontraspuren dieser Menge an Aktivitäten $CCXE(A', A'')$ aber dennoch die Ausführung aller $a \in A'$ ausgeschlossen werden. Die gemeinsamen charakteristischen Kontraspuren einer Menge A' sind alle charakteristischen Kontraspuren, die die Aktivitäten in A' bezüglich der Aktivitäten in A'' gemeinsam haben, wobei $A' \subseteq A$ und $A'' \subseteq A$.

Mithilfe der charakteristischen Spuren und Kontraspuren von Aktivitäten ist es nun theoretisch möglich, auf Basis einer Teilmenge der Spuren eines Prozesses die einzeln ausgeführten Aktivitäten zu identifizieren bzw. deren Ausführung abzulehnen. Im folgenden Abschnitt werden nun die Spuren des Prozesses bzw. die Spuren von Teilen eines Prozesses und einzelnen Aktivitäten mit den digitalen Spuren aus dem Modell von Dewald [Dew12] verglichen.

6.3.3 Unternehmensforensische Spuren im Vergleich

Durch $E(P)$ bzw. $E(a)$ und $ME(A)$ sind die zu erwartenden digitalen Spuren bei einer unternehmensforensischen Untersuchung sehr genau bestimmt. Allerdings geben Prozesse nur einen Teil der tatsächlich entstehenden digitalen Spuren preis, denn in der Regel finden sich nur die für den Prozess relevanten Daten in der Prozessbeschreibung. Abbildung 6.6 stellt diesen Aspekt dar. Die Anwendungssoftwareebene ist als Teil der Systemebene dargestellt. Dabei wird deutlich, dass die Menge der Aktionen Σ der jeweiligen Systeme $S = (V, \Sigma, q_0)$ deutlich größer ist als die Menge an Aktionen, die von der Anwendungssoftware des AWS genutzt und von der Aufgaben- respektive Prozessebene über die maschinellen Aufgabenträger referenziert sind. Die $\Sigma(AWS) \subseteq \Sigma$ entsprechen daher in der Regel nur einem Teil der vom Basissystem S bereitgestellten bzw. dort vorhandenen Aktionen. Der Prozess P nutzt durch seine Aktivitäten A unter Umständen wiederum nur einen Teil der dann vom AWS bereitgestellten Aktionen. Aus diesem Grund sind auch die Spurenmengen $E(inst(P)) \in E(P)$, die durch Prozessinstanzen $inst(P) \in IN$ entstehen, jeweils nur Teilmengen der Spuren des Systems S. Es gilt:

$$(ME(GP) \cap ME(\Sigma)) \subseteq ME(\Sigma) \tag{6.6}$$

Durch die obige Definition ergibt sich zudem eine weitere Aussage: Die Spuren der Prozesse müssen nicht zwangsweise nur in einem System S entstehen. Da in einem Unternehmen eine Reihe von AWS für die Abarbeitung der Prozesse vorhanden sein können und diese unter Umständen auch keine direkte Verbindung besitzen, wodurch sich ein großes Gesamtsystem S ergeben würde, kann es sein, dass sich in unterschiedlichen S Spuren eines Prozesses finden. In der Gesamtheit lassen sich diese Spuren aber über die Prozessbeschreibung bestimmen. Abbildung 6.6 verdeutlicht dies, indem zwei getrennte Systeme auf der Systemebene dargestellt sind. Während zwischen den beiden Systemen offensichtlich keine direkte Verbindung besteht, werden beide dennoch vom Prozess auf der Aufgabenebene referenziert und als maschinelle

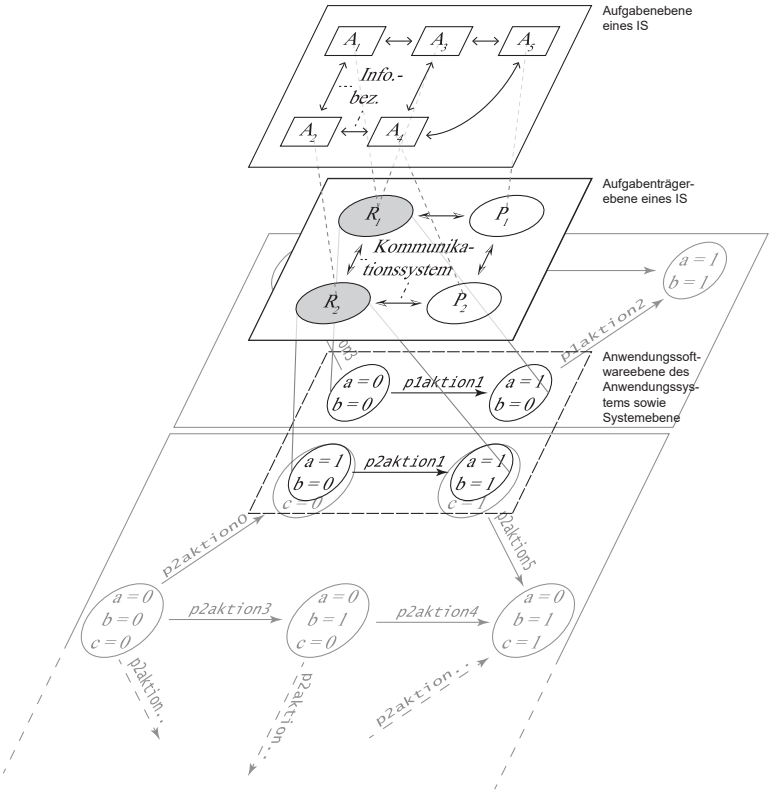


Abbildung 6.6 – Funktionen zur Umsetzung eines Prozesses im Vergleich zu den theoretisch möglichen Funktionen des Anwendungs- bzw. Basissystems

Aufgabenträger zu dessen Ausführung genutzt. Auf Ebene der Aufgaben wie auch auf Ebene der Aufgabenträger finden sich Verbindungen zwischen den beiden Systemen. Die Systeme selbst haben allerdings keine direkte Verbindung.

Neben dem Unterschied bei den durch die jeweiligen Formalismen erklärten digitalen Spuren ist eine Prozessbeschreibung, wie im Abschnitt 6.3.1 bereits erläutert, aber nur das Regelwerk, das festlegt, wie ein Prozess in Form einer Instanz ausgeführt werden kann [HMN15, S. 65]. Anders als zum Modell des Systems $S = (V, \Sigma, q_0)$ bei dem alle Zustände Q und Zustandsübergänge durch Σ vorab bekannt sind, kann dies bei Prozessen nicht in dieser Genauigkeit vorab bestimmt werden. Die Eingabedaten D_i, die maßgeblich den Prozessablauf einer konkreten Instanz bestimmen, ändern sich unter Umständen sogar im Laufe der Ausführung eines Prozesses [HS15]. Dadurch können

sich dann auch der Prozessablauf und die Ausgabedaten ändern. Eine Vorausplanung im Sinne einer Bestimmung aller zu erwartenden Zustände und Spuren ist also anders als beim endlichen Automaten nicht in dieser Form möglich.

6.4 Zusammenfassung

In diesem Kapitel wurden die Spuren, die bei der Ausführung einer Prozessinstanz entstehen, formal beschrieben und definiert. Dadurch lassen sich nun ausgehend von Prozessbeschreibungen die zu erwartenden digitalen Spuren bestimmen. Weiter ist durch den Prozess das *normale* Verhalten des AWS festgehalten. Unabhängige Sachverständige können nun von einer gemeinsamen Basis aus agieren und die Entstehung von digitalen Spuren (er)klären, was sonst für solch komplexe Umgebungen nur wenigen eingeweihten Personen möglich wäre und sich dadurch jedweder Überprüfbarkeit entziehen würde [Coh10]. Durch diese Vergrößerung der zum Assoziieren in der digitalen Forensik und besonders in der Unternehmensforensik vorhandenen Wissensbasis wurde auch die Abbildung 2.8 entsprechend erweitert. Abbildung 6.7 zeigt die Prozesse analog zu den Systemmodellen und den Ergebnissen aus einer DFA als Teil der Wissensbasis zur Herstellung von Assoziationen bei digitalen forensischen Untersuchungen.

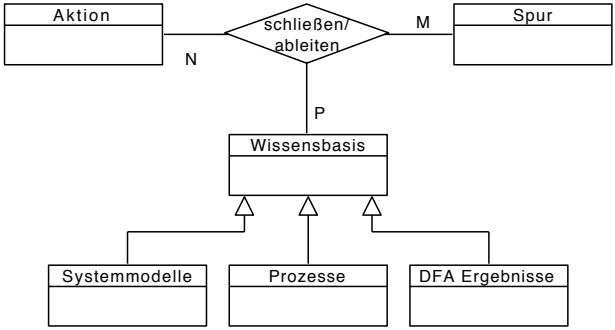


Abbildung 6.7 – Digitale Spuren, Prozesse und die Wissensbasis

Die Beschränkung der digitalen Spuren auf Prozesse hat aber auch Grenzen, was unter anderem anhand der Ausführungen in Abschnitt 6.3.3 deutlich wird. Da nur ein Teil der bei der Ausführung von Prozessaktivitäten tatsächlich über Systemaktivitäten entstehenden Spuren bestimmt und dann betrachtet werden kann, ist zur Aufklärung von Anomalien oder anderen maliziösen Zuständen des zugrunde liegenden Systems unter Umständen wieder ein Rückgriff auf die allgemeine digitale Forensik notwendig. Eine vertiefende Diskussion dieser Limitationen findet sich daher im Anschluss an die Vorstellung der Methodik für unternehmensforensische Untersuchungen am Ende des nächsten Kapitels.

KAPITEL 7

Methodik für unternehmensforensische Untersuchungen

In diesem Kapitel werden die Grundprinzipien der forensischen Wissenschaften aus Kapitel 2 und deren Anwendung im Kontext von AWS, auf Basis der Grundlagen zu den digitalen Spuren von Prozessen aus dem vorherigen Kapitel 6 betrachtet. Dazu wird eine Methodik zur Nutzung der Erkenntnisse aus Kapitel 6 zur Assoziation und schlussendlich zur Rekonstruktion bei digitalen forensischen Untersuchungen in Unternehmen vorgestellt.

Im nächsten Abschnitt 7.1 werden unternehmensforensische Untersuchungen, die notwendigen Voraussetzungen sowie die Methodik für unternehmensforensische Untersuchungen kurz im Überblick beschrieben. Anschließend wird in Abschnitt 7.2 die Anwendung der forensischen Prinzipien bei unternehmensforensischen Untersuchungen als zentraler Teil der Methodik detailliert betrachtet. In Abschnitt 7.3 werden dann die Grenzen der Methodik bei unternehmensforensischen Untersuchungen diskutiert. Die wesentlichen Ergebnisse des Kapitels werden in Abschnitt 7.4 abschließend kurz dargestellt.

7.1 Unternehmensforensische Untersuchungen

Die Unternehmensforensik, basierend auf den Grundlagen aus dem Kapitel 6 nutzt als zentralen Dreh- und Angelpunkt die Prozessbeschreibungen des Unternehmens. Das grundsätzliche Ziel ist, wie in der digitalen Forensik im Allgemeinen herauszufinden,

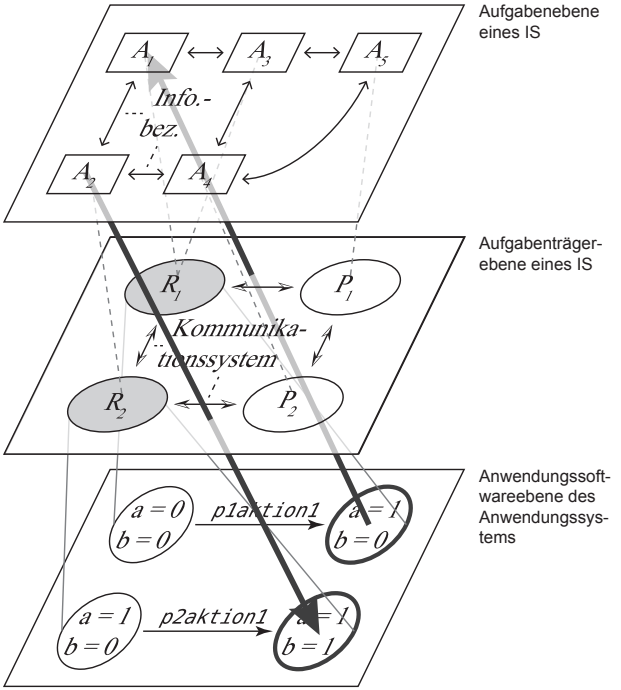


Abbildung 7.1 – Top-Down und Bottom-Up Vorgehen bei unternehmensforensischen Untersuchungen

welche digitalen Spuren existieren und was passiert ist [Car09]. Dabei kann die Herstellung von Assoziationen bzw. die Rekonstruktion in der Unternehmensforensik initial aus zwei Richtungen erfolgen: Vom Prozess zu den Daten (Top-Down) und von den Daten zum Prozess (Bottom-Up). Die beiden dunkelgrauen Pfeile von der Aufgabenebene des IS bzw. der Aktivität A_2 des Prozesses zum Zustand des AWS bzw. umgekehrt vom Zustand des Anwendungssystems zur Aktivität A_1 in Abbildung 7.1 verdeutlichen die beiden möglichen Ausgangspositionen einer unternehmensforensischen Untersuchung.

Da die Unternehmensforensik nach der Definition in Abschnitt 6.1 eine Teildisziplin der digitalen Forensik ist, sind unternehmensforensische Untersuchungen ebenfalls auf digitale Spuren beschränkt. Weiter stellen die Prozessbeschreibungen die Wissensbasis, im Sinne der Ausführungen aus Abschnitt 2.5, für das Ziehen von Schlüssen dar. Daher sind die digitalen Spuren auf die Daten, die im Rahmen der Ausführung von Prozessen wie in Kapitel 6 erläutert in Form digitaler Spuren des Prozesses bzw. seiner Instanz $E(inst(P)) \subseteq E(P)$ entstehen, beschränkt. Dies wird auch über Abbildung 7.1 deutlich

bei der, anders als in Abbildung 6.6 die über die Beschreibung des Prozesses hinausgehenden Datenelemente bzw. Variablen der Systeme sowie die Systeme selbst nicht weiter dargestellt sind. Mithilfe der Unternehmensforensik kann aber untersucht werden, ob sich die Entstehung der Daten respektive digitalen Spuren im Anwendungssystem über einen Prozess erklären lässt (Bottom-Up). Weiter kann geprüft werden, ob ein Prozess wie definiert ausgeführt wurde oder ob es Abweichungen von den definierten digitalen Outputs gibt (Top-Down).

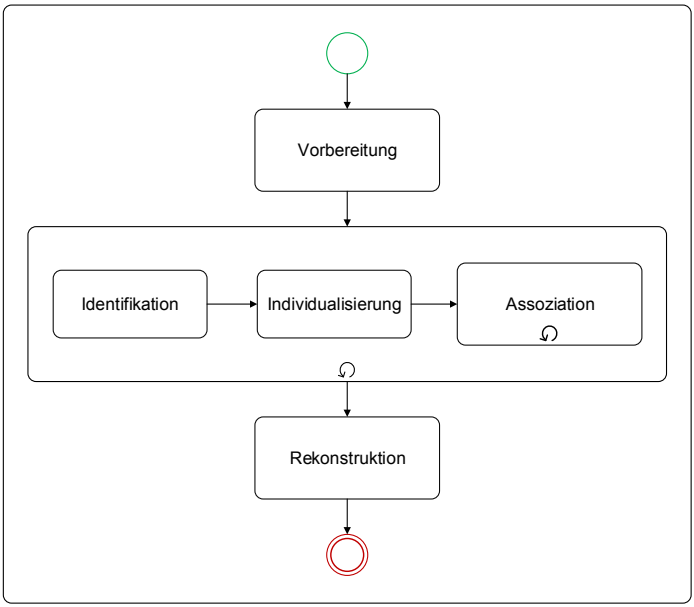


Abbildung 7.2 – Globales Vorgehensmodell für unternehmensforensische Untersuchungen

Eine unternehmensforensische Untersuchung folgt dann der in Abbildung 7.2 abstrakt dargestellten Schritte. Die Vorbereitungsphase dient dazu, die Wissensbasis in Form der im vorherigen Kapitel 6 definierten Mengen für jeden Prozess $P \in GP$ zu erstellen. Die notwendige Voraussetzung für die Unternehmensforensik ist daher, dass die Prozessbeschreibungen vorhanden sind. Wie in Abschnitt 3.2 festgestellt, ist es aber heute Standard, die Aufgaben in Unternehmen mittels Prozessen zu modellieren bzw. zu beschreiben. Dabei ist es prinzipiell unerheblich wie die Prozesse beschrieben sind, solange die Modelle oder Beschreibungen vollständig im Sinne der in Abschnitt 6.2 definierten Komponenten eines Prozesses sind und alle beschriebenen Komponenten enthalten. Durch den essentiellen Einfluss der Qualität der Prozessmodelle auf unternehmensforensische Untersuchungen werden diese sowie die sich dadurch ergebenden

Implikationen in Abschnitt 7.3.1 nochmals ausführlich diskutiert.

Nach der Erstellung der formalen Prozessmodelle folgt die Assoziation von digitalen Spuren und Prozessen durch die Anwendung der ausführlich in Abschnitt 2.2 beschriebenen Grundprinzipien der forensischen Wissenschaften. Da mehrere Prozesse abgelaufen sein können, ist eine Assoziation in der Analogie zu forensischen Untersuchungen im Allgemeinen ebenfalls mehrfach möglich. Aus diesem Grund ist in Abbildung 7.2 der Schritt *Assoziation* als Schleife dargestellt, wodurch eine mehrfache Ausführung ermöglicht wird. Assoziationen selbst basieren auf den in den verfeinerten Schritten *Identifikation* und *Individualisierung* bestimmten digitalen Spuren. Im Schritt *Rekonstruktion* werden diese mehrfachen Assoziationen, wie in Abschnitt 2.2 erläutert, schließlich in Zeit und Raum geordnet um, wie von Inman und Rudin [IR02] definiert, das *wo*, *wann* und *wie* zu beantworten. Die Schritte *Identifikation*, *Individualisierung* und *Assoziation* werden im folgenden Abschnitt 7.2 nochmals detaillierter dargestellt.

Durch die Assoziationen zwischen dem aktuellen (Speicher-)Zustand des AWS und den betrieblichen Aufgaben, respektive Prozessen, lässt sich die Entstehung dieses Zustandes des AWS bzw. die durch den Prozess beschriebenen Teile davon erklären. Die Erhebung des aktuellen (Speicher-)Zustands des AWS ist explizit nicht Teil der hier vorgestellten Methodik. Wie in Abschnitt 6.1 bereits festgestellt, sind zur Erhebung der digitalen Spuren aus AWS unter Umständen spezielle digitale forensische Werkzeuge notwendig, die auf das jeweils verwendete AWS zugeschnitten sind. Die in diesem Kapitel vorgestellte Methodik setzt voraus, dass die für die Sammlung und Akquise der digitalen Spuren notwendigen Hard- und Softwarekomponenten vorhanden sind und bei Bedarf entsprechend eingesetzt werden, um die digitalen Spuren forensisch sichern zu können. In Unternehmen kommen dazu z.B. Werkzeuge wie GRR zum Einsatz, mit deren Hilfe digitale Spuren live und ohne große Betriebsunterbrechung von den verteilten Systemen des Unternehmens in einem zentralen Repository gesammelt werden können [MC13, Cas13b].

7.2 Forensische Prinzipien in der Unternehmensforensik

Als Teildisziplin der digitalen Forensik folgt auch die Unternehmensforensik den in Abschnitt 2.2 beschriebenen Grundprinzipien forensischer Wissenschaften. Abbildung 7.3 zeigt ein auf den Grundprinzipien aufbauendes Vorgehensmodell für unternehmensforensische Assoziationen. Die beiden Startoptionen, Top-Down und Bottom-Up sind jeweils gekennzeichnet, wobei sich das Vorgehen der beiden Optionen nur geringfügig unterscheidet. Die Bottom-Up Analyse hat, wie in Abbildung 7.3 dargestellt, zwei Schritte mehr, nämlich die Identifikation von digitalen Daten als potentielle Spuren eines Prozesses im Schritt *Identifikation von Datenelementen* und der Aufstellung der Hypothese, dass dieser Prozess ausgeführt wurde im Schritt *Verdacht auf Ausführung von P*. Bei einer Top-Down Analyse ist die Vermutung, dass ein bestimmter Prozess ausgeführt wurde die Voraussetzung für den Start einer unternehmensforensischen

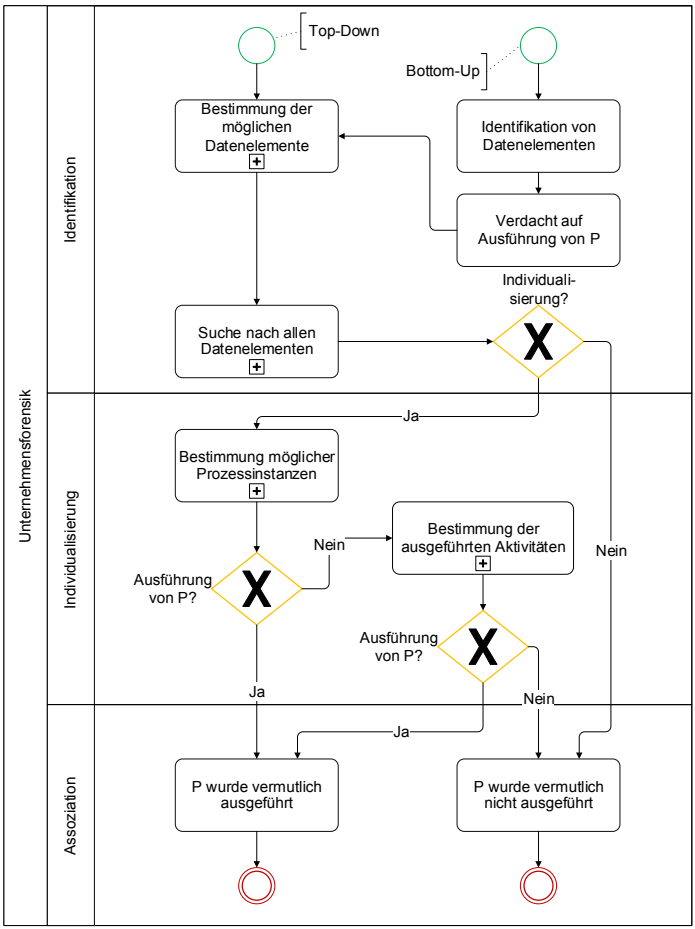


Abbildung 7.3 – Übersicht über das Vorgehen hin zur Assoziierung in der Unternehmensforensik

Untersuchung. Aus Sicht der klassischen digitalen Forensik ist aber besonders die Frage nach der Herkunft der Daten und den Umständen, wie diese entstanden sind, interessant [Car09],[Dew12, S. 69ff], was der Bottom-Up Analyse entspricht.

Nachdem bei einer Bottom-Up Analyse die Ausführung eines bestimmten Prozesses vermutet wurde, bzw. durch den Start einer Top-Down Untersuchung, werden zunächst die überhaupt möglichen Datenelemente des Prozesses im Schritt *Bestimmung der möglichen Datenelemente* bestimmt. Nach der Bestimmung der Datenelemente müssen diese im Rahmen des Schrittes *Suche nach allen Datenelementen* in den Datenspeichern,

der über die Rollen festgelegten maschinellen Aufgabenträger, respektive AWS für die in Frage kommenden Prozessinstanzen gesucht und als potentielle digitale Spuren identifiziert werden. Können keine Datenelemente gefunden werden, so wurde P vermutlich nicht ausgeführt und die entsprechende Untersuchungshypothese ist abzulehnen.

Können hinreichend viele Datenelemente identifiziert werden, so sind darauf aufbauend die potentiell ausgeführten Instanzen des Prozesses im Schritt *Bestimmung möglicher Prozessinstanzen* zu bestimmen. Können mithilfe der Datenelemente mögliche Instanzen identifiziert werden, so ist die Hypothese hinsichtlich der Ausführung des Prozesses unter Umständen anzunehmen. Im anderen Fall, wenn nicht mindestens eine mögliche Prozessinstanz bestimmt werden kann, sind mithilfe der Datenelemente Teilprozesse oder einzelne Aktivitäten des Prozesses im Schritt *Bestimmung der ausgeführten Aktivitäten* zu bestimmen. Können Aktivitäten oder Teilprozesse identifiziert werden, so ist unter Umständen die Hypothese hinsichtlich der Ausführung des Prozesses ebenfalls anzunehmen. Ansonsten muss die Hypothese final abgelehnt werden.

Die einzelnen Schritte hin zur Assoziation werden in den folgenden Abschnitten 7.2.1 - 7.2.3 nun noch im Detail beschrieben.

7.2.1 Identifikation

Das hauptsächliche Ziel der Identifikation im Rahmen unternehmensforensischer Untersuchungen ist die Bestimmung potentiell als digitale Spuren zu betrachtender digitaler Daten. Abbildung 7.4 zeigt das verfeinerte Vorgehensmodell für die Identifikation.

Bei einer Bottom-Up Untersuchung wird, wie im einleitenden Teil zu diesem Abschnitt 7.2 beschrieben, ausgehend von Daten im AWS schrittweise die Hypothese aufgestellt, dass die gefundenen Daten durch die Ausführung eines bestimmten Prozesses erklärt werden können. Die Daten können z.B. im Rahmen der Jahresabschlussprüfung durch eine Wirtschaftsprüfungsgesellschaft, durch ein Audit oder durch Zufall entdeckt werden. Wichtig ist, dass die Daten als potentielle Spuren einer Prozessausführung im ersten Schritt *Identifikation von Datenelementen* identifiziert werden und darauf aufbauend im zweiten Schritt *Verdacht auf Ausführung von P* ein Anfangsverdacht hinsichtlich der Ausführung des Prozesses entsteht. Wird dem Verdacht nachgegangen, so führt dies zum dritten Schritt *Bestimmung der möglichen Datenelemente* in dem die möglichen Datenelemente bestimmt werden. Dieser Schritt ist zugleich der erste Schritt einer Top-Down Untersuchung.

Die Bestimmung der möglichen Datenelemente ist in mehrere Unterschritte aufgeteilt. Zunächst muss im ersten Verfeinerungsschritt *Einschränken der Menge IN* geklärt werden, ob die Menge der möglichen Instanzen IN des Prozesses P eingeschränkt werden kann. Durch Fallspezifika, die Kenntnis von D_i oder die Identifikation bestimmter Datenelemente bei der Bottom-Up Untersuchung können unter Umständen bereits Prozessinstanzen $inst(P) \in IN$ ausgeschlossen werden, was die Menge an zu

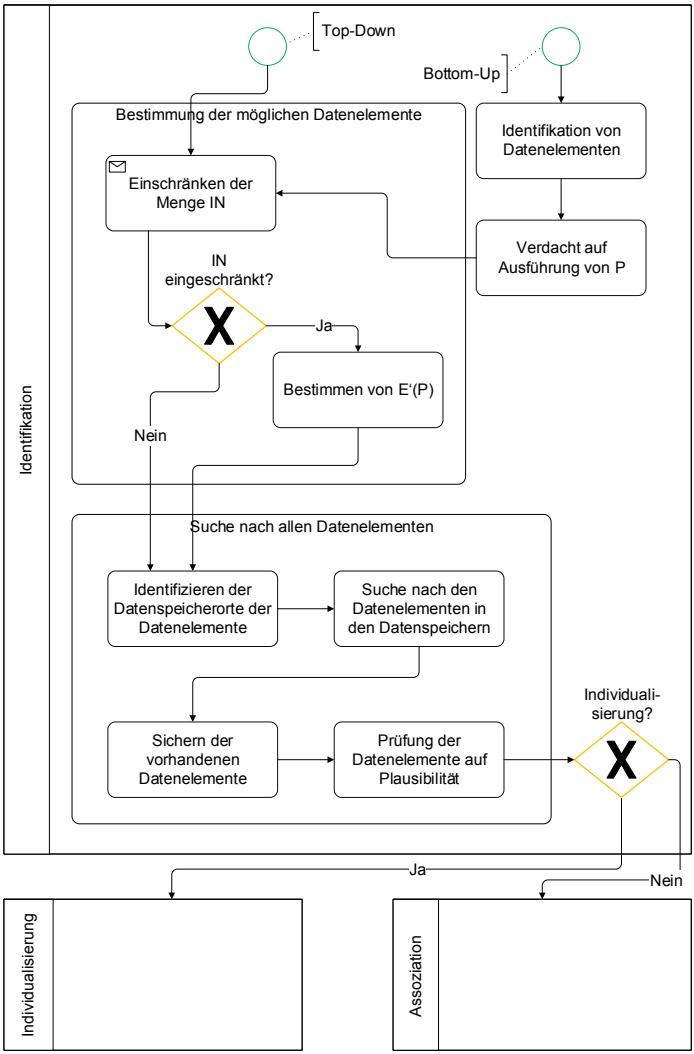


Abbildung 7.4 – Identifikation bei unternehmensforensischen Untersuchungen

untersuchenden Datenelementen einschränken und die Untersuchung dadurch potentiell beschleunigen würde. In diesem Schritt ist auch ein expliziter Austausch mit anderen, unter Umständen parallel laufenden digitalen forensischen Untersuchungen vorgesehen. Weiter ist auch der Einbezug von *analogen* Spuren wie z.B. von Papierausdrucken oder

handschriftlich unterschriebenen Prüfprotokollen für das Vier-Augen-Prinzip denkbar, um die Menge IN weiter einschränken zu können. Der Prozessschritt ist daher als annehmender Schritt im Sinne der verwendeten BPMN Notation gekennzeichnet.

Wenn Einschränkungen an der Menge IN vorgenommen werden können, so sind die Menge an verbliebenen Instanzen IN' sowie die, um die weggefallenen digitalen Spurenmengen der ausgeschlossenen Instanzen verkürzte Spurenmenge $E'(P)$ des Prozesses im Schritt *Bestimmen von* $E'(P)$ zu bestimmen. Sind keine Einschränkungen der Menge IN möglich, so ist $E'(P) = E(P)$ und $IN' = IN$.

Im Anschluss an die Bestimmung von $E'(P)$ müssen die darin enthaltenen Datenelemente zusammengefasst werden. Dazu wird im ersten verfeinerten Schritt *Identifizieren der Datenspeicherorte der Datenelemente* des Schrittes *Suche nach allen Datenelementen* aus Abbildung 7.4 zunächst die neue investigative Menge an Datenelementen $Invest(P)$ wie folgt erstellt:

$$Invest(P) = \bigcup_{inst(P) \in IN'} \bigcup_{d \in E(inst(P))} d \tag{7.1}$$

Nachdem alle potentiell als Spuren vorhandenen Datenelemente über die Menge $Invest(P)$ bekannt sind, können die tatsächlich in den AWS gespeicherten Datenelemente gesucht werden. Dazu werden im Schritt *Identifizieren der Datenspeicherorte der Datenelemente* zudem die tatsächlichen Speicherorte der Daten bestimmt. Die Bestimmung der Datenspeicherorte erfolgt konkret durch die Identifikation der AWS bzw. maschinellen Aufgabenträger über R.

Nach der Bestimmung der Datenspeicherorte können die Datenelemente im Schritt *Suche nach den Datenelementen in den Datenspeichern* in den Datenspeichern der AWS gesucht und im folgenden Schritt *Sichern der vorhandenen Datenelemente* forensisch gesichert werden, soweit diese vorhanden sind. Sollten die Daten nicht oder nicht mehr in den Datenspeichern des AWS auffindbar sein, müssen in jedem Fall auch Datensicherungen oder andere potentiell vorhandene Kopien der Daten des AWS mit durchsucht werden.

Im letzten verfeinerten Schritt *Prüfen der Datenelemente auf Plausibilität* müssen die identifizierten und gefundenen Daten bzw. $v \in V$ noch auf Plausibilität hinsichtlich ihres Wertebereichs $w \in W$ untersucht werden. Gibt es hier Unstimmigkeiten, so sind die entsprechenden Datenelemente unter Umständen zu verwerfen und die Menge $Invest(P)$ ist um diese sowie um die nicht auffindbaren Elemente zu kürzen, sodass am Ende der Identifikationsphase die Menge $Invest'(P)$ nur noch alle tatsächlich vorhandenen digitalen Daten $d \in D_o$ enthält. Gibt es grundsätzlich zu wenig oder gar keine digitalen Spuren bzw. finden sich in den Datenelementen Kontraspuren bei der Prüfung auf Plausibilität, so ist an dieser Stelle bereits ein Wechsel in die Assoziationsphase möglich oder gar notwendig.

7.2.2 Individualisierung

Nachdem alle tatsächlich vorhandenen digitalen Daten über $Invest'(P)$ bestimmt sind, folgt die Individualisierungsphase in der unternehmensforensischen Untersuchung, soweit die Untersuchung aufgrund der Entscheidung in der Identifikationsphase nicht vorzeitig in die Assoziationsphase gewechselt ist. Abbildung 7.5 zeigt alle Schritte der Individualisierungsphase im Detail.

Im ersten Schritt *Bestimmung möglicher Prozessinstanzen* bzw. im Rahmen dessen ersten Teilschritts *Suche nach möglichen Prozessinstanzen* muss die Menge $Invest'(P)$ mit den in $E'(P)$ enthaltenen Mengen an digitalen Spuren potentieller Instanzen verglichen werden. Entspricht eine Menge $E(inst(P)) \in E'(P)$ exakt der Menge $Invest(P)$, so ist über die charakteristischen Spuren sowie einer Bewertung der Datenelemente mithilfe der in Abschnitt 2.3.5 enthaltenen Tabelle 2.1 die Rechtssicherheit der Spuren zu bestimmen.

Neben der Bewertung der Datenelemente über Caseys [Cas11] Sicherheitskategorien digitaler Spuren aus Tabelle 2.1 ist bei der Bestimmung der Rechtssicherheit im Schritt *Bestimmung der Wahrscheinlichkeit einer Ausführung* auch wieder ein Austausch mit parallel ablaufenden forensischen Untersuchungen vorgesehen. Dadurch können z.B. physische Spuren des Prozesses mit in die Bewertung einbezogen werden.

Zudem können auch Medienbrüche im Prozess zur Bewertung der Rechtssicherheit der digitalen Spuren mit heran gezogen werden. Hierbei sind besonders die echten Medienbrüche interessant, bei denen ein menschlicher Aufgabenträger *Zwischenspeicher* und *Übertragungsweg* darstellt und Systeme physisch voneinander getrennt sind. Wenn dann z.B. eine Menge an digitalen Spuren $Invest'(P)$ über zwei solch physisch getrennte Systeme verteilt ist, so sind die Spuren potentiell als sicherer anzusehen, als wenn die Spuren zwar vorhanden sind, die Systeme aber eine direkte Verbindung aufweisen, da ein nur digital agierender Angreifer im System die Systemgrenze bei verbundenen Systemen leicht überwinden könnte. Bei physisch getrennten Systemen ist dies nicht so einfach möglich. Wie die Erläuterung zeigt, ist die Bewertung ähnlich wie bei den Kategorien nach Casey [Cas11] allerdings subjektiv und kann nur fallbezogen erfolgen.

Nach der Bewertung der digitalen Spuren und je nachdem, ob ausreichend viele sichere charakteristische digitale Spuren der potentiellen Instanz des Prozesses vorhanden sind, kann bereits an dieser Stelle ein Wechsel in die Assoziationsphase der Untersuchung erfolgen.

Wenn die Menge $Invest'(P)$ im Vergleich zu den Mengen an Spuren von Instanzen $E(inst(P)) \in E'(P)$ sehr klein ist oder sehr wenige charakteristische digitale Spuren enthält, wodurch auf die Ausführung einer Instanz des Prozesses nicht direkt geschlossen werden kann, so muss in den Schritt *Bestimmung der ausgeführten Aktivitäten* gewechselt werden, um ggf. ausgeführte Aktivitäten oder Teilprozesse zu identifizieren.

Der Schritt *Bestimmung der ausgeführten Aktivitäten* ist wieder unterteilt und startet mit dem Teilschritt *Suche nach möglichen Aktivitäten*. Hierbei werden zunächst alle

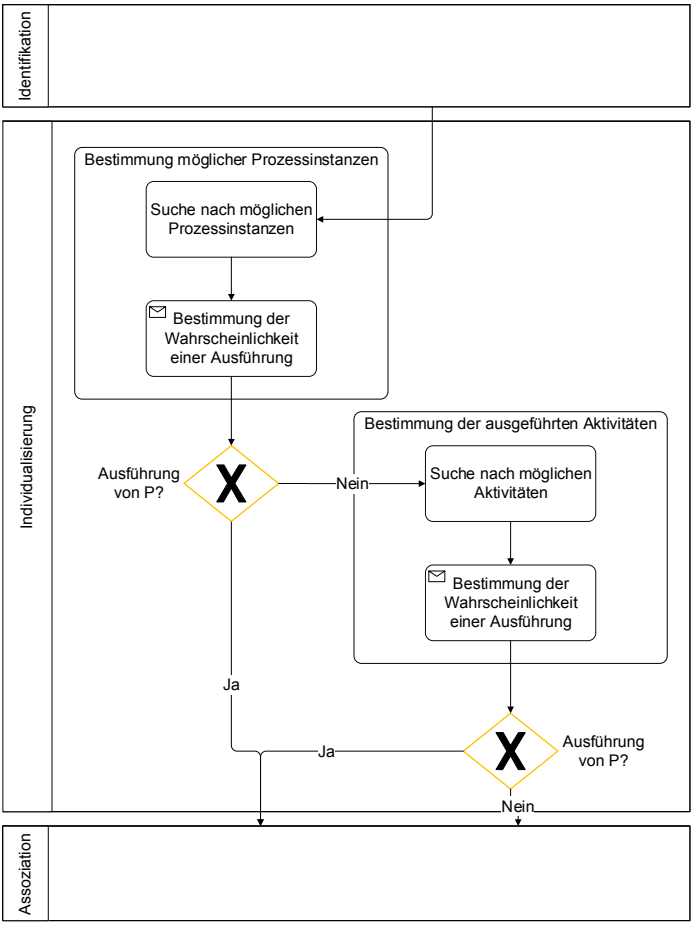


Abbildung 7.5 – Individualisierung bei unternehmensforensischen Untersuchungen

Aktivitäten $A' \subseteq A$ über die möglichen Instanzen IN' bestimmt und anschließend deren Spurenmengen $E(a)$ mit den in $Invest'(P)$ enthaltenen digitalen Spuren verglichen. Stimmen die in $Invest'(P)$ vorhandenen Datenelemente mit den in $E(a)$ enthaltenen Datenelementen überein, so sind die digitalen Spuren wiederum zu bewerten.

Die Bewertung wird im Schritt *Bestimmung der Wahrscheinlichkeit einer Ausführung* vorgenommen. Dieser Schritt wird analog zum ebenso benannten Teilschritt des Schrittes *Bestimmung möglicher Prozessinstanzen* ausgeführt. Die Bewertung der Rechtssicherheit der Spuren und der Wahrscheinlichkeit der Ausführung der $a \in A'$

erfolgt daher über die vorhandenen charakteristischen Spuren, die Qualität der Datenelemente bezüglich deren Sicherheit im Sinne der Ausführung aus Abschnitt 2.3.5 sowie der obigen Ausführungen bezüglich der Bewertung von Medienbrüchen.

Im Anschluss an den Teilschritt *Bestimmung der Wahrscheinlichkeit einer Ausführung* wechselt die Untersuchung in die Assoziationsphase.

7.2.3 Assoziation

In der Assoziationsphase wird entweder auf die Ausführung des Prozesses geschlossen und die Hypothese, dass der Prozess ausgeführt wurde, angenommen oder die Hypothese wird auf Basis der Analyse final abgelehnt. Wenn in der Individualisierungsphase eine entsprechende Menge an sicheren und charakteristischen Spuren des Prozesses gefunden wurde, so ist die Hypothese hinsichtlich der Ausführung des Prozesses anzunehmen. Konnten nicht hinreichend viele digitale Spuren des Prozesses oder dementsprechend viele Aktivitäten oder Teilprozesse des Prozesses bestimmt werden, so ist die Ausführung des Prozesses abzulehnen. Unter Umständen kann auch nur auf die Ausführung von Teilprozessen oder einzelner Aktivitäten geschlossen werden, nicht jedoch auf die Ausführung des Gesamtprozesses. Die Annahme oder Ablehnung entsprechender Hypothesen kann aber im Grunde nur fallbezogen begründet und entschieden werden.

An dieser Stelle der Methodik ist auch die bereits in Abbildung 6.6 bzw. Abschnitt 6.3.3 dargestellte Grenze der Unternehmensforensik zur digitalen Forensik im Allgemeinen. Demnach beschreiben die Prozessbeschreibungen nicht alle eventuellen Zustände des Systems, wodurch bei einer Ablehnung der Hypothese, dass ein bestimmter Prozess ausgeführt wurde, der Zustand des Systems über die hier vorgestellte Methodik unter Umständen nicht erklärt werden kann.

7.3 Grenzen der Unternehmensforensik

Durch die für die Unternehmensforensik in Abschnitt 7.1 festgelegten und näher besprochenen Voraussetzungen sowie die im vorherigen Abschnitt 7.2 vorgestellte Methodik ergeben sich Einschränkungen und Grenzen für unternehmensforensische Untersuchungen. Im folgenden Abschnitt 7.3.1 wird auf die Prozessbeschreibungen sowie deren Qualität und Aktualität als zentrale Voraussetzung für unternehmensforensische Untersuchungen näher eingegangen. Das Identitätsmanagement und seine wichtige Rolle in der Unternehmensforensik wird dann im Abschnitt 7.3.2 diskutiert. In Abschnitt 7.3.3 werden dann schließlich weitere technisch bedingte Grenzen unternehmensforensischer Untersuchungen dargestellt.

7.3.1 Qualität der Prozessdokumentation

Da die Prozessdokumentation den zentralen Dreh- und Angelpunkt in der Unternehmensforensik darstellt, ist deren Qualität essentiell. Während die Qualität von

Prozessmodellen unter verschiedenen Gesichtspunkten *gemessen* werden kann [OBS12, MSRRM15, RMR15], sind für die Unternehmensforensik besonders korrekte und vollständige Prozessbeschreibungen eine notwendige Voraussetzung.

Wenn Teile der Prozesse nicht oder nur unzureichend, z.B. ohne die am Prozess beteiligten Aufgabenträger oder Daten beschrieben oder modelliert sind, ist eine Nutzung in der Unternehmensforensik nur sehr eingeschränkt möglich. Insbesondere als Basis für Assoziationen kann die obligatorische und durch die Prozessmodelle realisierte Wissensbasis unter Umständen nicht mehr verwendet werden. Dadurch müssten andere digitale Spuren oder andere Quellen für die Erhebung der Prozessmodelle gefunden werden. Eine Möglichkeit sowohl zur Überprüfung der Qualität wie auch zur Ad-Hoc Erhebung aktueller, korrekter und vollständiger Prozessmodelle und Beschreibungen sind Interviews mit Schlüsselpersonen [Val10]. Interviews können aber ebenfalls genutzt werden, um Details der Prozesse, die z.B. aufgrund der bei der Modellierung gewählten Abstraktionsebene nicht mit modelliert wurden, zu ergründen.

Neben der Korrektheit und Vollständigkeit der einzelnen Prozessmodelle und -beschreibungen ist es zur Bestimmung charakteristischer Spuren eines Prozesses zudem wichtig, dass für alle Prozesse die Spurenmenge $E(P)$ bestimmt werden kann. Dementsprechend muss die Menge GP vollständig sein und zumindest alle Prozesse enthalten, die durch den oder die in Frage stehenden Prozesse verwendeten AWS ebenfalls nutzen.

7.3.2 Identitätsmanagement

Neben den Fragen nach dem *wo*, *wann* und *wie* sollte eine forensische Untersuchung auch das *wer* klären [IR02]. Auf der Ebene der Prozesse gibt es dazu die Möglichkeit nach der Rekonstruktion der ausgeführten Prozesse über die Mengen S und R die in Frage kommenden maschinellen und personellen Aufgabenträger zu bestimmen. Weitere Informationen sind allerdings regelmäßig nicht in Prozessbeschreibungen enthalten. Zwar gibt es Einschränkungen, die eine starke Authentifizierung und Autorisierung erforderlich machen, z.B. das Vier-Augen-Prinzip oder das Aufgabentrennungsprinzip. Deren konkrete technische Umsetzung wird aber selten detailliert in den Prozessmodellen festgehalten. Die Frage nach dem *wer* kann daher nur bedingt erschöpfend durch unternehmensforensische Untersuchungen geklärt werden.

Sollte dies auf digitaler Ebene dennoch gelingen und in den durch den Prozess definierten Datensätzen Informationen zu den personellen Aufgabenträgern enthalten sein, so gibt es weitere Probleme, da die Frage nach dem *Benutzer an der Tastatur* über digitale Spuren ohnehin sehr schwer zu beantworten ist [Ras04, Car09, PIP10]. Zur Beantwortung tragen ein strenges Identitätsmanagement mit einer regelmäßigen Kontrolle von Nutzern und deren Rechten sowie dessen technischer Umsetzung in Form von sicheren Authentifizierungs- und Autorisierungsverfahren bei. In der Praxis muss z.B. geprüft werden, ob jeder Benutzer eigene Passwörter hat, ob diese wirklich geheim sind oder ob die technischen Mechanismen bestimmte Bereiche eines Systems

tatsächlich effektiv gegen unbefugten Zugriff sichern [Car09].

7.3.3 Technische Barrieren und Einschränkungen

Technische Barrieren sind ein generelles Problem in der digitalen Forensik. Da unternehmensforensische Untersuchungen aber auf die im Prozess referenzierten digitalen Daten bzw. Spuren beschränkt sind, kann es sein, dass die Schlüsse aus unternehmensforensischen Untersuchungen gezielt manipuliert werden, ohne dass dies auf der jeweils untersuchten Abstraktionsebene erkannt werden kann. Um eine unternehmensforensische Untersuchung in die Irre zu führen, sind viele der unter dem Stichwort Anti-Forensik veröffentlichten Angriffsarten möglich. Darunter fallen z.B. die gezielte Manipulation, Löschung und das Verstecken von Spuren, sowie Attacken gegen die forensischen Werkzeuge selbst [RB10, SPO11]. Ein weiteres Problem sind Verschlüsselungstechnologien, die generell ein großes Hindernis für digitale forensische Untersuchungen darstellen [CFGS11].

Sollten nicht hinreichend viele und gute digitale Spuren, im Sinne der Skala in Tabelle 2.1, gesammelt werden können und zudem Probleme mit dem Identitätsmanagement, wie im vorherigen Abschnitt 7.3.2 dargestellt, bei einer Untersuchung zu Tage kommen, so ist in jedem Fall zusätzlich zur unternehmensforensischen Untersuchung eine digitale forensische Untersuchung der nicht von den Prozessmodellen referenzierten Systemteile und digitalen Daten notwendig, um eventuellen Manipulationen zu begegnen. Daneben können auch explizite Hinweise oder Verdachtsmomente bezüglich gezielter Manipulationen eine digitale forensische Untersuchung der nicht von der Unternehmensforensik betrachteten Systembestandteile oder Daten erforderlich machen.

7.4 Zusammenfassung

In diesem Kapitel wurden die allgemeinen forensischen Prinzipien aus Kapitel 2 auf die Unternehmensforensik übertragen und eine Methodik für unternehmensforensische Untersuchungen vorgestellt. Als Basis der Methodik dienen der in Kapitel 6 vorgestellte Formalismus sowie die aus der digitalen Forensik abgeleiteten Spurendefinitionen.

Obwohl die Methodik selbst auf das Definieren, Suchen und Bewerten von digitalen Spuren von Prozessen beschränkt ist, wurden in drei Schritten der Methodik Schnittstellen zu parallel laufenden digitalen forensischen und allgemeinen forensischen Untersuchungen definiert. Hierdurch soll ein Informationsaustausch ermöglicht werden, um auch andere Spuren der Prozesse im Kontext der Informationssysteme im Sinne soziotechnischer Systeme mit einzubeziehen.

In Abschnitt 7.3 wurden zudem nicht abschließend die Grenzen der vorgestellten Methodik diskutiert. Hierbei wurden sowohl die Voraussetzungen als auch die Limitierungen bei der Beantwortung der investigativen Fragen betrachtet.

Teil IV

Evaluation und Ausblick

KAPITEL 8

Evaluation

Die unternehmensforensischen Grundlagen aus Kapitel 6 sowie die darauf aufbauende Methodik aus dem vorherigen Kapitel 7 wurden anhand der im Folgenden vorgestellten Evaluation überprüft.

In Abschnitt 8.1 wird anhand eines real am Landgericht München verhandelten Falles ein Prozess sowie das maliziöse Verhalten der am Prozess beteiligten Buchhaltungsperson vorgestellt. Anschließend wird die Aufdeckung des Falles mithilfe einer unternehmensforensischen Untersuchung anstelle der tatsächlich für die Urteilsbegründung genutzten Zeugenaussagen dargestellt.

Die Anwendung der Methodik auf ein echtes System wird in Abschnitt 8.2 vorgestellt. Dabei wurden die Echtdaten eines KMU sowie die durch den Prozess der Rechnungsbearbeitung in diesem KMU erzeugten digitalen Spuren untersucht und die Anwendung der Methodik in der Praxis getestet.

In Abschnitt 8.3 werden die Erkenntnisse aus der Evaluation abschließend zusammengefasst und bewertet.

8.1 Fallstudie: Untreue einer Buchhaltungsperson

Auf Basis des am Landgericht München I verhandelten Falles[1] von Untreue einer Buchhaltungsperson wird im Folgenden eine Fallstudie vorgestellt, die dann zur Evaluation der Methodik für unternehmensforensische Untersuchungen herangezogen wird.

Das Urteil im oben genannten Fall wurde im Wesentlichen auf Basis von Zeugenaussagen und Papierausdrucken aus Anwendungssystemen gefällt. Digitale forensische Methoden wurden dabei weder zur Sicherung und Analyse von Daten des Buchhaltungs-

[1] LG München I, 6. Juli 2012, Az: 4 KLs 263 Js 133878/11

programms noch zur Sicherung und Analyse von digitalen Spuren aus dem Anwendungssystem zur Transaktionsabwicklung einer dritten Bank verwendet. Dennoch lassen sich anhand der in den beteiligten Unternehmen implementierten Prozesse Schlüsse auf das Funktionieren und den Nutzen der in dieser Arbeit vorgestellten Methodik, wie im Folgenden dargestellt ziehen.

8.1.1 Prozesse

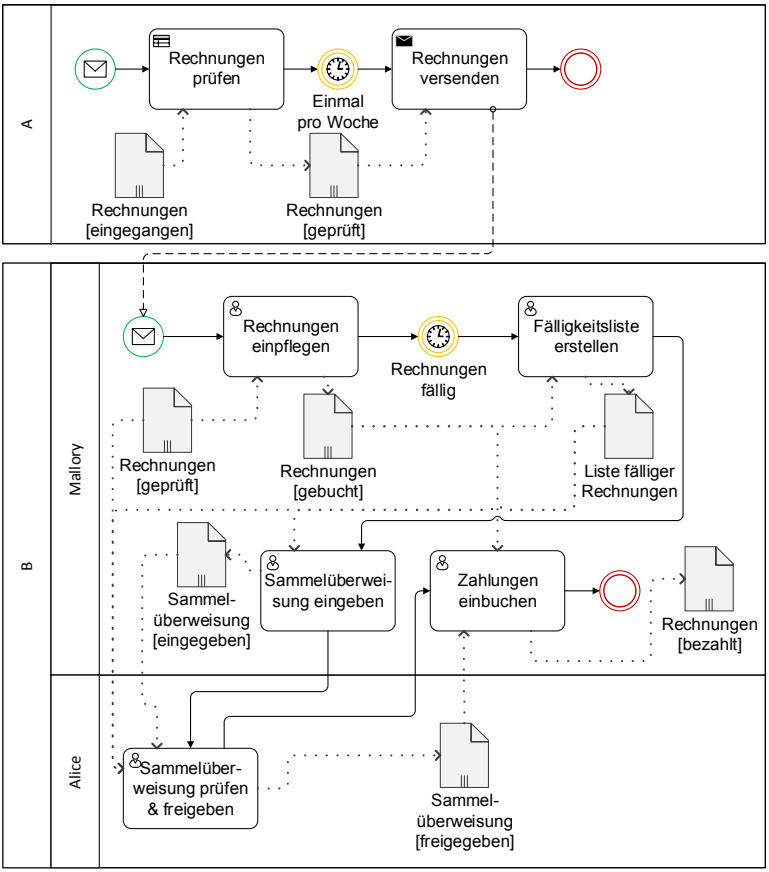


Abbildung 8.1 – Zahlung und Buchung von Rechnungen

An der Abwicklung der Buchhaltung des geschädigten Unternehmens, im Folgenden als A bezeichnet, waren regelmäßig drei Parteien beteiligt. Zum einen A selbst, ein Dienstleistungsunternehmen, im folgenden als B bezeichnet, das die Buchhaltung für

A übernommen hat und eine Bank, im folgenden als C bezeichnet, die die Konten verwaltet und Zahlungsaufträge durchgeführt hat.

Der reguläre Prozess zur Zahlung und Buchung von Rechnungen ist in Abbildung 8.1 dargestellt. Zunächst sind dabei die Rechnungen bei A eingegangen. Dort wurden sie von einer zuständigen Person auf inhaltliche Richtigkeit überprüft, gesammelt und einmal pro Woche an B gesendet.

Bei B hat die untreue Buchhaltungsperson, im folgenden Mallory genannt, die Rechnungen sowie deren Fälligkeiten in das Buchhaltungssystem SAP eingetragen. Am Tag der Fälligkeit der Rechnungen hat Mallory eine Fälligkeitsliste erstellt und die Zahlungen in Form einer Sammelüberweisung in das Banksystem von C zur Überweisung eingetragen. Das Banksystem von C und das Buchhaltungssystem von B sind explizit zwei voneinander getrennte Systeme ohne jegliche digitale Schnittstelle.

Nach der Eintragung der fälligen Zahlungen in das Transaktionssystem von C hat Mallory seiner vorgesetzten Person, im folgenden Alice genannt, die Fälligkeitsliste inkl. der Rechnungen übergeben. Alice hat die Fälligkeitsliste mit den Rechnungen stichprobenartig überprüft und anschließend die Sammelüberweisung im Banksystem von C freigegeben.

Nach der Überweisung der fälligen Rechnungen hat Mallory deren Bezahlung im Buchhaltungsprogramm von B als bezahlt entsprechend verbucht, wodurch der Vorgang abgeschlossen war.

8.1.2 Untreue und Scheinrechnungen

Den in Abbildung 8.1 dargestellten regulären Prozess hat Mallory neben der intendierten Weise auch für Scheinrechnungen verwendet, vorwiegend um sich selbst zu bereichern. Dazu hat Mallory, wie in Abbildung 8.2 dargestellt, Scheinrechnungen in Form von tatsächlich nie existenten Rechnungen in das Buchhaltungssystem von B eingepflegt. Anschließend wurde der Prozess, wie bereits im vorherigen Abschnitt 8.1.1 beschrieben durchgeführt. Im Rahmen des Gerichtsverfahrens war nicht mehr zweifelsfrei nachweisbar, ob Mallory die Zahlungen, die eigentlich von Alice freigegeben werden müssen, selbst freigegeben hat, indem er die digitale Identität von Alice übernommen hat, oder ob er Alice vorsätzlich getäuscht hat und diese dann die Zahlungen, wie im regulären Prozess geplant freigegeben hat.

An diesem Aspekt des Falles zeigt sich, dass das Identitätsmanagement sowie die Geheimhaltung von Passwörtern und der Schutz von Hardwaretokens vor unbefugtem Zugriff im Falle besitzbasierter Authentifizierungsverfahren, wie in Abschnitt 7.3.2 diskutiert enorm wichtig sind. Mallory hatte potentiell sowohl Zugang zum Passwort als auch zum Hardwaretoken für das Anwendungssystem von C, wodurch Mallory selbst Zahlungen freischalten konnte.

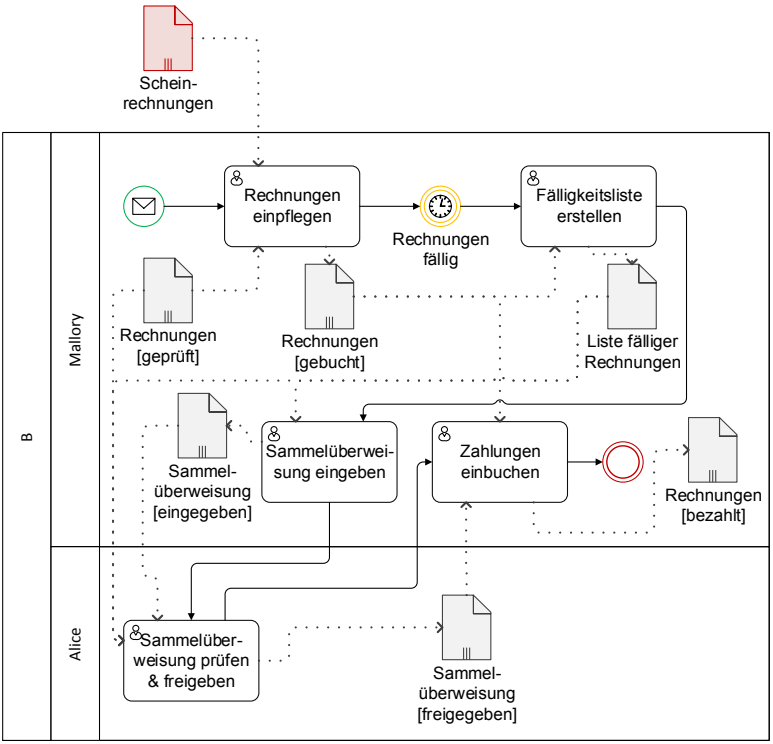


Abbildung 8.2 – Einschleusung von Scheinrechnungen in den Prozess

8.1.3 Unternehmensforensische Untersuchung

Anhand der obigen Prozessbeschreibung wird im Folgenden auf theoretischer Basis der Nutzen von unternehmensforensischen Untersuchungen nach der Methodik aus dem vorherigen Kapitel 7 sowie die erwarteten Ergebnisse aus einer solchen Untersuchung anhand der in diesem Abschnitt vorgestellten Fallstudie validiert.

Der Anfangsverdacht entstand im echten Fall aufgrund einer Mahnung wegen einer nicht bezahlten Rechnung. Die unternehmensforensische Untersuchung ist daher eine Top-Down Untersuchung, mit deren Hilfe herauszufinden ist, ob die Bearbeitung der Rechnung entsprechend dem Prozess aus Abbildung 8.1 ausgeführt wurde.

8.1.3.1 Vorbereitung

Zur Vorbereitung auf die Untersuchung müssen zunächst die in Abbildung 8.1 dargestellten Prozesse in das formale Prozessmodell aus Kapitel 6 überführt werden. Der in A ausgeführte Prozess $P(A)$ hat die beiden Aktivitäten *Rechnungen prüfen* und

Rechnungen versenden, die daher die Menge $A(P(A))$ bestimmen. Weiter gibt es einen Pfad von *Rechnungen prüfen* zu *Rechnungen versenden*. $G(P(A))$ sowie $t(P(A))$ sind beide leere Mengen, da der Prozess keine Gateways hat. $S(P(A))$ ist über die für die Rechnungsprüfung zuständige Person sowie die Person, die die Rechnungen versendet, definiert. $R(P(A))$ ist über die Zuordnung des Subjektes zur Rechnungsprüfung, dessen Aufgabe sowie der Zuordnung der Person zum Rechnungsversand und der entsprechenden verbundenen Pflicht bestimmt. Aufgrund von $D = \{\varnothing\}$ sind auch alle digitalen Spurenmengen leer, wodurch eine unternehmensforensische Untersuchung nach der Methodik aus Kapitel 7 für $P(A)$ nicht durchgeführt werden kann.

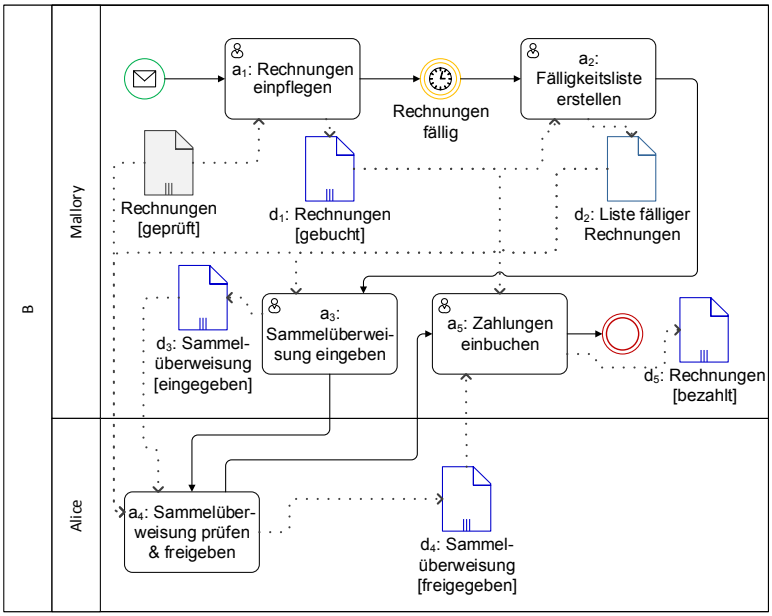


Abbildung 8.3 – Prozess mit Kennzeichnung seiner Daten

Für den zweiten Prozess $P(B)$, der bei B ausgeführt wird, gibt es fünf Aktivitäten. Abbildung 8.3 zeigt den Prozess im Detail, wobei die Aktivitäten und Datenelemente mit Kürzeln versehen sind. Die Menge der Aktivitäten ist demnach $A(P(B)) = \{a_1, a_2, a_3, a_4, a_5\}$. Die Menge der Pfade $F(P(A)) = \{(a_1, a_2), (a_2, a_3), (a_3, a_4), (a_4, a_5)\}$. Die Menge der Gateways sowie die Menge der Zuordnungen sind wie bei $P(A)$ die leere Menge. Die Menge der Subjekte ist $S = \{Alice, Mallory, SAP, Banksystem\}$ und die Menge der Rollen ist $R = \{r_1, r_2, r_3, r_4\}$. Die einzelnen Rollen sind definiert als $r_1 = (\{a_1, a_2, a_3, a_5\}, \{Mallory\}, \{\varnothing\})$, $r_2 = (\{a_4\}, \{Alice\}, \{\varnothing\})$, $r_3 = (\{a_1, a_2, a_5\}, \{SAP\}, \{\varnothing\})$ und $r_4 = (\{a_3, a_4\}, \{Banksystem\}, \{\varnothing\})$.

Die digitalen Daten $D(P(B))$ sind definiert als $D = \{d_1, d_2, d_3, d_4, d_5\}$, wobei d_2

sowohl digital (vor dem Ausdrucken) wie auch analog (nach dem Ausdrucken) vorliegt und nur in analoger Form wiederum als Input bei a_4 verwendet wird. Daher ist $d_2 \notin D_i$. $D_i(0) = \{\varnothing\}$, da der Prozess keine digitalen Inputs hat, weil die zu verbuchenden Rechnungen in Form von Papierrechnungen bei der Übernahme in das Buchhaltungssystem vorliegen. Die Ausgabedaten des Prozesses sind daher $D_o = D$, da alle digitalen Daten im Laufe der Prozessausführung generiert werden.

8.1.3.2 Identifikation

Nachdem das formale Prozessmodell erstellt ist, müssen in der Identifikationsphase zuerst die möglichen Datenelemente bestimmt werden. Die Menge IN kann in diesem Fall nicht eingeschränkt werden. Da es aber keine Gateways gibt, existiert ohnehin nur eine mögliche Instanz des Prozesses $P(B)$. Aus diesem Grund ist $E(P(B)) = E'(P(B))$. $E'(P(B))$ selbst ist dadurch definiert als $E'(P(B)) = \{D_o\}$.

Nachdem die Menge D_o die einzige Menge mit Datenelementen ist, ist $Invest(P(B))$ $= D_o$ und es müssen die Datenspeicherorte nur für diese Menge gesucht werden. Die Datenobjekte $\{d_1, d_2, d_5\}$ werden im SAP von B gespeichert und $\{d_3, d_4\}$ im Banksystem bei C. Da es sich in diesem Abschnitt um eine Fallstudie handelt, bei der die Prozesse nicht implementiert und keine reale Suche möglich ist, wurde auf die Dokumente zum Urteil zurück gegriffen. Aus den Dokumenten zum Urteil ergeben sich die, wenn auch nicht mittels Methoden der digitalen Forensik gesicherten digitalen Spuren insbesondere in Gestalt von ausgedruckten Datenauszügen aus den Systemen von B und C.

8.1.3.3 Individualisierung

Die gedruckten Datenauszüge zeigen, dass im Falle der Scheinrechnungen die digitalen Spuren des Prozesses teilweise vorhanden sind. Die Fälligkeitsliste taucht nicht in den digitalen Spuren auf, da es sich dabei scheinbar um eine nur temporär im System vorhandene Liste handelt, die nach dem Ausdrucken nicht persistent gespeichert wird. Auch im Zuge der Ermittlungen waren diese Listen nicht wiederbeschaffbar, was aus den Gerichtsdokumenten hervorgeht. In Abbildung 8.3 ist d_2 daher im Gegensatz zu den anderen Variablen anders eingefärbt. Im Modell kann dies über $d_2 = [v = NULL]$ ausgedrückt werden.

Außer d_2 können alle anderen Datenelemente in der Menge $E'(P(B))$ in beiden unabhängig voneinander arbeitenden Systemen von B und C nachgewiesen werden. Inhaltlich gibt es allerdings Diskrepanzen. Zum einen sind die Scheinrechnungen nicht vorhanden und zum anderen gibt es zwei leicht abgewandelte Betrugsschemata auf Basis der Scheinrechnungen.

Das erste Schema beinhaltet nicht vorhandene Rechnungen einer angeblichen Zulieferfirma ZA. Mit dieser hat A aber niemals wissentlich Geschäfte gemacht und die Firma war im konkreten Fall Mallory zuzuordnen. Bezüglich dieser Scheinrechnungen kann auf Ebene der Unternehmensforensik aber weder ein Fehler gefunden noch nach-

gewiesen werden. Alle Daten scheinen korrekt verarbeitet worden zu sein. Selbst die Freigabe der Zahlung, die für d_4 erforderlich ist, ist den Dokumenten aus dem Urteil nach konsistent im Sinne der Prozessbeschreibung erfolgt. Alle Transaktionen wurden von Alice regulär freigegeben.

Das andere Betrugsschema war leicht abgewandelt. Hierbei wurden Scheinrechnungen eines regelmäßig mit A handelnden Geschäftspartners ZB über das in Abbildung 8.2 dargestellte Verfahren eingeschleust. Hierbei stimmen die in d_3 gespeicherten und für die Transaktion im System von C verwendeten Informationen allerdings nicht mit den Informationen für ZB überein. Anstelle der Kontoinformationen von ZB wurden Kontoinformationen verwendet, die Mallory zugeordnet werden konnten.

8.1.3.4 Assoziation

Aufgrund der Daten kann auf die Ausführung des Prozesses $P(B)$ geschlossen werden. Das Fehlen von d_2 in beiden Betrugsschemata hat aufgrund seiner Eigenschaften als nicht persistentes Datenelement keine negativen Auswirkungen auf diese Assoziation. d_4 ist zudem eine sehr sichere digitale Spur, da die Erstellung von d_4 einen hybriden Authentifizierungsprozess voraussetzt.

Die inhaltlichen Diskrepanzen des zweiten Betrugsschemas sind im Rahmen einer reinen unternehmensforensischen Untersuchung nur erkennbar, wenn die Eingabedaten $D_i \subseteq D$ ebenfalls digital vorliegen, da die Veränderungen der Informationen für ZB dadurch in d_3 erkennbar wären. Andernfalls könnten die Unstimmigkeiten durch den Austausch von Informationen, mit parallel laufenden nicht digitalen forensischen Untersuchungen in den in der Identifikations- und Individualisierungsphase vorgesehenen Schritten, z.B. anhand von analogen Spuren auf Papier, erkannt werden.

8.1.3.5 Rekonstruktion

Nach wiederholter Assoziation und der Überprüfung der Systeme von B und C konnten mehrere ausgeführte Instanzen von $P(B)$ im Rahmen der Untersuchung nachgewiesen werden. In allen Fällen wurde entweder das eine oder das andere in Abschnitt 8.1.3.3 beschriebene Betrugsschema genutzt.

8.1.4 Ergebnisse

Die auf Basis der Fallstudie durchgeführte unternehmensforensische Untersuchung zeigt, dass das Modell aus Kapitel 6 sowie die darauf aufbauende Untersuchungsmethodik aus Kapitel 7 valide sind. Weiter zeigt die Untersuchung im Rahmen der Fallstudie die Möglichkeiten und potentiellen Ergebnisse einer unternehmensforensischen Untersuchung.

Im vorliegenden Fall konnte im Rahmen der Ermittlungen im realen Fall, wie auch anhand der im vorherigen Abschnitt 8.1.3 beschriebenen unternehmensforensischen Untersuchung kein weiteres maliziöses Verhalten im System von B oder C nachgewiesen

werden. Aufgrund der Freigabe der Überweisungen im Transaktionssystem von C durch Alice könnte auf Basis der unternehmensforensischen Untersuchung auch ihre Beteiligung am Betrug vermutet werden. Im realen Fall war Alice tatsächlich eine im Laufe der Jahre wechselnde Person mit jeweils neuem Passwort und Hardwaretoken. Die in Abschnitt 7.3.2 dargestellten Probleme aus einem schlechten Identitätsmanagement zeigen sich aber anhand des Falles sehr deutlich. Der Wechsel von Alice hatte in der Praxis weder die zeitnahe Sperrung des Accounts im System von C noch den Entzug des Hardwaretokens zur Folge. Weiter war der physische Zugang zum Hardwaretoken bei manchen Personen, die die Rolle von Alice inne hatten, nicht geregelt, was zur Folge hatte, dass Mallory potentiell darauf zugreifen konnte.

Durch das Schließen auf den Prozess $P(B)$ als Quelle der digitalen Spuren zeigt sich anhand der Ergebnisse aus der in Abschnitt 8.1.3 beschriebenen unternehmensforensischen Untersuchung zudem das Potential der Unternehmensforensik. Anders als z.B. in der *Forensic Readiness* propagiert, wurden im Rahmen der obigen Untersuchung keine klassischen Logdateien verwendet, um das Geschehen zu rekonstruieren. Die Annahme der Hypothese hinsichtlich der Abläufe in den Systemen von B und C stützt sich rein auf die über die Prozessbeschreibung bekannten und für den Prozess $P(B)$ essentiellen Datenelemente. Viele der Prozessinstanzen wurden bereits drei Jahre vor der Einleitung der Ermittlungen ausgeführt. Selbst wenn sowohl B als auch C ein ausführliches Logging betrieben hätten, wäre die Aufbewahrung der Logdaten über einen solch langen Zeitraum in der Praxis eher unwahrscheinlich. Die Nutzung von Bestandsdaten in der Unternehmensforensik ist daher ein entscheidender Vorteil gegenüber manch anderer Verfahren aus der digitalen Forensik, die auf Logdaten angewiesen sind.

8.2 Rechnungsbearbeitung in einem KMU

Neben der theoretischen Evaluation des Modells sowie der Methodik im vorherigen Abschnitt 8.1, wurde die Methodik auch in der Praxis anhand von Echtdaten evaluiert. Der untersuchte Prozess beschreibt die Rechnungsbearbeitung in einem kleinen Unternehmen, im Folgenden K genannt, mit weniger als zehn Mitarbeitern und einem Umsatz von weniger als einer Million € pro Jahr. K hat seinen Sitz in Deutschland und ausschließlich deutsche Kunden. Die Kerntätigkeitsfelder sind der Verkauf von Gütern sowie die Erbringung von dazu passenden Dienstleistungen im Bereich Informations- und Telekommunikationssysteme.

8.2.1 Prozesse

Abbildung 8.4 zeigt die beiden wesentlichen Prozesse zur Rechnungsbearbeitung von K in Form eines BPMN 2.0 Prozessmodells. Die beiden Prozesse sind einmal der vom Verkauf ausgeführte Geschäftsprozess zur Rechnungserstellung, im Folgenden als $P(A)$ bezeichnet, und der auf diesen folgende Prozess, im Folgenden als $P(B)$ bezeichnet, zur

Buchung der Rechnung sowie der Prüfung der Zahlung. $P(B)$ wird von der Buchhaltung ausgeführt. Weiter sind die Datenspeicher der Datenobjekte dargestellt und mit den zugehörigen Datenobjekten assoziiert.

Die einzelnen Aktivitäten von $P(A)$ sind wie folgt festgelegt:

Informationen zum Auftrag sammeln In diesem Schritt werden alle relevanten Informationen für die Abrechnung gesammelt. Neben Angeboten zählen dazu auch Regieberichte, Notizen und E-Mails mit abrechnungsrelevanten Daten wie verhandelten Preisen oder geleisteten Stunden.

Angebot weiterführen Wurde im ersten Schritt ein entsprechendes Angebot identifiziert, so wird dieses in diesem Schritt als Rechnungsdokument weitergeführt.

Neues Rechnungsdokument anlegen Kann im ersten Schritt kein passendes Angebot zum Auftrag identifiziert werden, so wird ein neues Rechnungsdokument erstellt und mit den Stammdaten des Kunden befüllt.

Positionen anpassen Im Rahmen der Aktivität werden Positionen zum Rechnungsdokument hinzugefügt sowie bestehende oder aus einem weitergeführten Angebot stammende Positionen angepasst oder entfernt.

Rechnung ausdrucken In diesem Schritt wird die fertige Rechnung auf Papier zur Archivierung ausgedruckt.

Rechnung archivieren Die ausgedruckte Rechnung wird in diesem Schritt in einem Ordner abgeheftet und archiviert.

Rechnung auf Formular ausdrucken Zum postalischen Versand an den Kunden wird die Rechnung im Rahmen dieser Aktivität auf, mit dem Briefkopf von K vorgedruckten Formularen ausgedruckt.

Rechnung versenden Nach dem Ausdrucken auf dem Formularpapier wird die Rechnung in diesem Schritt postalisch an den Kunden versandt.

PDF-Rechnung erstellen In diesem Schritt wird die Rechnung digital in Form einer PDF-Datei erstellt.

E-Mail versenden Im Rahmen dieser Aktivität wird die PDF-Rechnung als E-Mail an den Kunden versendet.

Der Ablauf des Prozesses stellt sich im Detail wie folgt dar: Nach der Sammlung der abzurechnenden Ware und der Dienstleistungen im Schritt *Informationen zum Auftrag sammeln* wird entweder ein bestehendes Angebot weitergeführt, indem der Schritt *Angebot weiterführen* ausgeführt wird, oder es wird ein gänzlich neues Rechnungsdokument durch die Ausführung der Aktivität *Neues Rechnungsdokument anlegen* erstellt. Im Anschluss an entweder die Aktivität *Angebot weiterführen* oder die Aktivität *Neues*

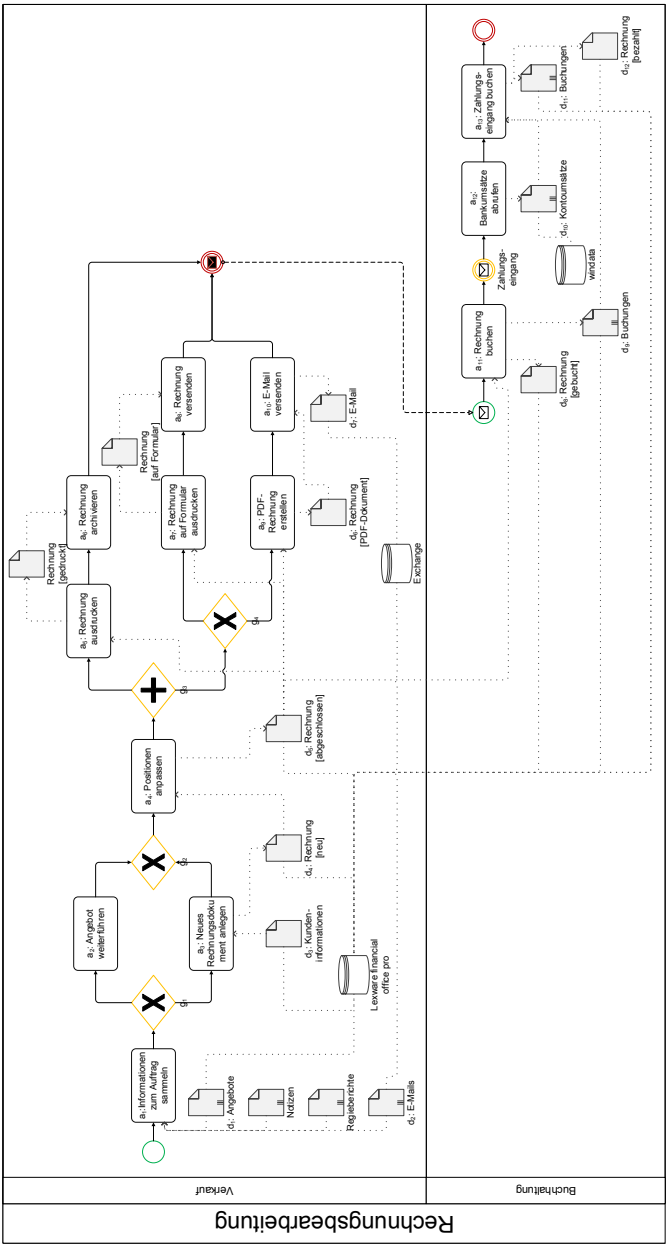


Abbildung 8.4 – Prozesse zur Rechnungsbearbeitung bei K

Rechnungsdokument anlegen, werden die Rechnungspositionen im Schritt *Positionen anpassen* angepasst und die Rechnung dadurch finalisiert.

Nach dem Fertigstellen der Rechnung wird diese auf Papier im Schritt *Rechnung ausdrucken* ausgedruckt und anschließend im Schritt *Rechnung archivieren* archiviert. Parallel zum Drucken der Rechnung auf Papier wird entweder der Schritt *Rechnung auf Formular ausdrucken* oder die Aktivität *PDF-Rechnung erstellen* ausgeführt, je nachdem, ob der Kunde eine Rechnung in Papierform oder eine elektronische Rechnung wünscht. Wurde der Schritt *Rechnung auf Formular ausdrucken* ausgeführt, so wird anschließend der Schritt *Rechnung versenden* abgearbeitet. Wurde eine PDF-Rechnung erstellt, so wird im Anschluss an die Aktivität *PDF-Rechnung erstellen* der Schritt *E-Mail versenden* durchgeführt. Der Prozess endet damit und die Buchhaltung wird über eine neue Rechnung benachrichtigt.

Grundsätzlich ist der in diesem Abschnitt dargestellte und bei K implementierte Prozess nicht an ein bestimmtes AWS gebunden. Die detaillierten Funktionen, wie das Weiterführen eines Angebotes oder das Erstellen einer PDF-Rechnung müssen aber vom implementierenden AWS unterstützt werden. Weiter müssen die rechtlichen und regulatorischen Vorgaben, z.B. hinsichtlich der in Deutschland im Rechnungsdokument erforderlichen Informationen, der steuerrechtlichen Vorgaben oder der Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) [Bun14b], vom AWS implementiert und eingehalten werden.

8.2.2 Formales Prozessmodell

Zur Vorbereitung auf unternehmensforensische Untersuchungen wurden analog zur Untersuchung aus dem vorherigen Abschnitt 8.1 zunächst die Prozesse aus dem in Abbildung 8.4 dargestellten Prozessmodell in das formale Modell aus Kapitel 6 überführt. Die Menge der Gesamtprozesse ist $GP = \{P(A), P(B)\}$.

Die Menge der Aktivitäten von $P(A)$ ist definiert als $A(P(A)) = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}\}$. $G(P(A)) = \{g_1, g_2, g_3, g_4\}$ beschreibt die Menge der Gateways, wobei den Gateways die folgenden Typen zugeordnet werden: $t : g_1 \rightarrow xor; g_2 \rightarrow xor; g_3 \rightarrow and; g_4 \rightarrow xor$. Die Menge der Knoten ist definiert als $N(P(A)) = A(P(A)) \cup G(P(A))$ und die Menge der Pfade ist $F = \{(a_1, g_1), (g_1, a_2), (g_1, a_3), (a_2, g_2), (a_3, g_2), (g_2, a_4), (a_4, g_3), (g_3, a_5), (a_5, a_6), (g_3, g_4), (g_4, a_7), (a_7, a_8), (g_4, a_9), (a_9, a_{10})\}$. Die am Prozess beteiligten Subjekte sind $S(P(A)) = \{s_1, s_2, s_3\}$ und die Menge der Rollen ist $R(P(A)) = \{r_1, r_2, r_3\}$. Der Bezeichner s_1 entspricht dabei einem Mitarbeiter im Vertrieb, s_2 dem maschinellen Aufgabenträger *Lexware financial office pro* und s_3 dem maschinellen Aufgabenträger *Exchange*. Die einzelnen Rollen sind definiert als $r_1 = (A(P(A)), \{s_1\}, \{\varnothing\})$, $r_2 = (\{a_1, a_2, a_3, a_4, a_5, a_7, a_9\}, \{s_2\}, \{\varnothing\})$ und $r_3 = (\{a_{10}\}, \{s_3\}, \{\varnothing\})$.

Die Menge der Datenelemente ist $D(P(A)) = \{d_1, d_2, d_3, d_4, d_5, d_6, d_7\}$, wobei die Menge der Inputs des Gesamtprozesses $P(A)$ durch $D_i(0) = \{d_1, d_2, d_3\}$ und die Outputs

des Prozesses durch $D_o = \{d_4, d_5, d_6, d_7\}$ beschrieben sind.

Die Menge der Aktivitäten von $P(B)$ ist definiert als $A(P(B)) = \{a_{11}, a_{12}, a_{13}\}$. Da $P(B)$ keine Gateways enthält, ist $G(P(B)) = \{\varnothing\}$ und $N(P(B)) = A(P(B))$. Die Pfade sind definiert als $F(P(B)) = \{(a_{11}, a_{12}), (a_{12}, a_{13})\}$. Die Subjekte sind $S(P(B)) = \{s_2, s_4, s_5\}$. s_4 entspricht einem Mitarbeiter in der Buchhaltung und s_5 dem maschinellen Aufgabenträger *windata*. Die Menge der Rollen von $P(B)$ ist definiert als $R(P(B)) = \{r_4, r_5, r_6\}$ und die einzelnen Rollen sind $r_4 = (A(P(B)), \{s_4\}, \{\varnothing\})$, $r_5 = (\{a_{11}, a_{13}\}, \{s_2\}, \{\varnothing\})$ und $r_6 = (\{a_{12}, a_{13}\}, \{s_5\}, \{\varnothing\})$.

Die Menge der Datenelemente von $P(B)$ ist definiert als $D(P(B)) = \{d_5, d_8, d_9, d_{10}, d_{11}, d_{12}\}$. Die Inputs des Gesamtprozesses $P(B)$ sind $D_i(0) = \{d_5\}$ und die Outputs des Prozesses sind $D_o = \{d_8, d_9, d_{10}, d_{11}, d_{12}\}$.

8.2.3 Anwendungssysteme zur Implementierung des Prozesses

Die AWS, die die im vorigen Abschnitt 8.2.2 definierten Prozesse bei K unterstützen, sind in Abbildung 8.4 als die den Datenobjekten zugeordneten Datenspeicher dargestellt. Bei K werden zur Bearbeitung der beiden Geschäftsprozesse die drei Systeme *Lexware financial office pro*[2], *Exchange*[3] und *windata*[4] eingesetzt. Lediglich der PDF-Rechnung wurde kein System zugewiesen, da diese von der PDF-Druckersoftware *qvPDF*[5] erzeugt und im Dateisystem abgelegt wird. Die Software *qvPDF* sowie das verwendete Dateisystem *NTFS* stellen keine spezielle unternehmensspezifische Software dar.

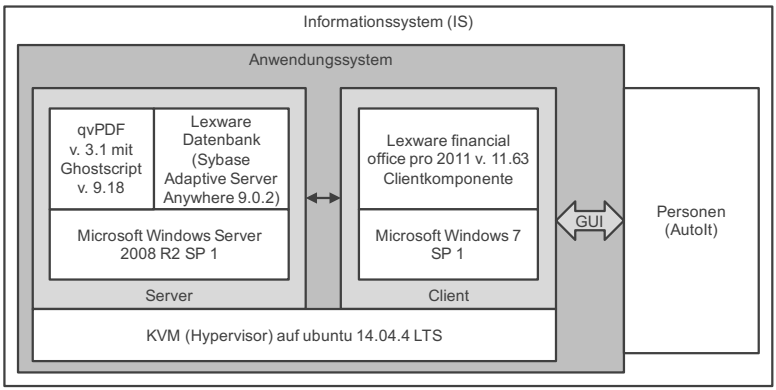


Abbildung 8.5 – Systemarchitektur des untersuchten Systems von K

Lexware financial office pro wurde zum Zeitpunkt der Untersuchung in der Version 11.63 eingesetzt. Die Software basiert auf dem Datenbankmanagementsystem *Sybase*

[2] http://shop.lexware.de/lexware-financial-office-pro
[3] https://products.office.com/de-DE/exchange/email
[4] http://2016.windata.de/Site/Produkte/produktWDpro.html
[5] https://sourceforge.net/projects/qvpdf/

Adaptive Server Anywhere in der Version 9.0.2, dessen Weiterentwicklung aktuell von der Firma SAP unter dem Produktnamen *SQL Anywhere*[6] vertrieben wird. *Lexware financial office pro* ist ein auf die Bedürfnisse von kleinen und mittleren Unternehmen zugeschnittenes ERP-System mit dem die Warenwirtschaft, die Buchhaltung sowie die Lohn- und Gehaltsabrechnungen vorgenommen werden können. Bei K werden lediglich die Module für die Warenwirtschaft sowie die Buchhaltung genutzt. Im Folgenden wird *Lexware financial office pro* allgemein als ERP-System bezeichnet.

Zur Abwicklung des E-Mail Verkehrs und zum Versand von Rechnungen wurde zum Zeitpunkt der Untersuchung das Produkt *Microsoft Exchange Server*, in Abbildung 8.4 nur als *Exchange* bezeichnet, eingesetzt. Zur Abwicklung des elektronischen Zahlungsverkehrs, der auch das Abrufen der Kontoauszüge einschließt, wurde zum Zeitpunkt der Untersuchung die Software *windata* verwendet. Beide Systeme haben aber im Folgenden keine Relevanz, da für die Untersuchung lediglich der Zugriff auf die Daten aus dem ERP-System bzw. der Datenbank möglich war.

Um den operativen Geschäftsbetrieb von K bei der Durchführung der Untersuchung nicht zu stören oder gar gänzlich zu gefährden, wurde eine Datensicherung aus dem ERP-System in einem parallel installierten System eingespielt. Dabei wurde die selbe Software wie bei K verwendet. Für das ERP-System sowie für *qvPDF* wurde zudem der exakt gleiche Updatestand der Software wie im Echtsystem von K verwendet. Abbildung 8.5 zeigt die Architektur sowie die Softwarestände der weiteren Systemkomponenten. Weiter wurde für die Aufgaben, die bei K von den personellen Aufgabenträgern ausgeführt werden die Software *AutoIt*[7] eingesetzt. *AutoIt* ist eine Software zur Automatisierung der Windows GUI, die z.B. Tastatur- und Mauseingaben simuliert. Mithilfe dieser Software wurden die einzelnen Eingaben, die zur Erstellung der Rechnung von s_1 notwendig sind, im Rahmen der im folgenden Abschnitt 8.2.4 beschriebenen DFA abgebildet.

8.2.4 Differential Forensic Analysis zur Bestimmung der digitalen Spuren

Das ERP-System von K ist eine proprietäre closed-source Anwendung, die nicht in der aktuellsten am Markt verfügbaren Programmversion bei K installiert ist. Wie in Abschnitt 6.1 festgestellt, gibt es noch eine erhebliche Lücke bei den Tools zur Sicherung und Auswertung von digitalen Spuren aus und von betrieblicher Anwendungssoftware. Auch für das ERP-System von K konnte kein spezielles Werkzeug für digitale forensische Untersuchungen auf dem Markt identifiziert werden. Aus diesem Grund wurde zur Vorbereitung der unternehmensforensischen Untersuchung eine DFA durchgeführt, um die bei der Erstellung einer Rechnung entstehenden digitalen Spuren zu bestimmen.

Da das System wie in Abbildung 8.5 dargestellt installiert ist, wurden mithilfe der Software *AutoIt* die vom personellen Aufgabenträger s_1 im Vertrieb durchzuführenden Handlungen automatisiert. Die Teilmenge der im Rahmen der DFA ausgeführten

[6] http://go.sap.com/germany/product/data-mgmt/sql-anywhere.html
[7] https://www.autoitscript.com/

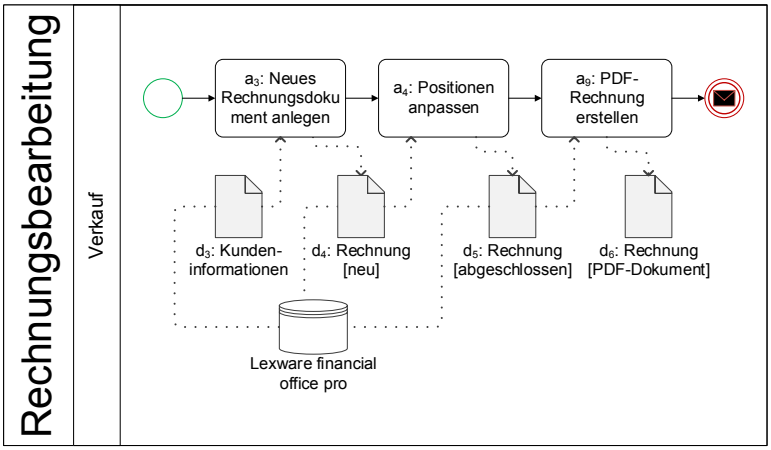


Abbildung 8.6 – Untersuchte Prozessschritte aus dem Prozessmodell von K

Aktivitäten des Prozesses $P(A)$ ist in Abbildung 8.6 dargestellt. Konkret war das Ziel der DFA die digitale Repräsentation im AWS im Sinne einer Variable nach der Definition aus Abschnitt 6.2.3 für die Datenelemente d_4, d_5 und d_6 zu bestimmen.

Im folgenden Abschnitt 8.2.4.1 werden zunächst der Untersuchungsaufbau und der genaue Ablauf beschrieben und in den Abschnitten 8.2.4.2 und 8.2.4.3 die Ergebnisse der DFA vorgestellt. In Abschnitt 8.2.4.4 werden die Erkenntnisse aus der Analyse dann abschließend kurz zusammengefasst.

8.2.4.1 Untersuchungsaufbau und -ablauf

Durch die Installation eines zum System bei K identischen Systems und die Nutzung von *KVM*[8], wie in Abbildung 8.5 dargestellt, konnte eine durch den Untersuchungsaufbau in [KDF13] inspirierte DFA durchgeführt werden. Anders als in [KDF13] war bei dieser DFA das Ziel, wie oben definiert, die bei der Ausführung des in Abbildung 8.6 dargestellten Prozesses entstehenden digitalen Spuren und die Repräsentation von d_4, d_5 und d_6 im AWS zu bestimmen. Daher wurden keine Fingerprints im Sinne von [KDF13] erzeugt. Weiter wird in [KDF13] eine auf einem isolierten Rechner laufende Anwendung und die Änderungen im Dateisystem betrachtet. Wie in Abbildung 8.5 dargestellt, nutzt das ERP-System aber eine Datenbank und die GUI wird typischerweise auf dem Client ausgeführt. Daher wurden die Komponenten GUI-Anwendung des ERP-Systems und die Datenbank auch entsprechend aufgeteilt und wie bei K in den zwei in Abbildung 8.5 dargestellten separaten Maschinen mit *Windows 7* bzw. *Windows Server 2008 R2* betrieben.

[8] http://www.linux-kvm.org/

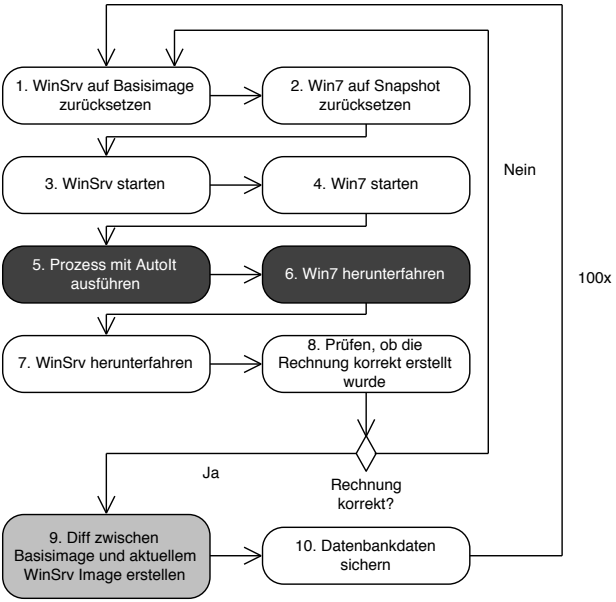


Abbildung 8.7 – Ablauf der Differential Forensic Analysis

Der genaue Untersuchungsablauf ist in Abbildung 8.7 enthalten. Die DFA wurde hauptsächlich durch ein Bash-Script auf dem, mit *ubuntu Server 14.04* laufenden *KVM* Hostsystem gesteuert und besteht aus zehn abgrenzbaren Aktivitäten. Alle in Abbildung 8.7 nicht farblich hinterlegten Aktivitäten wurden vom zentralen Bash-Script direkt ausgeführt. Die dunkelgrau hinterlegten Aktivitäten fünf und sechs wurden von einem *AutoIt*-Skript und die leicht grau hinterlegte Aktivität neun mittels *fiwalk*[9] bzw. *idifference2*[10] ausgeführt. Für die Aktivität acht wurde zudem ein Ruby-Script zur Prüfung des PDF-Inhalts mittels Regex mit verwendet.

Jeder der Analysedurchläufe hat im ersten Schritt mit dem Zurücksetzen des Servers, im Folgenden wie in Abbildung 8.7 als WinSrv bezeichnet, begonnen. Dazu wurde ein direkt nach der Einrichtung des AWS gesichertes Image der Festplatte von WinSrv (Basisimage) an den von *KVM* verwendeten Speicherort kopiert.

Im zweiten Schritt wurde der *Windows 7* Client, im Folgenden als Win7 bezeichnet, auf den Ursprungszustand zurückgesetzt. Dazu wurde ein mittels *KVM* erstellter Snapshot benutzt. Im Anschluss an das Zurücksetzen von Win7 wurde die Maschine WinSrv im dritten Schritt gestartet. Nach einer kurzen Pause von einer Minute wurde der vierte Schritt ausgeführt und die zweite Maschine Win7 in *KVM* eingeschaltet.

[9] https://github.com/kfairbanks/sleuthkit/tree/master/tools/fiwalk
[10] https://github.com/simsong/dfxml/blob/master/python/idifference2.py

Das Bash-Script hat an dieser Stelle bis zum Herunterfahren von Win7 gewartet.

Der fünfte Schritt bzw. das *AutoIt*-Skript wurde unmittelbar beim Start von Win7 über einen Eintrag im Autostart von Win7 ausgeführt. Das *AutoIt*-Skript hat zunächst die GUI-Komponente des ERP-Systems gestartet und dann eine neue Rechnung, wie in Abschnitt 8.2.1 beschrieben bzw. in Abbildung 8.6 dargestellt erstellt. Nach dem Erzeugen der PDF-Rechnung wurde die GUI des ERP-Systems beendet und die Maschine Win7 heruntergefahren. Im Anschluss an das Herunterfahren der Maschine hat das Bash-Script im siebten Schritt das Herunterfahren der Maschine WinSrv angestoßen und gewartet bis die Maschine ausgeschaltet war.

Im Schritt acht wurde zuerst die zweite Festplatte der Maschine WinSrv auf dem Hostsystem gemountet und mittels Ruby-Script geprüft, ob eine PDF-Datei vorhanden ist und ob diese der erwarteten Rechnung entspricht. Um die Analyse der Festplatte der WinSrv Maschine nicht durch etwaige Manipulationen zu gefährden, wurde die PDF-Rechnung auf einem separaten zweiten Datenträger der Maschine WinSrv abgelegt, der lediglich als Ziel für *qvPDF* eingerichtet und konfiguriert wurde.

War keine Rechnung vorhanden oder diese nicht richtig, so wurde der Analysedurchlauf verworfen und ein neuer Durchlauf ab Schritt eins gestartet. Gründe für das Fehlschlagen eines Durchlaufs waren z.B. Updateprozesse oder andere unvorhergesehene und das Skript blockierende Meldungen in der Maschine Win7. Beim Vorliegen einer gültigen Rechnung wurde die Systemfestplatte von WinSrv auf der alles, außer dem PDF aus *qvPDF* gespeichert und installiert wurde, mit dem Basisimage mittels *idifference2* verglichen und das Ergebnis gespeichert. Im letzten Schritt wurden dann die Datenbankdateien aus der Systemfestplattendatei von WinSrv gesichert, um die spätere Auswertung der Datenbank zu ermöglichen.

Der oben skizzierte Analyseprozess wurde 100 mal durchgeführt, wobei nur erfolgreiche Durchläufe im Sinne einer richtigen PDF-Rechnung gezählt wurden. Neben der vollständigen Analyse nach dem oben skizzierten Ablauf aus Abbildung 8.7 wurden zusätzlich drei weitere Analysen mit je 100 Durchläufen durchgeführt.

Bei der zweiten Analyse wurde keine Rechnung mehr erstellt, sondern es wurde vom *AutoIt*-Skript nurmehr die GUI des ERP-Systems geöffnet. Dadurch hat sich im Gegensatz zur ersten Analyse der Schritt fünf geändert und der Schritt acht wurde nicht mehr ausgeführt. Bei der dritten Analyse wurde die Maschine Win7 nur noch gestartet und durch das *AutoIt*-Skript im Anschluss daran gleich wieder herunter gefahren. Hierbei wurden im Unterschied zum Ablauf in Abbildung 8.7 die Schritte fünf und acht komplett weggelassen. Im vierten Ablauf wurde der in Abbildung 8.8 verkürzt dargestellte Prozess, im Folgenden als $P(C)$ bezeichnet, zur Angebotserstellung ausgeführt. Dabei sind in Abbildung 8.8 nur die vom ERP-System unterstützten Aktivitäten a_{14}, a_{15} und a_{16} dargestellt. Durch den vierten Analysedurchlauf sollten Aussagen bezüglich charakteristischer Spuren und etwaiger Spuren-Interferenzen ermöglicht werden. Daher wurde ein dem Rechnungserstellungsprozess $P(A)$ ähnlicher Prozess gewählt. Bei der Betrachtung von Abbildung 8.6 im Vergleich mit Abbildung 8.8 zeigt sich diese Ähnlich-

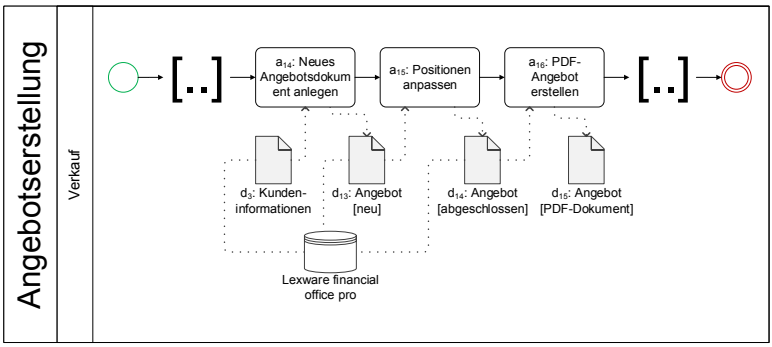


Abbildung 8.8 – Über das ERP-System unterstützte Prozessschritte der Angebotserstellung bei K

keit deutlich. Ein Angebotsdokument selbst ist inhaltlich auch kaum von der Rechnung unterscheidbar und wird über die selben Steuerelemente und GUI-Komponenten des ERP-Systems bearbeitet, weshalb auch eine Interferenz der digitalen Spuren im Sinne der Ausführungen von Dewald [Dew12, S. 96ff] als sehr wahrscheinlich erachtet wurde.

Bei der vierten Analyse wurden allerdings nur die in der Datenbank entstehenden Spuren untersucht. Aus diesem Grund unterscheidet sich die vierte Analyse zum Ablauf aus Abbildung 8.7 in den Schritten fünf und neun. In Schritt fünf wurde anstelle des Rechnungsbeleges ein Angebot erstellt und Schritt neun wurde ausgelassen, da aufgrund der im Folgenden Abschnitt 8.2.4.2 vorgestellten Ergebnisse aus dem Dateisystem nur mehr die Ebene der Datenbanken betrachtet werden sollte.

8.2.4.2 Ergebnis auf Dateisystemebene

Das ERP-System nutzt zur Ablage seiner Nutzdaten grundsätzlich die Datenbank. Aber, weder für das ERP-System noch für *qvPDF* ist bekannt, ob weitere digitale Spuren im Dateisystem bei der Erstellung der Rechnung entstehen. Daher wurde im Rahmen der Auswertung der Daten aus der DFA auch das Dateisystem näher untersucht. Abbildung 8.9 stellt die Änderungen im Dateisystem grafisch dar. Auf der x-Achse sind lediglich die Dateien der zweiten Partition angetragen, die der Partition *C:* der Maschine WinSrv entspricht. Die Änderungen in der obligatorischen Wiederherstellungspartition von Windows sind nicht dargestellt, da dort keine Dateien des ERP-Systems identifiziert werden konnten. Die horizontale Streuung der Punkte ergibt sich durch einen Algorithmus[11] der künstlich versucht, das Übermalen von Datenpunkten zu verhindern. Ansonsten würden sich alle Punkte entlang einer vertikalen Linie befinden, da das Plotten einer regulären x-Achse aufgrund der Menge an Datenpunkten auf dieser Achse keine brauchbaren Ergebnisse erzeugt hat. Die Grafiken wurden mit

[11] http://docs.ggplot2.org/current/geom_jitter.html

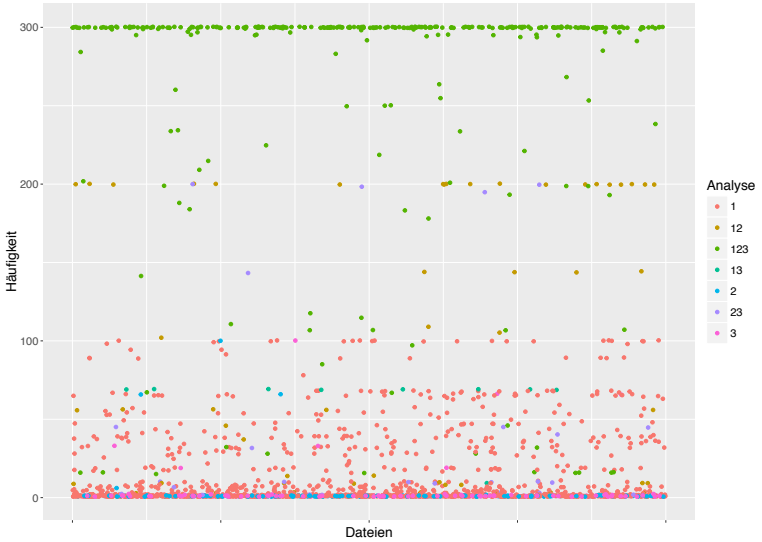


Abbildung 8.9 – Änderungen im Dateisystem

R[12] und der Bibliothek *ggplot*[13] erstellt.

Auf der y-Achse in Abbildung 8.9 ist die Häufigkeit der Änderungen pro eindeutig identifizierbarer Datei angetragen. Dateien wurden über die Attribute Partition, Dateiname (kompletter Pfad der Datei) und dem von *idifference2* festgelegten Änderungstyp eindeutig identifiziert.

Die jeweiligen Datenpunkte sind zudem eingefärbt. Die Legende *Analyse* enthält dabei für alle Kombinationen aus den ersten drei Analysen mit je hundert Durchläufen die jeweils zugeordnete Farbe. Die 1 entspricht dabei der ersten Analyse, bei der alle in Abbildung 8.7 dargestellten Aktivitäten komplett inkl. der Erstellung der Rechnung ausgeführt wurden. Die 2 steht für die zweite Analyse, bei der lediglich die GUI des ERP-Systems geöffnet wurde und die 3 steht für die dritte Analyse, bei der nur Windows gestartet und anschließend wieder beendet wurde, ohne das ERP-System auf der Maschine Win7 zu öffnen. Insgesamt konnten aus den 111.572 Änderungen über die 300 Durchläufe 2.101 eindeutige Änderungen identifiziert werden, wobei viele Dateien nur in einem oder wenigen Durchläufen geändert wurden. Dies ist auch in Abbildung 8.9 anhand der vielen Datenpunkte nahe der x-Achse zu beobachten.

Im Detail konnten die in Tabelle 8.1 aufgeführten Dateien als digitale Spur der Prozessausführung identifiziert werden. Die beiden ersten Dateien sind Dateien, die dem PDF-Drucker *qvPDF* zugeordnet werden können und vermutlich beim Erstellen von

[12] https://www.r-project.org
[13] http://ggplot2.org

Tabelle 8.1 – Digitale Spuren der Prozessausführung im Dateisystem auf Partition Nr. 2

#	Dateiname	Typ	Anz.	Anal.
1	Program Files (x86)/qvPDF/qvPDF.log	changed_file	100	1
2	Program Files (x86)/qvPDF/qvRedRun.log	changed_file	100	1
3	Daten/Lexware/Datenbank/f0/LxCompany.db	changed_file	200	12
4	Daten/Lexware/Datenbank/f0/LxCompany.log	changed_file	200	12
5	Daten/Lexware/Datenbank/F3/lxcompany.db	changed_file	200	12
6	Daten/Lexware/Datenbank/F3/lxcompany.log	changed_file	200	12
7	Daten/Lexware/Datenbank/LexKK.DB	changed_file	200	12
8	Daten/Lexware/Datenbank/LexKK.LOG	changed_file	200	12
9	Daten/Lexware/Datenbank/LxCatalog.db	changed_file	100	1
10	Daten/Lexware/Datenbank/LxCatalog.log	changed_file	100	1

d_6 entstehen. Die Dateien drei bis zehn sind dem ERP-System zuzuordnen. Im ERP-System sind drei Mandanten (Firmen) angelegt, wobei *F3* K entspricht. Entsprechend der Konfiguration des ERP-Systems ist die Datei fünf die Datenbankdatei des ERP-Systems von K und die Datei sechs die zugehörige Logdatei.

Obwohl die Datei *Daten/Lexware/Datenbank/F3/lxcompany.db* den Datenspeicher der Datenelemente d_4 und d_5 darstellt, konnten die Datenelemente auf dieser Abstraktionsebene nicht detaillierter identifiziert werden. Wie Tabelle 8.1 anhand der Spalte *Anal.* zeigt, wurde die Datenbankdatei nämlich sowohl in Analyse 1 wie auch in Analyse 2 in der selben Weise geändert.

8.2.4.3 Ergebnis auf Datenbankebene

Aufgrund der Feststellung, dass auf Ebene des Dateisystems keine Erkenntnisse zur genauen Repräsentation von d_4 und d_5 zu finden sind, wurde die Datei *Daten/Lexware/Datenbank/F3/lxcompany.db* auf Ebene der Datenbank weiter untersucht. Abbildung 8.10 zeigt in Analogie zur Abbildung 8.9 aus dem vorherigen Abschnitt 8.2.4.2 die Änderungen in der Datenbank und deren Vorkommenshäufigkeit in den Durchläufen. Zur Auswertung wurden nur die Daten aus den Datenbanksicherungen der Analysen eins und zwei heran gezogen. Dies ist dadurch begründet, dass bei der dritten Analyse, wie anhand von Tabelle 8.1 erkennbar keine Änderungen an der Datei *Daten/Lexware/Datenbank/F3/lxcompany.db* vorgenommen wurden. Die Legende *Analyse* in Abbildung 8.10 zeigt aber dennoch eine 3, die in diesem Fall für das Basisimage steht.

Augenscheinlich sind in Abbildung 8.10 deutlich weniger Datenpunkte als in Abbildung 8.9 enthalten. Im Vergleich zu den 2.101 Änderungen im Dateisystem gibt es auf der Ebene der Datenbank auch nur lediglich 48 eindeutige Änderungen. Die Eindeutigkeit wurde über den Tabellennamen und den Primärschlüssel der Einträge bestimmt. Tabelle 8.2 zeigt die Datenbanktabellen an denen Änderungen vorgenommen wurden. Dabei sind nur die Einträge, die 100 mal oder 101 mal vorkommen, aufgeführt.

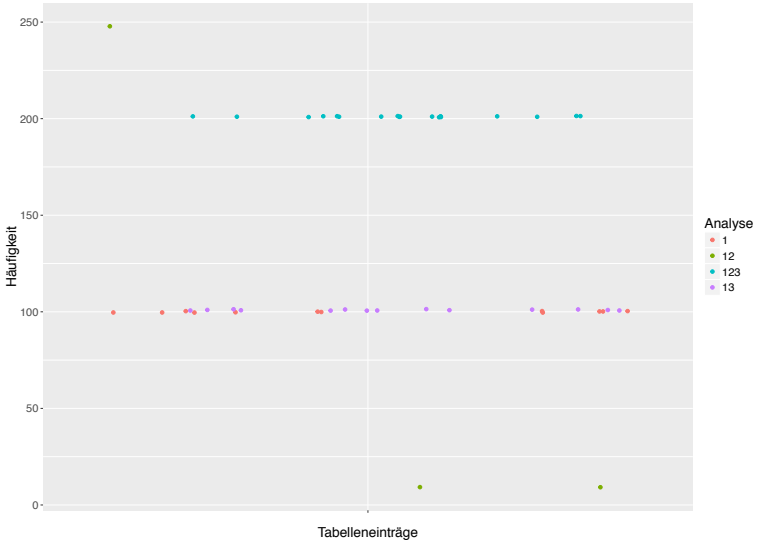


Abbildung 8.10 – Änderungen in der Datenbank

Die Einträge mit einer Vorkommenshäufigkeit von 100 mal sind nur in den Daten aus der Analyse 1 enthalten und die Einträge mit einem Vorkommen von 101 mal sind sowohl in den Datensätzen aus der Analyse 1 als auch im Basisimage enthalten.

Die 100 mal vorkommenden Einträge sind daher neue Einträge, weshalb in der Spalte *Operation* in Tabelle 8.2 *INSERT* als Aktion ausgewiesen ist. Bei den Einträgen, die 101 mal vorkommen, haben sich jeweils ein oder mehrere Attribute geändert, weshalb hier in der Spalte *Operation* von Tabelle 8.2 die Aktion *UPDATE* steht. Die anderen Änderungen kommen entweder in allen Analysen oder gelegentlich vor und sind daher nicht eindeutig für den Prozess der Rechnungserstellung ($P(A)$), weshalb sie nicht aufgeführt sind.

Das Ergebnis der detaillierteren Untersuchung des Schemas der in Tabelle 8.2 aufgeführten Datenbanktabellen ist in Abbildung 8.11 dargestellt. Dabei sind Tabellen in Form von Rechtecken und ausgewählte Attribute der Datenbanktabellen mittels Ellipsen dargestellt. Die orange umrandeten Rechtecke sind die Tabellen, in denen beim Erstellen einer Rechnung eine Änderung vorgenommen wird und die grün umrandeten sowie die grünen Rechtecke stellen die Tabellen dar, in denen Zeilen hinzugefügt werden. Fremdschlüsselbeziehungen zwischen Datenbanktabellen sind in Abbildung 8.11 über die gestrichelten Linien, die jeweils die betroffenen Attribute verbinden dargestellt. Die Darstellung enthält dabei nur die Attribute, die sowohl eine Beziehungsrelation speichern als auch in der Tabelle 8.2 enthalten sind. Andere Beziehungen oder Attribute wurden zur Erhaltung der Übersichtlichkeit in Abbildung 8.11 weggelassen.

Tabelle 8.2 – Digitale Spuren der Prozessausführung in der Datenbank

#	Tabelle	Operation	Anzahl
1	BH_OFFENEPOSTEN	INSERT	1
2	CW_FK_AuftragsPos1	INSERT	1
3	CW_FK_OFFENEPOSTEN_DEB1	INSERT	1
4	FK_Auftrag	INSERT	1
5	FK_AuftragKontakt	INSERT	1
6	FK_AuftragPos	INSERT	1
7	FK_Dokument	INSERT	1
8	FK_KalkAuftragPos	INSERT	1
9	FK_Kontakt	INSERT	1
10	FK_KundeKontakt	INSERT	1
11	FK_PosSum	INSERT	1
12	FK_Vorgang	INSERT	1
13	FK_Kunde	UPDATE	1
14	FK_Nummerkreis	UPDATE	2
15	FK_Preismatrix	UPDATE	1
16	LX_ID	UPDATE	5
17	SYSCOLSTAT	UPDATE	1
18	SYSCOLUMN	UPDATE	4

Neben der genauen Analyse des Schemas ist auch eine inhaltliche Prüfung der Tabellen und einzelner Einträge durchgeführt worden, um d_4 und d_5 genauer zu bestimmen. Dabei konnten die grün ausgefüllten Rechtecke in Abbildung 8.11 als diejenigen Einträge identifiziert werden, die den Datenelementen d_4 und d_5 zuzuordnen sind. Eine genaue Unterscheidung zwischen den beiden Datenelementen ist auf Basis der Daten aus der in Abschnitt 8.2.4.1 beschriebenen Untersuchung jedoch nicht zweifelsfrei möglich. Weiter ergibt sich die Erkenntnis, dass die Erstellung der Rechnung und besonders der Druckvorgang weitere Einträge in der Datenbank erzeugen.

Die grün umrandeten und mit einem Druckersymbol versehenen Rechtecke zeigen die Tabellen, in denen offensichtlich erst beim Drucken des Dokumentes ein Eintrag erzeugt wird. Der Eintrag in der Tabelle *CW_FK_OFFENEPOSTEN_DEB1*, der in Abbildung 8.11 als gestrichelt umrandetes Rechteck dargestellt ist, ist scheinbar nur temporär vorhanden und wird von einem folgenden Prozess wieder entfernt, da der Eintrag beim stichprobenartigen Test für ältere Rechnungen nicht mehr vorhanden war. Für die Einträge in der Tabelle *CW_FK_AuftragsPos1* konnte auf Basis der Daten aus der in Abschnitt 8.2.4.1 beschriebenen Untersuchung kein eindeutiges Schema erkannt werden. Aus diesem Grund ist dieses Rechteck in Abbildung 8.11 ebenfalls gestrichelt umrandet.

Da auf Basis der bislang vorgestellten Ergebnisse der DFA noch keine Aussagen bezüglich charakteristischer Spuren oder etwaiger Spuren-Interferenzen möglich sind, wurde im vierten Analysedurchlauf, wie in Abschnitt 8.2.4.1 erwähnt, zusätzlich die Erstellung eines Angebotes untersucht. Tabelle 8.3 zeigt die Spuren, die bei der

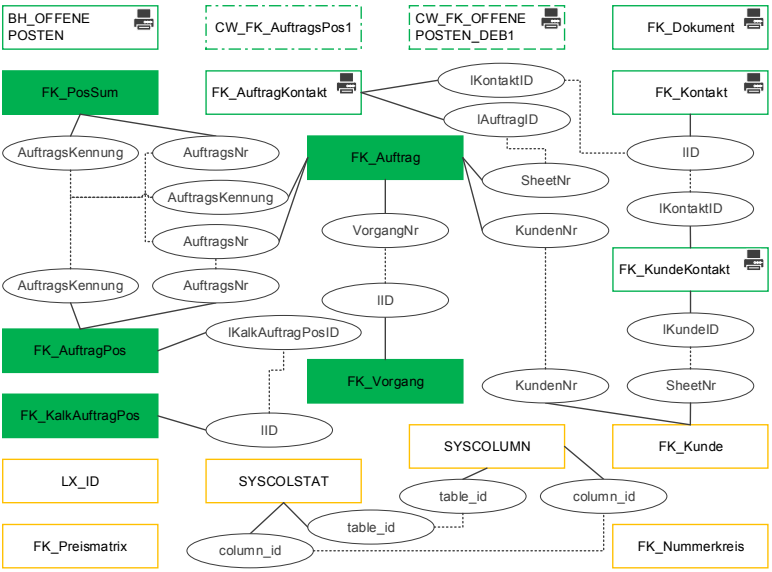


Abbildung 8.11 – Beziehungen der Datenbanktabellen

Erstellung eines Angebotes entstehen ($E(P(C))$) im Vergleich zu den Spuren der Rechnungserstellung ($E(P(A))$). Die Beschriftung der Tabelle 8.3 entspricht der von Tabelle 8.2, wobei zusätzlich die Spalte *Spurentyp* mit dem jeweiligen Typ der digitalen Spuren nach den Definitionen aus Kapitel 6 mit enthalten ist.

Die Änderungen in den Datenbanktabellen, die in den Zeilen 1 - 11 der Tabelle 8.3 eingetragen sind, sind die dem Prozess der Rechnungserstellung bezüglich der Spuren der Erstellung des Angebotes zuzuordnenden charakteristischen Spuren $CE(P(A), \{P(C)\})$. In den Zeilen 12 - 14 der Tabelle 8.3 sind die weiteren Spuren von $P(A)$ angetragen. Im Vergleich mit den Spuren von $P(C)$ ist ersichtlich, dass sich die Spurenmengen hier überschneiden und sowohl $P(A)$ als auch $P(C)$ jeweils eine Zeile in der jeweiligen Datenbanktabelle hinzufügt. Die Spuren sind in Tabelle 8.3 daher als Kontraspuren $XE(P(A))$ von $P(A)$ angegeben bzw. als Spuren $E(P(C))$ von $P(C)$, da $P(C)$ die selben Datenbankzeilen wie $P(A)$, im Sinne von Variablen erzeugt. $P(C)$ belegt den Primärschlüssel aber mit Werten aus anderen Wertebereichen. Davon sind jeweils die Spalten *AuftragsNr* und *AuftragsKennung* in allen drei Datenbanktabellen betroffen. Für $P(C)$ ist W für die *AuftragsKennung* $W = \{0\}$. Für $P(A)$ ist der Wertebereich für die *AuftragsKennung* dagegen $W = \{3\}$. Weiter ist der Wertebereich W für die *AuftragsNr* über einen jeweils anderen Nummernkreis aus der Tabelle *FK_Nummerkreis* bestimmt.

Neben den charakteristischen Spuren von $P(A)$ kann durch die durchgeführte DFA

Tabelle 8.3 – Digitale Spuren von $P(A)$ und $P(C)$ auf Ebene der Datenbank im Vergleich

#	Tabelle	Operation	Anzahl	Spurentyp
1	BH_OFFENEPOSTEN	INSERT	1	$CE(P(A), \{P(C)\})$
2	CW_FK_AuftragsPos1	INSERT	1	
3	CW_FK_OFFENEPOSTEN_DEB1	INSERT	1	
4	FK_AuftragKontakt	INSERT	1	
5	FK_Dokument	INSERT	1	
6	FK_Kontakt	INSERT	1	
7	FK_KundeKontakt	INSERT	1	
8	FK_Kunde	UPDATE	1	
9	SYSCOLUMN	UPDATE	3	
10	FK_Nummerkreis	UPDATE	1	
11	LX_ID	UPDATE	1	
12	FK_Auftrag	INSERT	1	$XE(P(A))$ bzw. $E(P(C))$
13	FK_AuftragPos	INSERT	1	
14	FK_PosSum	INSERT	1	
15	FK_Nummerkreis	UPDATE	1	$CE(P(C), \{P(A)\})$
16	SYSCOLSTAT	UPDATE	1	
17	FK_KalkAuftragPos	INSERT	1	$ME(\{P(A), P(C)\})$
18	FK_Vorgang	INSERT	1	
19	SYSCOLSTAT	UPDATE	1	
20	SYSCOLUMN	UPDATE	1	
21	LX_ID	UPDATE	4	
22	FK_Preismatrix	UPDATE	1	
23	FK_Nummerkreis	UPDATE	1	

zudem auf die charakteristischen Spuren von $P(C)$ in Form der in den Zeilen 15 und 16 von Tabelle 8.3 angegebenen Änderungen an den Datenbanktabellen geschlossen werden. Die Änderungen an den Datenbanktabellen in den Zeilen 17 - 23 von Tabelle 8.3 entsprechen schließlich den gemeinsamen Spuren von $P(A)$ und $P(C)$.

Durch die Ausführung des zu $P(A)$ auf technischer Ebene offensichtlich sehr ähnlichen Prozesses $P(C)$, sind sowohl Interferenzen der Spurenmengen, im Sinne der Ausführungen von Dewald [Dew12, S. 96ff] in Form der gemeinsamen Spuren, als auch charakteristische Spuren von $P(A)$ erkennbar. Natürlich müssten alle mit dem ERP-System bzw. von den Benutzern ausführbaren Operationen im ERP-System getestet werden, um die (charakteristischen) Spuren- und Kontraspurenmengen vollständig zu bestimmen. Durch die zusätzliche inhaltliche Untersuchung der Datenbankeinträge sind auf Basis der Ergebnisse der DFA aber bereits Aussagen möglich. Im folgenden Abschnitt werden diese Ergebnisse aus der DFA kurz zusammengefasst und diskutiert.

8.2.4.4 Erkenntnisse aus der Differential Forensic Analysis

Die Daten aus der DFA zeigen, wie die Datenelemente d_4, d_5 und d_6 aus dem Prozess $P(A)$ im AWS abgespeichert werden. Wenngleich die Ergebnisse mit einer gewissen

Restunsicherheit behaftet sind, da es z.B. weitere Prozesse wie $P(B)$ gibt, die die Spurenmengen unter Umständen beeinflussen könnten, kann mit hoher Wahrscheinlichkeit von der Korrektheit der Schlussfolgerungen ausgegangen werden. Durch eine weiterführende inhaltliche Analyse der Datenbankinhalte konnten z.B. die Einträge in den Tabellen, die in Abbildung 8.11 mit einem grünen Rechteck dargestellt sind, auch für ältere Rechnungen, die mit dem Prozess $P(A)$ erstellt wurden, genau so nachgewiesen werden.

Daneben zeigen auch die in Tabelle 8.3 dargestellten Spuren der Rechnungserstellung im Vergleich zur Erstellung eines Angebotes, dass selbst bei inhaltlich fast identischen Ergebnisdokumenten im Hintergrund ein Unterschied bei den Spurenmengen besteht. Die Spuren-Interferenz ist daher wenig überraschend im Gegensatz zur Erkenntnis, dass rein auf Basis der erstellten Zeilen in den Datenbanktabellen eine Unterscheidung zwischen der Ausführung von $P(A)$ und $P(C)$ möglich ist. Weiter wurde die in Abschnitt 6.1 aufgeworfene Forderung nach dedizierten Werkzeugen zur forensischen Sicherung und Analyse von digitalen Spuren aus den AWS von Unternehmen unterstrichen. Die DFA zeigt, dass ohne solche Werkzeuge die konkrete Repräsentation der Datenelemente in Form der Variablen im AWS nicht ohne weiteres bekannt ist. Zudem könnten auf Basis des Prozessmodells in diesem Fall weder charakteristische Spuren, Spuren-Interferenzen noch Kontraspuren bestimmt werden. Die Datenelemente d_4 und d_5 bzw. d_{13} und d_{14} aus den in Abbildung 8.6 bzw. Abbildung 8.8 dargestellten Prozessausschnitten enthalten hierzu nicht genügend Informationen.

Neben dem primären Ergebnis der Bestimmung von d_4 und d_5 zeigt die Analyse auch, dass das Modell aus Kapitel 6 und insbesondere der Vergleich der Spuren aus Abschnitt 6.3.3 valide sind. Dies trifft sowohl auf die Spuren im Dateisystem, wie in Abschnitt 8.2.4.2 beschrieben, als auch auf die Spuren in der Datenbank, wie in Abschnitt 8.2.4.3 beschrieben, zu. In beiden Fällen entstehen rund um die durch den Prozess beschriebenen digitalen Spuren in Form seiner digitalen Outputs weitere, nicht im Prozess verzeichnete Spuren. Abbildung 8.11 zeigt dies mitunter sehr deutlich anhand der nicht grün ausgefüllten grün bzw. orange umrandeten Rechtecke. Die dort neu hinzugefügten oder veränderten Einträge konnten den Datenelementen d_4 und d_5 im Gegensatz zu den grün ausgefüllten Rechtecken und den Einträgen in den entsprechenden Datenbanktabellen inhaltlich nicht direkt zugerechnet werden.

8.2.5 Unternehmensforensische Untersuchung

Da bei K kein echter Vorfall stattgefunden hat, wurde zur Evaluation der Methodik folgende Untersuchungshypothese anhand einer Bottom-Up Untersuchung überprüft: H_0: Die elektronische Rechnung mit einer bestimmten Nummer wurde durch die Ausführung von $P(A)$ erstellt. Dabei wird davon ausgegangen, dass die elektronische Rechnung bei einem Kunden von K gefunden wurde und unklar ist, ob hier ein Betrug vorliegt. Wie in der ersten Fallstudie aus dem Abschnitt 8.1 könnte es sein, dass

sich jemand unberechtigterweise bereichern möchte und dazu Rechnungen von K gefälscht und in das Buchhaltungssystem des Kunden von K, ähnlich wie die maliziöse Buchhaltungsperson aus dem vorherigen Abschnitt 8.1, eingeschleust hat.

8.2.5.1 Vorbereitung

Vor dem tatsächlichen Start der Untersuchung musste zunächst die Menge der Spuren $E(P(A))$ bestimmt werden. Für das in Abschnitt 8.2.2 vorgestellte formale Prozessmodell und den Prozess $P(A)$ ist $E(P(A))$ definiert als:

$$E(P(A)) = \{\{d_4, d_5, d_6, d_7\}, \{d_4, d_5\}\} \tag{8.1}$$

8.2.5.2 Identifikation

Aufgrund der eingangs, unter Abschnitt 8.2.5 aufgeworfenen Untersuchungshypothese, dass die beim Kunden von K gefundene PDF-Rechnung durch $P(A)$ erzeugt wurde, konnte die Menge der möglichen Instanzen IN im Schritt *Einschränken der Menge IN* eingeschränkt werden. Die Spurenmenge konnte daher ebenfalls reduziert werden und die neue Spurenmenge für die Untersuchung ist:

$$E'(P(A)) = \{\{d_4, d_5, d_6, d_7\}\} \tag{8.2}$$

Auf Basis der neuen Spurenmenge $E'(P(A))$ wurde die Menge der investigativen Datenelemente bestimmt. Diese sind für diesen Fall:

$$Invest(P(A)) = \{d_4, d_5, d_6, d_7\} \tag{8.3}$$

Nach der Bestimmung der potentiell vorhandenen Spuren in Form der investigativen Datenelemente mussten deren Datenspeicherorte identifiziert werden. Wie in Abschnitt 8.2.3 beschrieben sind die Daten des ERP-Systems und damit d_4 und d_5 in der entsprechenden Datenbank des ERP-Systems gespeichert. d_6 ist eine PDF-Datei, die auf dem Server mittels *qvPDF* erstellt und in einem bestimmten Ordner des Dateisystems abgelegt wird. Der Ordner ist über die Konfiguration von *qvPDF* festgelegt. Für d_7 kann zwar der Speicherort bestimmt werden. Hierbei konnte aber, wie bereits unter Abschnitt 8.2.3 erwähnt nicht auf die Daten zugegriffen werden.

Dagegen konnte d_6 in Form der PDF-Datei der elektronischen Rechnung im entsprechenden Verzeichnis gefunden und sichergestellt werden. Die Datei sowie die Inhalte waren plausibel, da keine Veränderungen, weder im Rechnungsinhalt, noch in der äußeren Form, z.B. in den Stammdaten von K, der Rechnungsnummer, der Adresse, usw. festgestellt werden konnten.

Eine Suche in der Datenbank nach den Datenelementen d_4 und d_5 konnte die im Rahmen der DFA im Abschnitt 8.2.4 bestimmten Einträge für die Rechnung in den Datenbanktabellen *FK_Auftrag*, *FK_AuftragPos*, *FK_KalkAuftragPos*, *FK_PosSum*

und *FK_Vorgang* identifizieren. In den Tabellen *FK_AuftragPos* und *FK_KalkAuftragPos* waren mehr als ein Eintrag für die Rechnung vorhanden. Diese entsprechen aber den Rechnungspositionen der elektronischen Rechnung, da diese, anders als die im Rahmen der DFA angelegte Rechnung mehr als eine Position hat. Weiter sind alle Einträge in der Datenbank plausibel und stimmen inhaltlich mit der elektronischen Rechnung, respektive der PDF-Datei überein.

8.2.5.3 Individualisierung

Da in der ersten Phase der Untersuchung bereits eine Begrenzung auf eine mögliche Instanz mit der digitalen Spurenmenge $E(inst(P(A))) = \{d_4, d_5, d_6, d_7\}$ vorgenommen wurde, konnte in dieser Individualisierungsphase nur noch untersucht werden, ob diese spezielle Instanz auch ausgeführt wurde.

Im Rahmen der Identifikation konnten nur die Datenelemente d_4, d_5 und d_6 bestimmt werden. Diese stellen eine Teilmenge der Menge $E(inst(P(A)))$ dar. Da mangels Zugriff auf die Daten das Fehlen von d_7 in diesem Fall nicht gewertet werden konnte, ist an dieser Stelle direkt ein Wechsel in die nächste Untersuchungsphase möglich, weil die Ausführung der Instanz mit $A(inst(P(A))) = \{a_1, a_3, a_4, a_5, a_6, a_9, a_{10}\}$ dadurch sehr wahrscheinlich ist und diese auch die einzig mögliche Instanz war.

8.2.5.4 Assoziation

Da durch das Vorhandensein der Datenelemente d_4, d_5 und d_6 sowie deren inhaltlicher Stimmigkeit aus Sicht der Unternehmensforensik die Ausführung von $P(A)$ als Quelle für diese Daten sehr wahrscheinlich ist, wurde auf die Ausführung von $P(A)$ in Form der Instanz mit $A(inst(P(A))) = \{a_1, a_3, a_4, a_5, a_6, a_9, a_{10}\}$ geschlossen.

Für die Aufgaben a_1, a_5 und a_6 gibt es generell keine digitalen Outputs, die im Prozess definiert sind. Hierbei hätten zur weiteren Überprüfung Informationen aus einer klassischen digitalen forensischen Untersuchung oder einer nicht-digitalen forensischen Untersuchung mit betrachtet werden müssen, z.B. ob die Papierrechnung oder Regieberichte im Archiv vorhanden sind. Die digitale forensische Untersuchung hätte zudem die weiteren im Rahmen der DFA, wie in Abschnitt 8.2.4.3 beschrieben, identifizierten digitalen Spuren aufdecken können. Dadurch hätte unter Umständen auf den Druckvorgang, wie er sowohl für die elektronische Rechnung als auch für die Papierrechnung ausgeführt wird geschlossen werden können.

8.2.6 Ergebnisse

Sowohl die DFA, deren Ergebnisse in Abschnitt 8.2.4 beschrieben sind, wie auch die unternehmensforensische Untersuchung anhand der Echtdaten von K haben gezeigt, dass das in Kapitel 6 vorgestellte Modell sowie die darauf aufbauende Methodik aus Kapitel 7 funktionieren. Wenngleich auch die Grenzen der Unternehmensforensik, insbesondere aufgrund von fehlenden Informationen zu den digitalen Spuren des Druckvorgangs im

Prozessmodell anhand der Untersuchung offenkundig wurden, so war die Assoziation zwischen den digitalen Daten und deren Herkunft aus der Prozessausführung eines bestimmten Prozesses dennoch möglich.

Neben der erneuten erfolgreichen Evaluation der Methodik und des Modells hat dieser Fall auch die bereits in Abschnitt 6.1 identifizierte Notwendigkeit dedizierter und auf die AWS von Unternehmen zugeschnittener Tools für digitale forensische Untersuchungen unterstrichen. Da kein Tool für das spezifische AWS von K identifiziert werden konnte, war die Durchführung einer DFA essentiell, um die digitalen Spuren, die durch die Prozessausführung entstehen zu bestimmen.

8.3 Bewertung der Methodik

Die Methodik für unternehmensforensische Untersuchungen, das formale Prozessmodell sowie die Definition der digitalen Spuren von Prozessen konnte in den vorherigen beiden Abschnitten 8.1 und 8.2 erfolgreich evaluiert werden. In beiden Fällen konnten die forensischen Prinzipien mittels der Methodik angewandt und Assoziationen auf Basis der vom Prozessmodell abgeleiteten digitalen Spuren hergestellt werden.

Neben dem Gesamtergebnis der Evaluation wurden im Detail auch Vor- und Nachteile der unternehmensforensischen Untersuchungsmethodik offenkundig. Neben der großen Abhängigkeit vom Prozessmodell zeigt sich besonders bei der Evaluation der Methodik anhand der Echtdaten in Abschnitt 8.2, dass das Prozessmodell keine vollständige Beschreibung der weiteren vom AWS erzeugten Daten enthält. Hierbei ist daher ganz deutlich die Grenze zwischen der Unternehmensforensik, auf Basis von Prozessmodellen, und der digitalen Forensik im Allgemeinen erkennbar.

Neben der durch das Design begrenzten Sichtweise auf digitale Spuren in der Unternehmensforensik ist im Prozessmodell die Persistenz der Datenelemente nicht zwangsweise erkennbar. So kann es sein, dass digitale Outputs nur temporär entstehen und noch während des Prozessablaufs wieder gelöscht werden. Daher ist auch das Wissen über die konkrete Speicherung von Datenelementen essentiell für eine erfolgreiche unternehmensforensische Untersuchung. Zwar ist sowohl die Methodik für unternehmensforensische Untersuchungen wie auch das Modell aus Kapitel 6 unabhängig von der jeweiligen Implementierung. Ohne das Wissen über die konkrete Implementierung und Speicherung von Datenelementen kann aber nur die theoretisch mögliche digitale Spurenmenge bestimmt werden. Weiter wären weder die vollständige Identifikation noch die Individualisierung ohne das Wissen über die konkrete Implementierung der Datenelemente möglich. Die Notwendigkeit der DFA für die Untersuchung im Abschnitt 8.2 wie auch der Bedarf an Tools zur digitalen forensischen Untersuchung von AWS, wie in Abschnitt 6.1 identifiziert, leiten sich mitunter direkt aus dieser Problematik ab und unterstreichen diese.

Neben den begrenzenden Faktoren haben sich aber auch die Vorteile der Methodik gezeigt. Gerade der in Abschnitt 8.1 beschriebene Fall demonstriert, dass sich mit-

hilfe unternehmensforensicher Untersuchungen auf Basis von Prozessmodellen die zu erwartenden digitalen Spuren sicher bestimmen lassen. Auch ist das Prozessmodell sowie die Methodik, wie bereits im vorherigen Absatz erwähnt unabhängig von der jeweiligen konkreten Implementierung. Dies ist zwar, wie im vorherigen Absatz beschrieben einerseits ein Problem, da die konkrete Implementierung der Speicherung von Datenelementen zur Spurensicherung bekannt sein muss. Andererseits ist diese Unabhängigkeit von der Implementierung aber auch von Vorteil. Gerade im Bereich der Wirtschaftskriminalität reichen die Fälle oft Jahre in die Vergangenheit zurück, was unter anderem auch bei dem in Abschnitt 8.1 beschriebenen Vorfall der Fall war. Durch den ständigen Wandel in Unternehmen kann die Implementierung bereits auf eine neuere Version migriert worden oder gänzlich obsolet geworden sein. Auch hier wäre es aber immer noch möglich, die neue oder geänderte Implementierung von Datenelementen heraus zu finden. Weiter könnten alle theoretisch zu erwartenden digitalen Spuren durch historische Prozessmodelle immer noch bestimmt werden.

Ein zusätzlicher, bereits in Abschnitt 6.3.3 angeschnittener Vorteil der Unternehmensforensik auf Basis von Prozessmodellen wird ebenfalls anhand der Evaluationsergebnisse deutlich: Die Bestimmung und die Verfolgung von digitalen Spuren ist nicht auf die Grenzen eines digitalen Systems beschränkt. Anders als in der digitalen Forensik im Allgemeinen können digitale Spuren in mehreren und digital völlig isolierten Systemen bestimmt und für die Assoziation als Gesamtpaket digitaler Spuren eines Prozesses verwendet werden. In der in Abschnitt 8.1 betrachteten Fallstudie waren dies das Buchhaltungssystem sowie das System der Bank. Bei der Untersuchung in Abschnitt 8.2 waren dies die PDF-Dateien im Dateisystem sowie die Daten in der Datenbank des ERP-Systems. Beim ersten, in Abschnitt 8.1 beschriebenen Fall waren die Systeme tatsächlich isoliert und im zweiten Fall, der in Abschnitt 8.2 beschrieben ist, waren die beiden Anwendungen auf ein und demselben System installiert, wenngleich auch hier eine Trennung möglich wäre.

Neben der Identifikation und Betrachtung von digitalen Spuren aus isolierten Systemen ergibt sich ein weiterer Vorteil der unternehmensforensischen Methodik. Wenngleich immer mehr Daten nur noch digital vorliegen und automatisiert und durchgängig verarbeitet werden, so finden sich doch immer noch Medienbrüche. Hierbei geht die digitale Verbindung zwischen den Datenelementen oft verloren, wie der in Abschnitt 8.1 beschriebene Fall durch den Medienbruch zwischen dem Buchhaltungssystem bei B und dem Banksystem bei C zeigt. Die Unternehmensforensik kann aber dennoch die digitalen Spuren über Systemgrenzen hinweg identifizieren und in Verbindung bringen.

Gerade die letztgenannten Vorteile zeigen das Potential der Unternehmensforensik auf Basis von Prozessmodellen. Obwohl Nachteile existieren, ist die Methodik für unternehmensforensische Untersuchungen für viele Fälle anwendbar und bietet ein theoretisch fundiertes Vorgehen zur Anwendung der forensischen Prinzipien bei der digitalen forensischen Untersuchung von AWS in Unternehmen.

KAPITEL 9

Zukünftige Entwicklungen

Teil der *Schlussfolgerung* im Sinne der in Abschnitt 1.3 vorgestellten und in diesem Forschungsvorhaben verwendeten Methodik ist das Aufwerfen neuer Problemstellungen für zukünftige Forschungsvorhaben [VK07]. Die zukünftigen Problemstellungen ergeben sich in dieser Arbeit aus den Ergebnissen der im vorigen Kapitel 8 vorgestellten Evaluation der Methodik für unternehmensforensische Untersuchungen, der Literaturrecherche in Kapitel 4 sowie der Abgrenzung und Definition der Unternehmensforensik in Abschnitt 6.1. In den folgenden Abschnitten 9.1 und 9.2 werden die aufgedeckten Problemstellungen zusammengefasst und detailliert vorgestellt.

9.1 Werkzeuge für unternehmensforensische Untersuchungen

Untersuchungswerkzeuge zur Datenextraktion und Analyse
Durch die in Kapitel 4 vorgestellte Literaturstudie konnte der Bedarf für Werkzeuge zur forensisch sicheren Extraktion und Analyse von digitalen Spuren aus AWS identifiziert werden. Der Bedarf wurde durch die Evaluation der Methodik für unternehmensforensische Untersuchungen in der Praxis, wie in Abschnitt 8.2 vorgestellt zudem bestätigt. Sowohl in der Literatur als auch auf dem freien Markt konnte für die von der KMU verwendete Software kein Tool zur forensischen Sicherung und Analyse der digitalen Spuren aus dem AWS identifiziert werden.

Wenngleich Tools wie der in [FKS+13] vorgestellte Prototyp zur Rekonstruktion von Datenbankoperationen für *InnoDB* über Redologs existieren, so sind diese für die Anwendung bei unternehmensforensischen Untersuchungen eher ungeeignet, da z.B. die in Abschnitt 8.1 dargestellte Fallstudie zeigt, dass Fälle auch Jahre in die Vergangenheit reichen können, womit Logs aufgrund ihrer oft nur begrenzten zeitlichen Aufbewahrung

als Quelle für digitale Spuren vielfach ausscheiden. Für die in Abschnitt 8.2 vorgestellte Untersuchung hätte der in [FKS+13] vorgestellte Prototyp zudem keinen Nutzen, da dieser nur für *InnoDB* und nicht für die in *Sybase Adaptive Server Anywhere* verwendete Datenbankengine geschrieben ist und das vom ERP-System verwendete Datenbankschema nicht kennt.

Durch ein generisches Tool wären zudem auch keine Aussagen bezüglich der genauen Repräsentation von Datenelementen möglich. Neben der Extraktion und Sicherung der Daten muss für deren Analyse aber die Struktur und Semantik bekannt sein. Wie die in Abschnitt 8.2 vorgestellte Untersuchung zeigt, konnten aus den Datenbankdateien auf Basis der Daten aus dem Dateisystem keine brauchbaren Aussagen bezüglich der Datenelemente aus dem Prozess getroffen werden. Zur forensischen Analyse der Datenbank und zum Treffen von Aussagen bezüglich der ausgeführten Prozesse sind die genaue Kenntnis der durch das ERP-System ausgelösten Operationen und deren (persistente) digitale Spuren in der Datenbank daher essentiell. Ein Tool für die forensische Untersuchung von Unternehmenssoftware müsste eben diese Operationen und die dadurch entstehenden Daten kennen, um eine gezielte Extraktion und anschließende Analyse der digitalen Spuren aus den Datenspeichern des AWS zu ermöglichen.

Architektur für die Differential Forensic Analysis von Anwendungssystemen

Zur Erstellung von Tools für unternehmensforensische Untersuchungen braucht es zudem Methoden, um die genaue bei der Nutzung von AWS für bestimmte Operationen entstehende Menge an digitalen Spuren zu bestimmen. Zur Durchführung einer DFA gibt es für dieses Umfeld aber bislang ebenfalls keine öffentlich bekannten und auf AWS zugeschnittenen Werkzeuge.

Für die in Abschnitt 8.2.4 vorgestellte DFA wurde auf Basis der Erkenntnisse aus [KDF13] eine entsprechende Architektur abgeleitet, implementiert und die Analyse durchgeführt. Eine automatisierte Erstellung und Wiederverwendung von Fingerprints, im Sinne von [KDF13] war mangels entsprechend verfügbarer Tools allerdings nicht möglich. Aus diesem Grund gibt es neben den fertigen Tools für die Nutzung bei unternehmensforensischen Untersuchungen auch einen Bedarf an Methoden und Tools zur Erstellung von Fingerprints von Operationen der AWS.

9.2 Weiterentwicklung der Methodik

Neben den Tools, die die forensische Sicherung und Extraktion für typischerweise nur in Unternehmen zu findenden AWS unterstützen, kann auch die Methodik selbst durch ein Tool unterstützt werden. Bei den beiden in Kapitel 8 vorgestellten Evaluationen wurden nur vergleichsweise kleine abgegrenzte Prozesse untersucht, wodurch die manuelle Erstellung und die Handhabung der formalen Prozesse gut möglich war. Für größere Mengen an Gesamtprozessen GP wird die Erstellung der formalen Prozesse aber sehr

schnell zeitaufwändig und komplex. Weiter sind die formalen Prozesse dann schlecht zu handeln, da durch die vielen Mengen der Überblick verloren gehen kann. Ein Tool könnte daher sowohl die (teil)automatisierte Überführung von Prozessmodellen, die Verwaltung der formalen Prozesse und die praktische Durchführung einer unternehmensforensischen Untersuchung nach der in Kapitel 7 vorgestellten Methodik unterstützen.

Ein weiterer Schritt wäre dann die Integration des Tools zur Unterstützung der Methodik mit den im vorigen Abschnitt 9.1 geforderten Tools zur forensischen Sicherung und Analyse der digitalen Spuren aus den AWS. Dadurch könnten unter Umständen auch Teile der Analyse automatisiert werden. Das Tool könnte anhand einer digitalen Spur eines Prozesses z.B. alle weiteren infrage kommenden Prozesse bestimmen und anschließend prüfen, welche digitalen Spuren der investigativen Spurenmenge $Invest(P)$ vorhanden sind. Dadurch wäre eine schnelle und dennoch zuverlässige Assoziation und Rekonstruktion auch in umfangreichen und massiv verteilten AWS denkbar. Die genauen Anforderungen eines solchen Tools sowie die tatsächlichen Vorteile müssen allerdings durch weitere Forschungsvorhaben umfassend entwickelt und evaluiert werden.

KAPITEL 10

Schlussfolgerungen

Dieses Forschungsvorhaben wurde durch den steigenden Bedarf an digitalen Spuren bei der Aufklärung von Verbrechen in Unternehmen motiviert. Der Bedarf ergibt sich unter anderem durch die stetig fortschreitende Digitalisierung, die Vernetzung und Integration von Informationssystemen unterschiedlichster Organisationen sowie die hohe Automatisierung und die dadurch entstehenden Risiken von Angriffen. Weiter nimmt die Menge an nicht elektronisch vorliegenden Dokumenten stetig ab. Bereits heute liegen viele der elektronisch erzeugten geschäftlichen Dokumente und geschäftsrelevanten Informationen nur noch in elektronischer Form vor [MZ11, S. 214],[Bec15, S. 319].

Die Unternehmensforensik und die Methodik für unternehmensforensische Untersuchungen stellen das zentrale Ergebnis dieser Arbeit dar. Sie adressieren den steigenden Bedarf an digitalen Spuren bei forensischen Untersuchungen in Unternehmen. Im folgenden Abschnitt 10.1 werden die zentralen Forschungsergebnisse der Arbeit nun detailliert im Rahmen der Forschungsfragen betrachtet. Im Abschnitt 10.2 werden dann abschließend die Ergebnisse der einzelnen Kapitel zusammengefasst und dargestellt.

10.1 Forschungsfragen

Die Agenda dieses Forschungsvorhabens war an den in Abschnitt 1.2 aufgeworfenen Forschungsfragen ausgerichtet. Im Folgenden werden die Ergebnisse und Antworten für jede der Forschungsfragen kritisch betrachtet und zusammengefasst.

Was sind die wesentlichen organisatorischen, personellen und technischen Maßnahmen welche in einem Unternehmen zur Vorbereitung auf digitale forensische Untersuchungen implementiert werden sollten und wie etabliert sind diese Maßnahmen in der Praxis?

Die Forschungsfrage nach den wesentlichen organisatorischen, personellen und technischen Maßnahmen, die Unternehmen zur Vorbereitung auf digitale forensische Untersuchungen implementieren sollten wird durch das Ergebnis der Literaturrecherche aus Abschnitt 4.2 beantwortet. Im Ergebnis konnten sowohl technische, organisatorische wie auch personelle Maßnahmen identifiziert werden. Wenngleich der Maßnahmenkatalog im Rahmen der Arbeit nicht in der Praxis evaluiert wurde, so bietet er dennoch eine gute Übersicht über zu implementierende Maßnahmen zur Vorbereitung auf digitale forensische Untersuchungen und fasst den Stand der Forschung in diesem Bereich zusammen.

In der Praxis findet bislang kaum eine Umsetzung der Maßnahmen statt, was die Ergebnisse der in Kapitel 5 vorgestellten Studie sowie die beiden vergleichbaren Studien, die in Abschnitt 5.5 betrachtet wurden, zeigen. Durch den Maßnahmenkatalog aus Abschnitt 4.2 kann aber das durch die Studie identifizierte Argument hinsichtlich fehlender Best Practice Ansätze als Grund für die fehlende *Forensic Readiness* größtenteils ausgeräumt werden. Die Evaluation und besonders die Bewertung der Wirksamkeit der Maßnahmen kann aber nur durch deren Bewertung nach einer tatsächlich stattgefundenen digitalen forensischen Untersuchung in der Praxis erfolgen.

Wie funktionieren digitale forensische Untersuchungen? Welche grundlegenden Methoden und Prinzipien gibt es in der digitalen Forensik?
Die wissenschaftlichen Grundsätze, Methoden und Prinzipien der forensischen Wissenschaften sowie der digitalen Forensik im Speziellen wurden in Kapitel 2 ausführlich diskutiert. Die durch die Ausführungen in Kapitel 2 gewonnenen Erkenntnisse zeigen, dass sich die digitale Forensik nach und nach zu einer *echten* forensischen Wissenschaft entwickelt. Weiter basieren die in der digitalen Forensik gültigen Prinzipien auf den grundlegenden Prinzipien forensischer Wissenschaften im Allgemeinen. Durch die Ausführungen in Kapitel 2 wird diese Forschungsfrage zudem beantwortet.

Was ist eine digitale Spur aus Sicht der Informationssysteme von Unternehmen?
Zur Beantwortung der Forschungsfrage 3 wurden im Kapitel 3 zunächst die Begriffe Informationssystem, Anwendungssystem sowie die Prozesse und deren Rolle in Unternehmen diskutiert. Anschließend wurde der aktuelle Stand bezüglich der Problemlösungsstrategien in der Literatur im Kapitel 4 ausführlich anhand zweiter strukturierter Literaturrecherchen untersucht.

Auf Basis der Ergebnisse aus den Kapiteln 2 - 4 wurden dann der digitale Spurenbegriff im Kontext der Informations- bzw. Anwendungssysteme in Unternehmen im Kapitel 6 umfassend definiert und die Grundlagen für die Beantwortung der Forschungsfrage 4 geschaffen. Durch das digitale Spurenverständnis über das in Kapitel 6 entwickelte Modell wird die Forschungsfrage umfassend beantwortet.

Wie kann man die grundlegenden digitalen forensischen Prinzipien im Kontext der Informationssysteme von Unternehmen anwenden?
Durch die Übertragung der in Kapitel 2 aufgezeigten Grundlagen und Prinzipien forensischer Wissenschaften auf die Unternehmensforensik wurde in Kapitel 7 eine Methodik zur Durchführung unternehmensforensischer Untersuchungen vorgestellt. Die Methodik als zentrales Ergebnis dieser Arbeit beantwortet zudem diese Forschungsfrage, indem eine Möglichkeit, die forensischen Prinzipien in der Praxis bei unternehmensforensischen Untersuchungen anzuwenden, gezeigt wurde.

Die Anwendbarkeit, Gültigkeit und grundsätzliche Funktion der Problemlösungsstrategie wurde zudem in Kapitel 8 evaluiert. Die Evaluationsergebnisse bestätigen, dass die Methodik grundsätzlich gültig und auch in der Praxis anwendbar ist.

10.2 Zusammenfassung der Ergebnisse

Die Antworten auf die Forschungsfragen aus dem vorigen Abschnitt 10.1 zeigen bereits einen guten Überblick der Ergebnisse dieser Arbeit auf. In diesem Abschnitt werden nun die Ergebnisse der einzelnen Kapitel abschließend zusammengefasst dargestellt.

In Kapitel 1 wurde das Thema dieser Arbeit motiviert und die Forschungsfragen sowie die Forschungsmethodik des Forschungsvorhabens vorgestellt. Die Motivation ergibt sich durch den steigenden Bedarf an digitalen Spuren bei der Aufklärung von Verbrechen in Unternehmen. Dieser Bedarf ist bedingt durch neue Risiken für Angriffe, durch die hohe Automatisierung sowie Vernetzung und Integration von Informationssystemen unterschiedlichster Organisationen und die stetig fortschreitende Digitalisierung, durch die immer mehr Spuren nur als digitale Spuren vorliegen.

Die Grundlagen zur digitalen Forensik sowie zu forensischen Wissenschaften wurden im anschließenden Kapitel 2 ausführlich diskutiert. Dazu wurden neben den Definitionen von Grundbegriffen sowie der Vorstellung der Grundprinzipien forensischer Wissenschaften im Allgemeinen sowohl digitale Spuren auf abstrakter als auch auf formaler Ebene vorgestellt. Im Ergebnis zeigt sich, dass die digitale Forensik heute als forensische Wissenschaft bezeichnet werden kann und die Qualität der Lösungen sowie die wissenschaftliche Strenge stetig steigen.

Im Kapitel 3 wurden anfangs die Begrifflichkeiten zu betrieblichen Informationssystemen sowie der grundsätzliche Aufbau und die Funktionsweise der Informations- und Anwendungssysteme betrachtet. Weiter wurde auf das Zusammenspiel von Prozessen und AWS sowie die Prozessmodellierung eingegangen. Prozesse wurden dabei als zentraler Mediator zwischen der Gestaltung, dem Aufbau und dem Betrieb der Informationssysteme sowie den betrieblichen Aufgaben identifiziert.

Kapitel 4 betrachtet die vorhandenen Problemlösungsstrategien der digitalen Forensik in Unternehmen anhand von strukturierten Literaturrecherchen. Durch diese Literaturrecherchen wurden sowohl vorbereitende Maßnahmen aus dem Themenbereich *Forensic Readiness* wie auch Vorgehensmodelle, Methoden und Werkzeuge für

digitale forensische Untersuchungen in Unternehmen identifiziert. Weiter wurde ein Maßnahmenkatalog für die Vorbereitung von Unternehmen auf digitale forensische Untersuchungen aus der Literatur zur *Forensic Readiness* zusammengestellt.

Die Implementierung und Verwendung der in Kapitel 4 untersuchten vorbereitenden Maßnahmen sowie die Verwendung von Methoden aus der digitalen Forensik in Unternehmen wurden anhand der in Kapitel 5 vorgestellten Studie untersucht. Bei der Studie wie auch bei ebenfalls einbezogenen vergleichbaren Studien zeigt sich, dass sich Unternehmen noch kaum auf digitale forensische Untersuchungen vorbereiten.

Auf Basis der Grundlagenkapitel sowie der Erkenntnisse aus den Literaturrecherchen und der Studie aus den Kapiteln 4 und 5 wurde in Kapitel 6 zunächst die Unternehmensforensik als Teildisziplin der digitalen Forensik abgegrenzt und definiert. Anschließend wurden die formalen digitalen Spuren aus der digitalen Forensik im Allgemeinen auf die digitalen Spuren von Prozessen transferiert. Durch die Definition der formalen digitalen Spuren von Prozessen wurde schließlich die theoretische Basis für unternehmensforensische Untersuchungen geschaffen.

In Kapitel 7 wurde anhand der formalen digitalen Spuren sowie des theoretischen Fundamentes aus Kapitel 6 eine Methodik für unternehmensforensische Untersuchungen entworfen. Die Methodik integriert dabei die Grundprinzipien forensischer Wissenschaften und die dabei gültige Vorgehensweise mit den formalen digitalen Spuren von Prozessen, um eine digitale forensische Untersuchung in den oftmals sehr komplexen AWS von Unternehmen zu ermöglichen.

Die Evaluation der in Kapitel 7 entworfenen Methodik wurde anhand einer theoretischen Fallstudie, die auf Basis eines echten Falles erstellt wurde, sowie der Anwendung der Methodik in der Praxis vorgenommen. In Kapitel 8 wurden die Ergebnisse der Evaluation vorgestellt und ausführlich diskutiert. Durch die Evaluation zeigt sich, dass die Methodik in der Praxis anwendbar ist und das formale Modell digitaler Spuren, dass dieser als Basis dient, auch in der Praxis gültig ist.

In Kapitel 9 wurden die durch das Forschungsvorhaben noch nicht zufriedenstellend gelösten Probleme der Unternehmensforensik diskutiert. Daraus wurde anschließend weiterer Forschungsbedarf für die Unternehmensforensik abgeleitet und konkrete Problemstellungen und voraussichtliche Lösungsstrategien definiert. Zukünftig müssen besonders Methoden und Werkzeuge zur forensischen Sicherung und Analyse von digitalen Spuren aus den AWS von Unternehmen entwickelt werden. Aber auch der Einsatz der in dieser Arbeit vorgestellten Methodik sollte zukünftig durch ein Softwaretool unterstützt werden, damit das volle Potential der Unternehmensforensik genutzt werden kann.

Literaturverzeichnis

[ABB+12] Anderson, Ross ; Barton, Chris ; Böhme, Rainer ; Clayton, Richard ; van Eeten, Michael ; Levi, Michael ; Moore, Tyler ; Savage, Stefan: Measuring the Cost of Cybercrime. In: *11th Annual Workshop on the Economics of Information Security (WEIS)*, 2012

[AK15] Aagesen, Gustav ; Krogstie, John: BPMN 2.0 for Modeling Business Processes. In: *Handbook on Business Process Management 1*. Springer Berlin Heidelberg, 2015

[AN95] Anderson, Ross ; Needham, Roger: Programming Satan's computer. In: *Computer Science Today*. Springer Berlin Heidelberg, 1995, S. 426–440

[AS04] Aguilar-Savén, Ruth S.: Business process modelling: Review and framework. In: *International Journal of Production Economics* 90 (2004), Nr. 2, S. 129–149

[AS06] Aier, Stephan ; Schönherr, Marten: Status quo geschäftsprozessorientierter Architekturintegration. In: *WIRTSCHAFTSINFORMATIK* 48 (2006), Nr. 3, S. 188–197

[ASM+12] Ahlemann, Frederik ; Stettiner, Eric ; Messerschmidt, Marcus ; Legner, Christine ; Schäfczuk, Daniel: Introduction. In: *Strategic Enterprise Architecture Management*. Springer Berlin Heidelberg, 2012, S. 1–33

[Ass07] Association of Chief Police Officers: *Good Practice Guide for Computer-Based Electronic Evidence*. 2007

[AWJT11] Alharbi, Soltan ; Weber-Jahnke, Jens H. ; Traoré, Issa: The Proactive and Reactive Digital Forensics Investigation Process: A Systematic

Literature Review. In: *Information Security and Assurance (ISA)*, 2011, S. 87–100

[AWS11] ACCORSI, Rafael ; WONNEMANN, Claus ; STOCKER, Thomas: Towards Forensic Data Flow Analysis of Business Process Logs. In: *Proceedings of the 2011 Sixth International Conference on IT Security Incident Management and IT Forensics (IMF)*, 2011, S. 3–20

[BC05] BEEBE, Nicole L. ; CLARK, Jan G.: A hierarchical, objectives-based framework for the digital investigations process. In: *Digital Investigation* 2 (2005), Nr. 2, S. 147–167

[Bec15] BECKER, Michael: Auf der Suche nach der Nadel im Heuhaufen – IT-Forensik bei Compliance-Verstößen. In: *Compliance 2015*. Helios Media, 2015

[Bee09] BEEBE, Nicole: Digital Forensic Research: The Good, the Bad and the Unaddressed. In: *Advances in Digital Forensics V*, Springer Berlin Heidelberg, 2009, S. 17–36

[BFGK09] BÖHME, Rainer ; FREILING, Felix C. ; GLOE, Thomas ; KIRCHNER, Matthias: Multimedia-Forensik als Teildisziplin der digitalen Forensik. In: *Informatik 2009: Im Focus das Leben, Beiträge der 39. Jahrestagung der Gesellschaft für Informatik e.V. (GI)*, 2009, S. 1537–1551

[BJS11] BURD, Stephen D. ; JONES, Darrin E. ; SEAZZU, Alessandro F.: Bridging Differences in Digital Forensics for Law Enforcement and National Security. In: *Proceedings of the 2011 44th Hawaii International Conference on System Sciences (HICSS)*, 2011, S. 1–6

[BK02] BREZINSKI, Dominique P. ; KILLALEA, Tom: Guidelines for Evidence Collection and Archiving / Internet Engineering Task Force. Version: 2002. http://www.rfc-editor.org/rfc/rfc3227.txt. 2002. – Forschungsbericht

[BK12] BECKER, Jörg ; KAHN, Dieter: Der Prozess im Fokus. In: *Prozessmanagement*. Springer Berlin Heidelberg, 2012

[BKSL08] BAEK, Eunju ; KIM, Yeog ; SUNG, Jinwon ; LEE, Sangjin: The Design of Framework for Detecting an Insider's Leak of Confidential Information. In: *Proceedings of the 1st International Conference on Forensic Applications and Techniques in Telecommunications, Information, and Multimedia and Workshop (e-Forensics)*, 2008, S. 14–17

[Bla11] BLACKWELL, Clive: An Investigative Framework for Incident Analysis. In: *Advances in Digital Forensics VII*, Springer Berlin Heidelberg, 2011, S. 23–34

[Bla12] Blackwell, Clive: A Forensic Framework for Incident Analysis Applied to the Insider Threat. In: *Digital Forensics and Cyber Crime*. Springer Berlin Heidelberg, 2012, S. 268–281

[BRR06] Brinson, Ashley ; Robinson, Abigail ; Rogers, Marcus: A cyber forensics ontology: Creating a new approach to studying cyber forensics. In: *Digital Investigation* 3 (2006), S. 37–43

[BRU00] Becker, Jörg ; Rosemann, Michael ; Uthmann, Christoph von: Guidelines of Business Process Modeling. In: *Business Process Management*. Springer Berlin Heidelberg, 2000, S. 30–49

[BSJ10] Barske, David ; Stander, Adrie ; Jordaan, Jason: A Digital Forensic Readiness Framework for South African SME's. In: *Information Security South Africa Conference (ISSA)*, 2010

[Bun14a] Bundesamt für Sicherheit in der Informationstechnik: *Die Lage der IT-Sicherheit in Deutschland 2014*. 2014

[Bun14b] Bundesministerium der Finanzen: *Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)*. http://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/Datenzugriff_GDPdU/2014-11-14-GoBD.pdf. Version: 2014, Abruf: 16.04.2016

[BV96] Becker, Jörg ; Vossen, Gottfried: Geschäftsprozeßmodellierung und Workflow-Management: Eine Einführung. In: *Geschäftsprozessmodellierung und Workflow-Management*. Internat. Thomson Publ., 1996, S. 17–26

[Car03] Carrier, Brian: Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers. In: *International Journal of Digital Evidence (IJDE)* (2003), Nr. 1

[Car06] Carrier, Brian D.: *A hypothesis-based approach to digital forensic investigations*, Purdue University, Diss., 2006

[Car09] Carrier, Brian D.: Digital Forensics Works. In: *IEEE Security and Privacy* 7 (2009), Nr. 2, S. 26–29

[Cas05] Casey, Eoghan: Case study: Network intrusion investigation – lessons in forensic preparation. In: *Digital Investigation* 2 (2005), Nr. 4, S. 254–260

[Cas09] CASEY, Eoghan: Digital forensics: Coming of age. In: *Digital Investigation* 6 (2009), Nr. 1-2, S. 1–2

[Cas11] CASEY, Eoghan: *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. 3. Academic Press, 2011

[Cas13a] CASEY, Eoghan: Experimental design challenges in digital forensics. In: *Digital Investigation* 9 (2013), Nr. 3-4, S. 167–169

[Cas13b] CASEY, Eoghan: Triage in digital forensics. In: *Digital Investigation* 10 (2013), Nr. 2, S. 85–86

[CBC11] COHEN, Michael I. ; BILBY, Darren ; CARONNI, Germano: Distributed forensics and incident response in the enterprise. In: *Digital Investigation* 8 (2011), S. 101–110

[CFGS11] CASEY, Eoghan ; FELLOWS, Geoff ; GEIGER, Matthew ; STELLATOS, Gerasimos: The growing impact of full disk encryption on digital forensics. In: *Digital Investigation* 8 (2011), Nr. 2, S. 129–134

[CG09] COMBI, Carlo ; GAMBINI, Mauro: Flaws in the Flow: The Weakness of Unstructured Business Process Modeling Languages Dealing with Data. In: *On the Move to Meaningful Internet Systems (OTM)*. Springer Berlin Heidelberg, 2009, S. 42–59

[CKO92] CURTIS, Bill ; KELLNER, Marc I. ; OVER, Jim: Process modeling. In: *Communications of the ACM* 35 (1992), Nr. 9, S. 75–90

[CLP11] COHEN, Fred ; LOWRIE, Julie ; PRESTON, Charles: The State of the Science of Digital Evidence Examination. In: *Advances in Digital Forensics VII*, Springer Berlin Heidelberg, 2011, S. 3–21

[CM11] CARLTON, Gregory H. ; MATSUMOTO, Joseph: A Survey of Contemporary Enterprise Storage Technologies from a Digital Forensics Perspective. In: *Journal of Digital Forensics, Security and Law* 6 (2011), Nr. 3, S. 63–74

[Coh10] COHEN, Fred: Toward a Science of Digital Forensic Evidence Examination. In: *Advances in Digital Forensics VI*, Springer Berlin Heidelberg, 2010, S. 17–35

[CS04] CARRIER, Brian D. ; SPAFFORD, Eugene H.: Defining Event Reconstruction of Digital Crime Scenes. In: *Journal of Forensic Sciences* 49 (2004), Nr. 6, S. 1–8

[CS06] CARRIER, Brian D. ; SPAFFORD, Eugene H.: Categories of digital investigation analysis techniques based on the computer history model. In: *Digital Investigation* 3 (2006), S. 121–130

[Dav93] Davenport, Thomas H.: *Process Innovation: Reengineering Work Through Information Technology*. Harvard Business School Press, 1993

[DEPG+14] Dardick, Glenn S. ; Endicott-Popovsky, Barbara ; Gladyshev, Pavel ; Kemmerich, Thomas ; Rudolph, Carsten: Digital Evidence and Forensic Readiness (Dagstuhl Seminar 14092) / Schloss Dagstuhl. 2014. – Forschungsbericht

[Dew12] Dewald, Andreas: *Formalisierung digitaler Spuren und ihre Einbettung in die Forensische Informatik*, Friedrich-Alexander-Universität Erlangen-Nürnberg, Diss., 2012

[Dew15] Dewald, Andreas: Characteristic Evidence, Counter Evidence and Reconstruction Problems in Forensic Computing. In: *2015 Ninth International Conference on IT Security Incident Management & IT Forensics (IMF)*, 2015, S. 77–82

[DF11] Dewald, Andreas ; Freiling, Felix: *Forensische Informatik*. 1. Books on Demand, 2011

[DF12] Dewald, Andreas ; Freiling, Felix C.: Is Computer Forensics a Forensic Science? In: *Proceedings of Current Issues in IT Security 2012*, 2012

[DF14] Dewald, Andreas ; Freiling, Felix: From Computer Forensics to Forensic Computing: Investigators Investigate, Scientists Associate / Friedrich-Alexander-Universität Erlangen-Nürnberg. 2014 (CS-2014-04). – Forschungsbericht

[Dij75] Dijkstra, Edsger W.: Guarded commands, nondeterminacy and formal derivation of programs. In: *Communications of the ACM* 18 (1975), Nr. 8, S. 453–457

[EAML15] Elyas, Mohamed ; Ahmad, Atif ; Maynard, Sean B. ; Lonie, Andrew: Digital forensic readiness: Expert perspectives on a theoretical framework. In: *Computers & Security* 52 (2015), S. 70–89

[EPFT07] Endicott-Popovsky, Barbara ; Frincke, Deborah A. ; Taylor, Carol A.: A Theoretical Framework for Organizational Network Forensic Readiness. In: *Journal of Computers* 2 (2007), Nr. 3, S. 1–11

[FAS12] Flores, Denys A. ; Angelopoulou, Olga ; Self, Richard J.: Combining Digital Forensic Practices and Database Analysis as an Anti-Money Laundering Strategy for Financial Institutions. In: *Proceedings of the 2012 Third International Conference on Emerging Intelligent Data and Web Technologies (EIDWT)*, 2012, S. 218–224

[FG15] FREILING, Felix ; GRUHN, Michael: What is Essential Data in Digital Forensic Analysis? In: *2015 Ninth International Conference on IT Security Incident Management & IT Forensics (IMF)*, 2015, S. 40–48

[FHPP11] FREILING, Felix C. ; HECKMANN, Dirk ; POLCÁK, Radim ; POSEGGA, Joachim: Forensic Computing (Dagstuhl Seminar 11401) / Schloss Dagstuhl. 2011. – Forschungsbericht

[FI06] FORRESTER, Jock ; IRWIN, Barry: A DIGITAL FORENSIC INVESTIGATIVE MODEL FOR BUSINESS ORGANISATIONS. In: *Proceedings of the ISSA 2006 from Insight to Foresight Conference (ISSA)*, 2006

[Fin16] FINKLE, Jim: *Exclusive: SWIFT warns customers of multiple cyber fraud cases.* http://www.reuters.com/article/us-cyber-banking-swift-exclusive-idUSKCN0XM2DI. Version: 2016, Abruf: 28.04.2016

[FKS+13] FRÜHWIRT, Peter ; KIESEBERG, Peter ; SCHRITTWIESER, Sebastian ; HUBER, Markus ; WEIPPL, Edgar: InnoDB database forensics: Enhanced reconstruction of data manipulation queries from redo logs. In: *Information Security Technical Report* 17 (2013), Nr. 4, S. 227–238

[Flu01] FLUSCHE, Karl J.: Computer Forensic Case Study: Espionage, Part 1 Just Finding the File is Not Enough! In: *Information Systems Security* 10 (2001), Nr. 1

[FQ16] FINKLE, Jim ; QUADIR, Serajul: *Bangladesh Bank hackers compromised SWIFT software, warning issued.* http://www.reuters.com/article/us-usa-nyfed-bangladesh-malware-exclusiv-idUSKCN0XM0DR. Version: 2016, Abruf: 28.04.2016

[FS13] FERSTL, Otto K. ; SINZ, Elmar J.: *Grundlagen der Wirtschaftsinformatik.* 7. Oldenbourg, 2013

[Ges11] GESCHONNECK, Alexander: *Computer-Forensik – Computerstraftaten erkennen, ermitteln, aufklären.* 5. dpunkt.verlag, 2011

[GFWS15] GESCHONNECK, Alexander ; FRITZSCHE, Thomas ; WEIAND, Klara ; SCHEBEN, Marc Oliver: e-Crime: Computerkriminalität in der deutschen Wirtschaft 2015 / KPMG AG. 2015. – Forschungsbericht

[GL07] GROBLER, Cornelia P. ; LOUWRENS, CP: Digital Forensic Readiness as a Component of Information Security Best Practice. In: *New Approaches for Security, Privacy and Trust in Complex Environments.* Springer US, 2007, S. 13–24

[GLv10a] Grobler, Talania ; Louwrens, CP ; von Solms, Sebastiaan H.: A Framework to Guide the Implementation of Proactive Digital Forensics in Organisations. In: *Fifth International Conference on Availability, Reliability and Security (ARES)*, 2010, S. 677–682

[GLv10b] Grobler, Talania ; Louwrens, CP ; von Solms, Sebastiaan H.: A Multi-component View of Digital Forensics. In: *Fifth International Conference on Availability, Reliability and Security (ARES)*, 2010, S. 647–652

[GNY12] Garfinkel, Simson ; Nelson, Alex J. ; Young, Joel: A general strategy for differential forensic analysis. In: *Digital Investigation* 9 (2012), S. 50–59

[GP04] Gladyshev, Pavel ; Patel, Ahmed: Finite state machine approach to digital event reconstruction. In: *Digital Investigation* 1 (2004), Nr. 2, S. 130–149

[Ham15] Hammer, Michael: What is Business Process Management? In: *Handbook on Business Process Management 1.* Springer Berlin Heidelberg, 2015, S. 3–16

[Har15] Harmon, Paul: The Scope and Evolution of Business Process Management. In: *Handbook on Business Process Management 1.* Springer Berlin Heidelberg, 2015

[HC10] Hevner, Alan ; Chatterjee, Samir: Design Science Research in Information Systems. In: *Design Research in Information Systems.* Springer US, 2010, S. 9–22

[HDL13] Härtl, Karolin ; Däs, Miriam ; Lindner, Georg: *Status Quo bei der Integration von digitaler Forensik in dasIT-Sicherheitsmanagement.* 2013

[HH06] Herrmann, Peter ; Herrmann, Gaby: Security requirement analysis of business processes. In: *Electronic Commerce Research* 6 (2006), Nr. 3-4, S. 305–335

[HMN15] Hansen, Hans R. ; Mendling, Jan ; Neumann, Gustaf: *Wirtschaftsinformatik: Grundlagen und Anwendungen.* 11. De Gruyter, 2015

[HMPR04] Hevner, Alan R. ; March, Salvatore T. ; Park, Jinsoo ; Ram, Sudha: Design science in information systems research. In: *MIS Q* 28 (2004), Nr. 1, S. 75–105

[HS15] Heinrich, Bernd ; Schön, Dominik: Automated Planning of Context-aware Process Models. In: *European Conference on Information Systems (ECIS)*, 2015

[HSW04] HAFNER, Martin ; SCHELP, Joachim ; WINTER, Robert: Architekturmanagement als Basis effizienter und effektiver Produktion von IT-Services. In: *HMD - Praxis der Wirtschaftsinformatik* 41 (2004), Nr. 237, S. 54–66

[HT06] HAGGERTY, John ; TAYLOR, Mark: Managing corporate computer forensics. In: *Computer Fraud & Security* 2006 (2006), Nr. 6, S. 14–16

[HW14] HARMON, Paul ; WOLF, Celia: The State of Business Process Management 2014 / Business Process Trends. 2014. – Forschungsbericht

[IR00] INMAN, Keith ; RUDIN, Norah: *Principles and Practice of Criminalistics: The Profession of Forensic Science*. CRC Press, 2000

[IR02] INMAN, Keith ; RUDIN, Norah: The origin of evidence. In: *Forensic Science International* 126 (2002), S. 11–26

[ISO13] *ISO/IEC 27001:2013 Information security management*. 2013

[JLT14] JOHANNSEN, Florian ; LEIST, Susanne ; TAUSCH, Reinhold: Wand and Weber's good decomposition conditions for BPMN. In: *Business Process Management Journal* 20 (2014), Nr. 5, S. 693–729

[KCGD06] KENT, Karen ; CHEVALIER, Suzanne ; GRANCE, Tim ; DANG, Hung: Guide to Integrating Forensic Techniques into Incident Response: NIST SP 800-86 / National Institute of Standards and Technology (NIST). 2006. – Forschungsbericht

[KDF13] KALBER, Sven ; DEWALD, Andreas ; FREILING, Felix C.: Forensic Application-Fingerprinting Based on File System Metadata. In: *Seventh International Conference on IT Security Incident Management and IT Forensics (IMF)*, 2013, S. 98–112

[Ker13] KERRIGAN, Martin: A capability maturity model for digital investigations. In: *Digital Investigation* 10 (2013), Nr. 1, S. 19–33

[Kes12] KESSLER, Gary C.: Advancing the Science of Digital Forensics. In: *Computer* 45 (2012), Nr. 12, S. 25–27

[KLW09] KO, Ryan K. ; LEE, Stephen S. ; WAH LEE, Eng: Business process management (BPM) standards: A survey. In: *Business Process Management Journal* 15 (2009), Nr. 5, S. 744–791

[Koo99] KOOPS, Bert-Jaap: *The crypto controversy: A key conflict in the Information Society*. Kluwer Law International, 1999

[Koo10] KOOPS, Bert-Jaap: Cybercrime Legislation in the Netherlands. In: *Electronic Journal of Comparative Law* 14 (2010), Nr. 3

[Kör95] KÖRMEIER, Klaus: Prozeßorientierte Unternehmensgestaltung. In: *Wirtschaftswissenschaftliches Studium (WiSt)* (1995), Nr. 24, S. 259–261

[Lei10] LEIBOLT, Gregory: The Complex World of Corporate CyberForensics Investigations. In: *CyberForensics*. Humana Press, 2010, S. 7–27

[LL14] LIAO, Yi-Ching ; LANGWEG, Hanno: Cost-benefit analysis of kernel tracing systems for forensic readiness in Communication Systems. In: *Proceedings of the 2nd International Workshop on Security and Forensics in Communication Systems (SFCS)*, 2014, S. 25–36

[LLS06] LAUDON, Kenneth C. ; LAUDON, Jane P. ; SCHODER, Detlef: *Wirtschaftsinformatik: Eine Einführung*. Pearson Studium, 2006

[May02] MAY, Cliff: Computer Forensics – the Morse or Clouseau Approach? In: *Computer Fraud & Security* 2002 (2002), Nr. 11, S. 14–17

[MC13] MOSER, Andreas ; COHEN, Michael I.: Hunting in the enterprise: Forensic triage and incident response. In: *Digital Investigation* 10 (2013), Nr. 2, S. 89–98

[MD10] MANES, Gavin W. ; DOWNING, Elizabeth: What Security Professionals Need to Know About Digital Evidence. In: *Information Security Journal: A Global Perspective* 19 (2010), Nr. 3, S. 124–131

[MGL11] MOUHTAROPOULOS, Antonis ; GROBLER, Marthie ; LI, Chang-Tsun: Digital Forensic Readiness: An Insight into Governmental and Academic Initiatives. In: *Proceedings of the 2011 European Intelligence and Security Informatics Conference (EISIC)*, 2011, S. 191–196

[MP14] MEIER, Stefan ; PERNUL, Günther: Einsatz von digitaler Forensik in Unternehmen und Organisationen. In: *Sicherheit 2014: Sicherheit, Schutz und Zuverlässigkeit, Beiträge der 7. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI)*, 2014, S. 103–114

[MS12] MAZURCZYK, Wojciech ; SZCZYPIORSKI, Krzysztof: Toward Effective and Reliable Digital Forensics. In: *The Computer Journal* 55 (2012), Nr. 6, S. 651–652

[MSRRM15] MORENO-MONTES DE OCA, Isel ; SNOECK, Monique ; REIJERS, Hajo A. ; RODRÍGUEZ-MORFFI, Abel: A systematic literature review of studies on business process modeling quality. In: *Information and Software Technology* 58 (2015), S. 187–205

[MW03] MCCOMBIE, Steve ; WARREN, Matt: Computer Forensics: An Issue of Definitions. In: *1st Australian Computer, Network & Information Forensics Conference*, 2003

[MZ11] MEYER, Jörg ; ZIRCH, Stephan: Forensische Datenanalyse. In: *Tax Fraud & Forensic Accounting*. Gabler Verlag / Springer Fachmedien Wiesbaden GmbH, 2011

[NDP10] NAQVI, Syed ; DALLONS, Gautier ; PONSARD, Christophe: Applying Digital Forensics in the Future Internet Enterprise Systems – European SME's Perspective. In: *Proceedings of the 2010 Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE)*, 2010, S. 89–93

[Nel06] NELSON, Anthony: ISO 27001 as a Support to Digital Forensics. In: *Journal of Digital Forensic Practice* 1 (2006), Nr. 1, S. 43–46

[NLZ+12] NNOLI, Henry ; LINDSKOG, Dale ; ZAVARSKY, Pavol ; AGHILI, Shaun ; RUHL, Ron: The Governance of Corporate Forensics Using COBIT, NIST and Increased Automated Forensic Approaches. In: *Proceedings of the 2012 ASE/IEEE International Conference on Social Computing and 2012 ASE/IEEE International Conference on Privacy, Security, Risk and Trust (SOCIALCOM-PASSAT)*, 2012, S. 734–741

[NV09] NGOBENI, Sipho J. ; VENTER, Hein S.: The Design of a Wireless Forensic Readiness Model (WFRM). In: *Information Security South Africa Conference (ISSA)*, 2009, S. 35–52

[ÖBF+10] ÖSTERLE, Hubert ; BECKER, Jörg ; FRANK, Ulrich ; HESS, Thomas ; KARAGIANNIS, Dimitris ; KRCMAR, Helmut ; LOOS, Peter ; MERTENS, Peter ; OBERWEIS, Andreas ; SINZ, Elmar J.: Memorandum zur gestaltungsorientierten Wirtschaftsinformatik. In: *Schmalenbachs Zeitschrift für betriebswirtschaftliche Forschung* 62 (2010), Nr. 6, S. 664–672

[Obj11] OBJECT MANAGEMENT GROUP: *Business Process Model and Notation (BPMN)*. 2.0. 2011

[OBS12] OVERHAGE, Sven ; BIRKMEIER, Dominik Q. ; SCHLAUDERER, Sebastian: Quality Marks, Metrics, and Measurement Procedures for Business Process Models. In: *Business & Information Systems Engineering* 4 (2012), Nr. 5, S. 229–246

[OG13] OLIVIER, Martin ; GRUNER, Stefan: On the Scientific Maturity of Digital Forensics Research. In: *Advances in Digital Forensics IX*, Springer Berlin Heidelberg, 2013, S. 33–49

[Ost16] OSTERMEIER, Wolfgang: *Enterprise Forensics – An Overview*. 2016

[Pal01] PALMER, Gary: *A Road Map for Digital Forensic Research: Report From the First Digital Forensic Research Workshop (DFRWS)*. 2001

[PIP10] PANGALOS, George ; ILIOUDIS, Christos ; PAGKALOS, Ioannis: The Importance of Corporate Forensic Readiness in the Information Security Framework. In: *Proceedings of the 2010 19th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE)*, 2010, S. 12–16

[PK10] PANGALOS, Georgios ; KATOS, Vasilios: Information Assurance and Forensic Readiness. In: *Next Generation Society. Technological and Legal Issues*. Springer Berlin Heidelberg, 2010, S. 181–188

[Pol08] POLLITT, Mark: Applying Traditional Forensic Taxonomy to Digital Forensics. In: *Advances in Digital Forensics IV*. Springer US, 2008, S. 17–26

[Qui05] QUINN, Spike: Examining the state of preparedness of Information Technology management in New Zealand for events that may require forensic analysis. In: *Digital Investigation* 2 (2005), Nr. 4, S. 276–280

[Ras04] RASCH, Mark: *The Giant Wooden Horse Did It!* http://www.securityfocus.com/columnists/208. Version: 2004, Abruf: 29.06.2015

[RB10] REKHIS, Slim ; BOUDRIGA, Noureddine: Formal Digital Investigation of Anti-forensic Attacks. In: *Proceedings of the 2010 Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE)*, 2010, S. 33–44

[Rec10] RECKER, Jan: Opportunities and constraints: The current struggle with BPMN. In: *Business Process Management Journal* 16 (2010), Nr. 1, S. 181–201

[RMR15] REIJERS, Hajo A. ; MENDLING, Jan ; RECKER, Jan: Business Process Quality Management. In: *Handbook on Business Process Management 1*. Springer Berlin Heidelberg, 2015

[Row04] ROWLINGSON, Robert: A Ten Step Process for Forensic Readiness. In: *International Journal of Digital Evidence (IJDE)* 2 (2004), Nr. 3

[RR15] RUMMLER, Geary A. ; RAMIAS, Alan J.: A Framework for Defining and Designing the Structure of Work. In: *Handbook on Business Process Management 1*. Springer Berlin Heidelberg, 2015

[RSD12] ROSEMANN, Michael ; SCHWEGMANN, Ansgar ; DELFMANN, Patrick: Vorbereitung der Prozessmodellierung. In: *Prozessmanagement*. Springer Berlin Heidelberg, 2012

[RV09] REDDY, Kamil ; VENTER, Hein: A Forensic Framework for Handling Information Privacy Incidents. In: *Advances in Digital Forensics V*, Springer Berlin Heidelberg, 2009, S. 143–155

[RV13] REDDY, Kamil ; VENTER, Hein S.: The architecture of a digital forensic readiness management system. In: *Computers & Security* 32 (2013), Nr. 0, S. 73–89

[RWR06] ROSS, Jeanne W. ; WEILL, Peter ; ROBERTSON, David: *Enterprise architecture as strategy: Creating a foundation for business execution*. Harvard Business School Press, 2006

[SDMW10] SMIRNOV, Sergey ; DIJKMAN, Remco ; MENDLING, Jan ; WESKE, Mathias: Meronymy-Based Aggregation of Activities in Business Process Models. In: *Conceptual Modeling – ER 2010*, Springer Berlin Heidelberg, 2010, S. 1–14

[SFH+15] SOHL, Eli ; FIELDING, Curtis ; HANLON, Tyler ; RRUSHI, Julian ; FARHANGI, Hassan ; HOWEY, Clay ; CARMICHAEL, Kelly ; DABELL, Joey: A Field Study of Digital Forensics of Intrusions in the Electrical Power Grid. In: *The First ACM Workshop*, 2015, S. 113–122

[Sim10] SIMS, Shane: Insider Threat Investigations. In: *CyberForensics*. Humana Press, 2010, S. 45–51

[SKW12] SCHRITTWIESER, Sebastian ; KIESEBERG, Peter ; WEIPPL, Edgar: Digital forensics for enterprise rights management systems. In: *The 14th International Conference on Information Integration and Web-based Applications & Services (IIWAS)*, 2012, S. 111–120

[SLJ+11] SON, Namheun ; LEE, Keun-gi ; JEON, SangJun ; CHUNG, Hyunji ; LEE, Sangjin ; LEE, Changhoon: The Method of Database Server Detection and Investigation in the Enterprise Environment. In: *Secure and Trust Computing, Data Management and Applications*. Springer Berlin Heidelberg, 2011, S. 164–171

[SLRG06] SOLMS, Sebastiaan ; LOUWRENS, Cecil ; REEKIE, Colette ; GROBLER, Talania: A Control Framework for Digital Forensics. In: *Advances in Digital Forensics II*, Springer New York, 2006, S. 343–355

[SLT+09] SLAY, Jill ; LIN, Yi-Chi ; TURNBULL, Benjamin ; BECKETT, Jason ; LIN, Paul: Towards a Formalization of Digital Forensics. In: *Advances in Digital Forensics V*, Springer Berlin Heidelberg, 2009, S. 37–47

[SOSF04] SADIQ, Shazia ; ORLOWSKA, Maria ; SADIQ, Wasim ; FOULGER, Cameron: Data Flow and Validation in Workflow Modelling. In: *Proceedings of the 15th Australasian Database Conference (ADC)*, 2004, S. 207–214

[SPO11] SHANMUGAM, Karthikeyan ; POWELL, Roger ; OWENS, Tom: An Approach for Validation of Digital Anti-Forensic Evidence. In: *Information Security Journal: A Global Perspective* 20 (2011), Nr. 4-5, S. 219–230

[SRWN12] SMIRNOV, Sergey ; REIJERS, Hajo A. ; WESKE, Mathias ; NUGTEREN, Thijs: Business process model abstraction: A definition, catalog, and survey. In: *Distributed and Parallel Databases* 30 (2012), Nr. 1, S. 63–99

[STA15] SIDOROVA, Anna ; TORRES, Russell ; AI BEAYEYZ, Alaa: The Role of Information Technology in Business Process Management. In: *Handbook on Business Process Management 1*. Springer Berlin Heidelberg, 2015

[SWM10] SMIRNOV, Sergey ; WEIDLICH, Matthias ; MENDLING, Jan: Business Process Model Abstraction Based on Behavioral Profiles. In: *Service-Oriented Computing*. Springer Berlin Heidelberg, 2010, S. 1–16

[SZS04] SUN, Sherry ; ZHAO, Leon ; SHENG, Olivia: Data Flow Modeling and Verification in Business Process Management. In: *Americas Conference on Information Systems (AMCIS)*. 2004

[Tan01] TAN, John: *Forensic Readiness*. 2001

[TEPF07] TAYLOR, Carol ; ENDICOTT-POPOVSKY, Barbara ; FRINCKE, Deborah A.: Specifying digital forensics: A forensics policy approach. In: *Digital Investigation* 4 (2007), Nr. 0, S. 101–104

[THG07] TAYLOR, Mark ; HAGGERTY, John ; GRESTY, David: The legal aspects of corporate computer forensic investigations. In: *Computer Law & Security Review* 23 (2007), Nr. 6, S. 562–566

[THG09] TAYLOR, Mark ; HAGGERTY, John ; GRESTY, David: The legal aspects of corporate e-mail investigations. In: *Computer Law & Security Review* 25 (2009), Nr. 4, S. 372–376

[Tip93] TIPTON, Hal: Investigating inside the corporation. In: *Computer Fraud & Security Bulletin* (1993), Nr. 2, S. 4–10

[TVTY90] TAKEDA, Hideaki ; VEERKAMP, Paul ; TOMIYAMA, Tetsuo ; YOSHIKAWA, Hiroyuki: Modeling Design Processes. In: *AI Magazine* 11 (1990), Nr. 4, S. 37–48

[Val10] VALENTINE, J. A.: Investigating Large-Scale Data Breach Cases. In: *CyberForensics*. Humana Press, 2010

[VK07] VAISHNAVI, Vijay K. ; KUECHLER, William J.: *Design Science Research Methods and Patterns: Innovating Information and Communication Technology*. 1. Auerbach Publications, 2007

[vSR+14] VOM BROCKE, Jan ; SCHMIEDEL, Theresa ; RECKER, Jan ; TRKMAN, Peter ; MERTENS, Willem ; VIAENE, Stijn: Ten principles of good business process management. In: *Business Process Management Journal* 20 (2014), Nr. 4, S. 530–548

[vtW03] VAN DER AALST, Wil M. P. ; TER HOFSTEDE, Arthur H. M. ; WESKE, Mathias: Business Process Management: A Survey. In: *Business Process Management*. Springer Berlin Heidelberg, 2003, S. 1–12

[VV13] VALJAREVIC, Aleksandar ; VENTER, Hein: A Harmonized Process Model for Digital Forensic Investigation Readiness. In: *Advances in Digital Forensics IX*, Springer Berlin Heidelberg, 2013, S. 67–82

[Wes12] WESKE, Mathias: *Business process management: Concepts, languages, architectures*. 2. Springer Berlin New York, 2012

[WH07] WILDE, Thomas ; HESS, Thomas: Forschungsmethoden der Wirtschaftsinformatik. In: *WIRTSCHAFTSINFORMATIK* 49 (2007), Nr. 4, S. 280–287

[Wil12] WILLIAMS, Janet: ACPO Good Practice Guide for Digital Evidence / Association of Chief Police Officers. 2012. – Forschungsbericht

[Wol04] WOLFE, Henry B.: The question of organizational forensic policy. In: *Computer Fraud & Security* (2004), Nr. 6, S. 13–14

[WWW03] WOLFE-WILSON, Jeni ; WOLFE, Henry B.: Management strategies for implementing forensic security measures. In: *Information Security Technical Report* 8 (2003), Nr. 2, S. 55–64

[WY05] WANG, Shiuh-Jeng ; YANG, Cheng-Hsing: Gathering Digital Evidence in Response to Information Security Incidents. In: *Intelligence and Security Informatics*. Springer Berlin Heidelberg, 2005, S. 644–645

[YM01] YASINSAC, Alec ; MANZANO, Yanet: Policies to Enhance Computer and Network Forensics. In: *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*, 2001

[YV14] YAMASATHIEN, Saran ; VATANAWOOD, Wiwat: An approach to construct formal model of business process model from BPMN workflow patterns. In: *2014 Fourth International Conference on Digital Information and Communication Technology and its Applications (DICTAP)*, 2014, S. 211–215