



universität
wien

MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

Die Rolle der forensischen Rechnungsprüfung bei der
Entdeckung von Finanzbetrug und
Wirtschaftskriminalität

verfasst von / submitted by

Aleksandra Pavlovic, BSc

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of
Master of Science (MSc)

Wien, 2018 / Vienna, 2018

Studienkennzahl lt. Studienblatt /
degree programme code as it appears on
the student record sheet:

A 066 915

Studienrichtung lt. Studienblatt /
degree programme as it appears on
the student record sheet:

Masterstudium Betriebswirtschaft UG2002

Betreut von / Supervisor:

ao. Univ.-Prof. Dr. Michaela-Maria Schaffhauser-Linzatti

In Zeiten von Globalisierung und globaler Vernetzung nimmt das Thema der forensischen Rechnungsprüfung stark an Bedeutung zu und spielt in der Bekämpfung von Korruption und Betrugsfällen in Großunternehmen eine unerlässliche Rolle. Um diese Aussage wissenschaftlich bestätigen zu können, hat es sich diese Arbeit zum Ziel gesetzt, anhand einer Literaturanalyse ein Verständnis für den Prüfungsablauf im Fall eines Finanzskandals zu ermöglichen sowie passende Präventionsmaßnahmen vorzuschlagen, um letztendlich ein Vertrauen in das Wirtschaftssystem wiederherzustellen. Die Hauptfragestellung dieser Arbeit: „Welche Rolle spielt die forensische Rechnungsprüfung bei der Untersuchung eines Finanzbetrugs in Großunternehmen?“ kann wie folgt beantwortet werden: Die Rolle, die bei der Aufdeckung und Untersuchung von Finanzbetrug in Unternehmen, von der forensischen Rechnungsprüfung eingenommen wird, ist äußerst wichtig: Forensische Rechnungsprüfer decken auf, analysieren und bekämpfen die Schwachpunkte im Unternehmen.

Inhaltsverzeichnis

ABKÜRZUNGSVERZEICHNIS.....	IV
ABBILDUNGSVERZEICHNIS	VI
1. EINFÜHRUNG	1
1.1. EINLEITUNG	1
1.2. FORSCHUNGSSTAND	3
1.3. AUFBAU DER ARBEIT.....	5
2. AUSPRÄGUNGEN VON BETRUG.....	6
2.1. BEGRIFFE UND ARTEN KRIMINELLER TÄTIGKEITEN.....	6
2.1.1. BESTIMMUNG DES BEGRIFFS „BETRUG“	10
2.1.2. BETRUGSARTEN	11
2.1.3. CYBERKRIMINALITÄT	14
2.1.4. MOTIVATIONSFAKTOREN, DIE ZUM BETRUG FÜHREN.....	19
2.1.5. FAKTOREN UND INDIKATOREN DES BETRUGSRISIKOS	20
2.2. INTERNATIONALE PRÜFUNGSSTANDARDS	22
2.3. AUSGEWÄHLTE EU-STATISTIK	27
3. KAMPF GEGEN BETRUG	31
3.1. ENRON-SKANDAL.....	31
3.1.1. UNTERNEHMENSGESCHICHTE	32
3.1.2. BETRÜGERISCHES GESCHÄFTSMODELL	33
3.1.3. GESETZGEBUNG	38
3.2. KAMPF GEGEN BETRUG	39
3.2.1. INTERNE PRÜFUNG.....	41
3.2.1.1. Interne Revision.....	42
3.2.1.2. Risikomanagement.....	46
3.2.1.3. Compliance	46
3.2.1.4. Bewertung des Betrugsrisikos	47
3.2.1.5. Beurteilung der Umsetzung interner Kontrollen	48
3.2.1.6. Betrugsuntersuchungen	50
3.2.2. EXTERNE PRÜFUNG: WIRTSCHAFTSPRÜFUNG.....	52
4. FORENSISCHE RECHNUNGSPRÜFUNG	54
4.1. KLASSISCHE FORENSISCHE RECHNUNGSPRÜFUNG	54
4.1.1. UMFANG UND ARTEN FORENSISCHER RECHNUNGSPRÜFUNG	56
4.1.2. FORENSISCHE RECHNUNGSPRÜFUNG- BERUFLICHE TÄTIGKEIT	57
4.1.3. EIGENSCHAFTEN UND VERFAHREN DER FORENSIK	58
4.1.3.1. Persönlicher Kontakt besser als Lügendetektor.....	61
4.1.3.2. Mittel zur Untersuchung der Handlung	62
4.1.3.3. Nachweisarten.....	63
4.2. DIGITALE FORENSISCHE RECHNUNGSPRÜFUNG.....	64
4.2.1. PRÜFUNGSABLAUF	66
4.2.2. DATENINTEGRITÄT.....	68
4.2.3. AUSGEWÄHLTE TECHNISCHE BERICHTE IN DIGITALER FORENSIK.....	69

4.2.3.1. Gefahr durch VPN-Clients.....	70
4.2.3.2. SSD-Technologie und Digitale Forensik.....	72
4.2.3.3. Digitale Analyse von Smartphones.....	72
4.2.4. QUALITÄTSFAKTOREN DER FORENSIK	74
4.2.5. MATHEMATISCHE STUDIE ZUR FORENSIK.....	75
4.2.6. ZUKUNFT DIGITALER FORENSIK	78
5. CONCLUSIO	80
5.1. DISKUSSION UND SCHLUSSFOLGERUNGEN	80
5.2. AUSBLICK.....	83
5.3. LIMITATIONEN DER ARBEIT	84
LITERATURVERZEICHNIS	85

Abkürzungsverzeichnis

ACFE	Association of Certified Fraud Examiners
AICPA	American Institute of Certified Public Accountants
AktG	Aktiengesetz
BKA	Bundeskriminalamt (Deutschland)
BMI	Bundesministerium für Inneres
CIA	Central Intelligence Agency
COSO	Committee of Sponsoring Organizations of the Treadway Commission
EOL	Enron Online
EY	Ernst & Young
FASB	Financial Accounting Standards Board
FBI	Federal Bureau of Investigation
FinStrG	Finanzstrafgesetz
FTC	Federal Trade Commission
GmbHG	GmbH Gesetz
HDD	Hard Disk Drive
HGB	Handelsgesetzbuch
HMAC	Hashbasierte Message Authentication Codes
IAASB	International Auditing and Assurance Standards Board
IAPC	Auditing Practices Committee
IFA	Institute of Forensic Auditors
IFAC	International Federation of Accountants
IFRS	International Financial Reporting Standards
IKS	Internes Kontrollsystem
IO/InsO	Insolvenzordnung
IoT	Internet of Things
IRR	Deutsches Institut für Interne Revision e.V.
IRS	Internes Revisionsystem
ISA	International Standard on Auditing
KonTraG	Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich

OECD	Organisation for Economic Co-operation and Development
PWC	PricewaterhouseCoopers
RAG	Revisionsaufsichtsgesetz
RMS	Risikomanagementsystem
RPA	Robotic process automation
SAS 99	Statement of Auditing Standards No.99
SEC	United States Securities and Exchange Commission
SOX	Sarbanes-Oxley Act
SPE	Special Purpose Entity
SSD	Solid State Disk
StGB	Strafgesetzbuch
URÄG 2008	Unternehmensrechts- Änderungsgesetz 2008
UrhG	Urheberrechtsgesetz
US GAAP	United States Generally Accepted Accounting Principles
UWG	Bundesgesetz gegen den unlauteren Wettbewerb
VPN	Virtual Private Network
WAG	Wertpapieraufsichtsgesetz

Abbildungsverzeichnis

ABBILDUNG 1: SAR, STR, UTR	28
ABBILDUNG 2: EU BERICHTS ÜBER VERDÄCHTIGE AKTIVITÄTEN	29
ABBILDUNG 3: AUFDECKUNGSURSACHEN	31
ABBILDUNG 4: ENRON SPE	35
ABBILDUNG 5: ENRON SPE.2	36
ABBILDUNG 6: HASHSYSTEM	69
ABBILDUNG 7: VPN	71
ABBILDUNG 8: FORENSIKMAßNAHMEN IMPLEMENTIERUNG	76
ABBILDUNG 9: INTERESSE AN FORENSIK	77

1. Einführung

1.1. Einleitung

Die Wirtschaftsprüfungsgesellschaft PricewaterhouseCoopers (PWC) veröffentlichte im Jahr 2018 eine globale Studie „Pulling fraud out of shadows. The biggest competitor you didn't know you had“, die ihren Fokus auf Betrugsfälle in Großunternehmen legt. Dabei wurden 7200 Teilnehmer aus mehr als 100 Ländern befragt. Ziel dieser Studie war es ein größeres Bewusstsein für die steigende Bedrohung von Wirtschaftsbetrug in Unternehmen aus der ganzen Welt zu schaffen. Die Studie zeigt, dass zwar bei knapp der Hälfte der befragten Unternehmen ein Betrugsfall festgestellt wurde und somit Vorkehrmaßnahmen für solche Gefahren in Betracht gezogen wurden oder bereits implementiert wurden, aber auch, dass bei mehr als 50% der Unternehmen dieses Risikobewusstsein durchaus noch Entwicklungsbedarf aufzeigt. Ergebnisse dieser weltweiten PWC Studie zeigen, dass jedes Unternehmen von Betrug betroffen sein kann auch wenn viele sich dessen nicht bewusst sind oder trotz der steigenden Wahrnehmung der globalen Wirtschaftskriminalität nicht bewusst sein wollen. Deshalb ist eine detaillierte Rechnungsprüfung umso relevanter, da ein Vorbeugen und Bekämpfen von Betrugsfällen Ziel eines jeden erfolgreichen Unternehmens sein müsste (Lavion, 2018).

Trotz aller Bemühungen der nationalen Regulierungsbehörden, ein verlässliches globales Finanzberichterstattungssystem aufzubauen, wurde die Welt von zahlreichen finanziellen Skandalen getroffen. Die Häufigkeit dieser Betrugsfälle und der dabei entstehende finanzielle Schaden, der vor allem durch die Managementebene (engl. „white collar“ oder deutsch „Weiße-Kragen“) verursacht wird, ist alarmierend hoch. Die Investoren und Gläubiger weltweit sind diejenigen die dabei die größten Schäden zu tragen haben, die durch verfälschte Finanzberichte verursacht worden sind. Dadurch wird die Zuverlässigkeit der Jahresabschlüsse ernsthaft in Zweifel gezogen. Zusätzlich zu diesen direkten Verlusten, führen finanzielle Betrügereien unter den Firmenkunden, Investoren und Gläubigern zu einem generellen Vertrauensverlust in das gesamte Berichtswesen (Hlavica et al. 2011, S. 53-57; Suput, 2009, S. 169-170; Albrecht et al. 2009, S. 358).

Verschiedene Betrugsformen in der Finanzwelt erregen die Aufmerksamkeit der Fachleute und der Öffentlichkeit. Es ist daher nicht verwunderlich, dass die Öffentlichkeit heute zunehmend auf Betrugereien im Bereich Finanzen und Wirtschaft fokussiert ist. Die größten Probleme umfassen Geldwäsche, organisierten Betrug, Verfälschung von Geld und Cyberkriminalität (Goebel, 2016). Die Untersuchung von Finanzbetrug ist eine mühsame und komplexe Aufgabe, da es sich um eine Analyse der wirtschaftlichen, rechtlichen, kriminologischen, psychologischen und soziologischen Aspekte und Beziehungen handelt (Hlavica et al. 2011, S. 53-57).

Die Konsequenzen, die durch große Wirtschaftsskandale verursacht wurden, haben die Regierungen und Wirtschaftsprüfer weltweit gezwungen, sich aktiv mit Wirtschaftsbetrug auseinander zu setzen und die neuen drohenden Gefahren zu verhindern. Die Wirtschaftskrisen haben dabei nicht zu positiven Veränderungen in der Wirtschaftswelt beigetragen, sondern ganz im Gegenteil: In den Jahren nach der Krise wurden nur noch überall Instabilität und Betrug wahrgenommen. Die Managementebenen in großen Banken und Unternehmen sind ständig unter Druck: Sie müssen die Performance des eigenen Unternehmens steigern und gleichzeitig kostensenkend arbeiten. Dieses Ziel ist am einfachsten durch Betrug zu realisieren. Gleichzeitig versuchen die oberen Unternehmensebenen ihre eigenen Interessen zu bewahren und müssen folglich oft gesetzeswidrig arbeiten (Mekic et al. S. 2-3; Hlavica et al. S. 53-57).

Heutzutage haben, neben den traditionellen Wirtschaftsprüfern, auch besonders ausgebildete Experten bei der Betrugsanalyse eine wichtige Rolle: Diese sind auf die Entdeckung des Wirtschaftsbetrugs spezialisiert (Belak & Vudric, Osnove suvremenog racunovodstva, 2012, S. 1). Die forensischen Rechnungsprüfer werden als „eine Mischung aus Wirtschaftsprüfer und Privatdetektiv angesehen (Gray, 2008, S. 115).“ Belak definiert die forensische Rechnungsprüfung als eine praktische Anwendung der Forschung und der analytischen Methoden mit dem Ziel, sowohl die Manipulationen in Finanzberichten zu entdecken als auch potentielle Steuermanipulationen und Missachtungen von Gesetzen zu finden (Belak, Poslovna forenzika i forenzicko racunovodjstvo- Borba protiv prijave, 2012, S. 2).

Die forensische Rechnungsprüfung ist auf die Entdeckung krimineller Tätigkeiten und Betrugs ausgerichtet, sowie auf die Beweisaufnahme und Sanktionierung der Täter vor

Gericht. Mile Stanisić legt dabei besonderen Wert auf die zweite Tätigkeit der Rechnungsprüfung, die Beweisaufnahme: „Der Großteil der Prüfungsarbeiten, die sich auf die Erstellung eines Prüfungsurteils konzentrieren, besteht aus der Erhebung von Nachweisen (Stanisić, Interna kontrola i revizija, 2014, S. 170).“ Gray definiert die forensischen Rechnungsprüfer als „Menschen, die ihre Leistungen für Gerichtsprozesse anbieten, u.a. Geschäftseinkäufe, Vermögenswertabschätzung bei der Scheidung, Entschädigungsanfragen, Steuervermeidung und Geldwäsche (Gray, 2008, S. 116).“

1.2. Forschungsstand

Das Thema der forensischen Rechnungsprüfung nimmt in Zeiten von Globalisierung und Vernetzung (Faigle, 2016) zunehmend an Bedeutung zu und ist in der Bekämpfung von Korruption und Betrugsfällen in Großunternehmen unerlässlich (BDI & KPMG, 2009, S. 1). Die Fachliteratur, wie unter anderem „Wirtschaftskriminalität und Prävention: Wie Führungskräfte Täterwissen einsetzen können“ aus dem Jahr 2017 von Alexander Schuchter, zeigt zu diesem Thema jedoch auf, dass Studien und wissenschaftliche Forschung immer noch große Lücken zu füllen haben. Kein Literaturwerk weist eine vollständige wissenschaftliche Problemanalyse zu diesem Thema auf und es sind somit weitere Forschungen zur Problemlösung nötig. Diese Arbeit hat es sich zum Ziel gesetzt den Wissensstand zu diesem Thema zu erweitern und dabei zu helfen besagte Lücken zu verkleinern. Weiterfolgend finden sich Studien, die einen Teil der aktuellen Wissensstände wiedergeben:

Vor allem die großen Wirtschaftsprüfungsgesellschaften und die Organisationen zur Bekämpfung der Wirtschaftskriminalität haben sich in den letzten Monaten stark mit dem Thema der Betrugsbekämpfung auseinandergesetzt. Die Wirtschaftsprüfungshäuser bieten neben der klassischen Wirtschaftsprüfung, auch eine tiefgreifende Analyse von Schwachstellen eines Unternehmens und dessen potentiellen Angriffsmöglichkeiten an. Diese Unternehmen versuchen sowohl bei eigenen Geschäftspartnern und Kunden, als auch in der Öffentlichkeit, ein Bewusstsein dafür zu schaffen, welche Gefahren die Wirtschaftskriminalität darstellt, insbesondere mit Hilfe der Entwicklung neuer Technologien, der Internetkommunikation und einer weltübergreifenden Vernetzung unterschiedlicher Unternehmen. Im Zuge dessen wurden viele Studien publiziert, die sich mit diesem Thema wissenschaftlich auseinander setzen:

EY hat eine länderübergreifende Befragung mit dem Thema „EY Fraud Survey – Ergebnisse für Österreich“ im Jahr 2017 durchgeführt, in der 4100 Unternehmen aus 41 Ländern Europas, dem Mittleren Osten, Afrikas und Indiens in Betracht gezogen wurden. In Österreich wurden 100 Befragungen durchgeführt. Die Studie hat die Erkenntnis gebracht, dass rein in Österreich mehr als ein Drittel der Manager das Benehmen eigener Mitarbeiter als unethisch empfinden. In den anderen befragten Ländern sind die Manager noch öfter mit Unethik konfrontiert worden. Eine Hälfte der Befragten ist der Meinung, dass die Unternehmen ihre Finanzergebnisse verfälschen und verschönern (Ernst & Young Österreich, 2017). Die vorgestellte EY Studie ist insoweit für die durchgeführte Masterarbeit relevant, da sie verdeutlicht, wie die allgemeine Meinung zum Thema „Betrug“ aussieht, und bestätigt die Vermutung, dass das Vertrauen in unternehmerische und wirtschaftliche Prozesse zum Teil verloren gegangen ist.

Die Recherche des American Institute of Certified Public Accountants (AICPA) hat einen Anstieg der Nachfrage nach forensischen Dienstleistungen nachgewiesen, in dem eine zunehmende Anzahl an Stellenangeboten für die forensischen Rechnungsprüfer entdeckt wurde. Es wurde gezeigt, dass immer mehr Menschen für diese Tätigkeiten benötigt werden, was darauf hinweist, dass die Wichtigkeit der forensischen Disziplin an Bedeutung gewinnt (AICPA, 2011). Diese Masterarbeit betont auch, dass eine starke Entwicklung dieser Tätigkeit zu erwarten ist.

Zudem wurde von den Association of Certified Fraud Examiners (ACFE) zum ersten Mal seit 2006 eine weitgreifende Studie verfasst. Ziel dieser Studie war es, die Meinungen der Experten zum Thema „Verlust wegen Betrugs“ zusammenzufassen, die Arten und Vorgehensweisen bei Wirtschaftsbetrug zu definieren, die Täter des Wirtschaftsbetrugs zu identifizieren, und folglich, die Muster zu erkennen, wie bestimmte Unternehmen leicht und oft zu Opfern der Wirtschaftskriminalität werden. Die Ergebnisse aus der Untersuchung von 2410 Betrugsfällen haben gezeigt, dass der Mittelwert der Verluste pro Fall bei USD 150 Tsd. liegt, wobei 23% aller Verluste Schäden in Höhe von über einer Million USD verursacht haben. Die Ergebnisse haben bestätigt, wie wichtig es ist, Kenntnisse im Bereich der Wirtschaftskriminalität aufzubauen und rechtzeitig Präventionsmaßnahmen zu implementieren (ACFE (Report to the nations), 2016). Die ACFE Studie ist für diese Masterarbeit deshalb von hoher Bedeutung und Relevanz, weil sie sich genau mit dieser Thematik beschäftigt, und analysiert welche Anreize im Fall eines Wirtschaftsbetrugs gegeben

sind, wie die Täter rechtzeitig erkannt werden können und welche Möglichkeiten die Unternehmen haben, sich vor Betrug zu schützen.

1.3. Aufbau der Arbeit

Die vorliegende Arbeit befasst sich thematisch mit der Rolle der forensischen Rechnungsprüfung bei der Entdeckung von Finanzbetrug und Wirtschaftskriminalität.

Die forschungsleitende Fragestellung ist hierbei: *„Welche Rolle spielt die forensische Rechnungsprüfung bei der Untersuchung eines Finanzbetrugs in Großunternehmen?“*

Um diese Frage wissenschaftlich untersuchen und beantworten zu können, hat es sich diese Arbeit zum Ziel gesetzt, anhand einer ausführlichen Literaturanalyse ein Verständnis für den Prüfungsablauf im Fall eines potenziellen Finanzskandals zu ermöglichen sowie passende Präventionsmaßnahmen vorzuschlagen, um letztendlich ein Vertrauen in das Wirtschaftssystem wieder herzustellen, indem relevante Informationen und eine größtmögliche Transparenz für die Öffentlichkeit zur Verfügung gestellt werden. Dabei erfolgt der Aufbau der Arbeit folgendermaßen: Zuerst werden Definitionen der verwendeten Begriffe, wie etwa Betrug oder Cyberkriminalität und eine theoretische Erklärung der vorgestellten Maßnahmen wie unter anderem interne Kontrollsysteme, Risikomanagement, etc. geliefert, um anschließend Unterscheidungsmerkmale der klassischen forensischen und der digitalen forensischen Rechnungsprüfung vorzustellen. Anhand von Beispielen und Statistiken, sowie durch die Analyse der aktuellen Gesetzeslage, sollen diese theoretischen Ausführungen durch Beispiele aus der Praxis verdeutlicht werden. Der Enron-Skandal dient hierbei als primäres Beispiel dieser Masterarbeit, um darzustellen welche Arten des Rechnungslegungsbetrugs sich am häufigsten in der Unternehmenswelt finden lassen. Abschließend befasst sich die Conclusio mit der Beantwortung der eingangs gestellten forschungsleitenden Fragestellung und der Interpretation der diskutierten Ergebnisse. Hierbei wird nicht nur zur Zukunft der digitalen forensischen Rechnungsprüfung Stellung bezogen, die sich vor allem mit dem Thema Robotics und Blockchain auseinander setzt, sondern es wird auch auf die Limitationen der durchgeführten Arbeit eingegangen und es werden Impulse für weitere Forschungen zu diesem Thema geliefert.

2. Ausprägungen von Betrug

2.1. Begriffe und Arten krimineller Tätigkeiten

Der Begriff Kriminalität ist durch seine Universalität gekennzeichnet. Das heißt Kriminalität herrscht im großen oder kleinen Umfang in allen Sphären des Lebens und in allen Ländern weltweit. Unterschiedlichsten Faktoren begünstigen eine Entwicklung von Kriminalität: offene Grenzen, starke wirtschaftliche Entwicklung, Urbanisierung, Globalisierung, Veränderungen im Lebensstil der Menschen, die neuen menschlichen Werte, usw. (Hlavica et al. 2011, S. 53-57).

Nach Angaben des „Verbunds der Rechnungsleger und des Wirtschaftsprüfers Serbiens“ ist eine kriminelle Aktivität in der Abschlussprüfung „eine vorsätzliche Handlung, die eine oder mehrere Personen, die für das Management, die Mitarbeiter oder für Dritte, verantwortlich sind, tätigen um die ungerechten oder die illegalen Vorteile zu erhalten (Savez racunovodja i revizora Srbije, 2005, S. 276).“

Kriminelle Tätigkeiten im breiteren Sinne implizieren den Ungehorsam in Form des Betruges oder der absichtlichen unwahren Darstellung materieller Tatsachen. Es gibt keine einheitliche Definition der Wirtschaftskriminalität, weil die „Wirtschaftskriminalität nicht nur eine rechtliche Kategorie ist, sondern in erster Linie ein soziales Phänomen, das viele Merkmale aufweist, die je nach sozioökonomischen und politischen Umständen von einer Gemeinschaftsgesellschaft zur anderen unterschiedlich sind (Nicevic & Ivanovic, 2012, S. 92).“ Es lässt sich dennoch festhalten, dass Wirtschaftskriminalität die hochgesteckten Staatsziele wie zum Beispiel wirtschaftliche Entwicklung, Beschäftigungsquoten etc. an einer erfolgreichen Verwirklichung hindert (Nicevic & Ivanovic, 2012, S. 89). Angriffsziele sind hierbei häufig das Wirtschaftssystem des Staates, sozioökonomische – und Eigentumsverhältnisse. Heutzutage ist dies die gefährlichste Form des Verbrechens in den Augen des Staates und der wirtschaftlichen Interessen, da es die wirtschaftliche Macht und das gesellschaftliche Leben eines Landes untergräbt (Hlavica et al. 2011, S. 53-57; Nicevic & Ivanovic, 2012, S. 89-92). Die europäische Gesetzgebung kann auch keine klare Definition der Wirtschaftskriminalität anbieten. Obwohl es durchaus auch vorkommt, dass Betrug bei der öffentlichen Arbeit von Staatsbediensteten festgestellt wird, fokussiert sich diese Masterarbeit in erster Linie auf Betrugsfälle in Großunternehmen. Die Polizei Niedersachsen hat beispielsweise eine pauschale Erklärung gegeben, die verdeutlicht, dass die

Wirtschaftskriminalität immer in Unternehmen entsteht und auf andere Unternehmen abzielt. Diese Straftaten resultieren in einem hohen negativen Einfluss auf wirtschaftliche Prozesse (Theurer, 2016). Die Entdeckung und Aufklärung solcher Verstöße erfordert ein besonderes unternehmerisches Wissen und Verständnis. Immer als Straftat der Wirtschaftskriminalität werden die folgenden Delikte bezeichnet:„

- Anlagedelikte - Anlagebetrug § 263 StGB - Beteiligungsbetrug § 263 StGB - Betrug bei Börsenspekulationen § 263 StGB - Wertpapierbetrug § 263 StGB - Untreue bei Kapitalanlagegeschäften § 266 StGB - Kapitalanlagebetrug (Prospektbetrug) § 264a StGB
- Finanzierungsdelikte - Kreditbetrug § 265b StGB - Kreditvermittlungsbetrug § 263 StGB - Stoßbetrug § 263 StGB
- Insolvenzdelikte - Bankrott § 283 StGB - Besonders schwerer Fall des Bankrotts § 283a StGB - Gläubigerbegünstigung § 283c StGB - Schuldnerbegünstigung § 283d StGB - Insolvenzverschleppung GmbHG, HGB - - Leistungskreditbetrug/Warenkreditbetrug im Zusammenhang mit Insolvenzen § 263 StGB
- Arbeitsdelikte – Arbeitsvermittlungsbetrug § 263 StGB - Beitragsbetrug zum Nachteil von Sozialversicherungsträgern § 263 StGB - Vorenthalten und Veruntreuung von Arbeitsentgelten § 266a StGB - Illegale Arbeitnehmerüberlassung §§ 15, 15a AÜG
- Wettbewerbsdelikte - Verrat von Geschäfts- oder Betriebsgeheimnissen § 17 UWG - Progressive Kundenwerbung §§ 6c, 16 UWG, - Ausschreibungsbetrug § 298 StGB - Subventionsbetrug § 264 StGB - Gewerbsmäßige Verstöße gegen Urheberrechtsbestimmungen (§ 108a UrhG)
- Gesundheitsdelikte - Abrechnungsbetrug § 263 StGB (Landeskriminalität Niedersachsen , 2017).“

Die Association of Certified Fraud Examiners (ACFE) hält fest, dass die am häufigsten auftretenden kriminellen Kategorien folgende sind: „Kriminelle Aktivitäten in Finanzberichten, die Aneignung von Vermögenswerten und Korruption (Silverstone & Sheetz, 2007, S. 12).“

Eine weitere Unterscheidung der Straftaten wird häufig vorgenommen in:

- Veruntreuung von öffentlichen Geldern oder Betrug und
- kriminelle Handlungen im Jahresabschluss - die sogenannten „Weiße-Kragen“ Verbrechen

Betrug in der Finanzberichterstattung, als eine von den häufigsten drei Straftatkategorien, ist eine Untergruppe von Straftaten, die am häufigsten seitens der Managementebenen oder seitens der unternehmensverantwortlichen Personen durchgeführt werden. Daraus entwickelte sich der Name „Weiße-Kragen“. Sie verwenden Täuschungen als Mittel zur Erlangung eines rechtswidrigen materiellen Gewinns. Infolgedessen treten im Jahresabschluss wesentliche Angaben gefälscht auf. Die spezifischen Kennzeichen dieser Gruppe lassen sich in ihrer besonderen Arbeitssphäre (Versicherungen, Banken, Börsen, ...), in ihrem Status (obere Mittelschicht und Oberschicht) und in ihrer Art und Weise wie sie Verbrechen begehen (diskret, latent und intelligent) feststellen. Diese „Weiße-Kragen“ Verdächtigen bewegen sich oft in hohen sozialen Kreisen, haben auch im Unternehmen gute Positionen inne, und nutzen diese aus, um eigene Interesse zu verwirklichen (Hlavica et al. 2011, S. 86-87; Suput, 2009, S. 169). Die Wirtschaftsprüfungsgesellschaft KPMG hat in Indien, im Nahen Osten, in Südafrika und in Europa eine umfangreiche Untersuchung durchgeführt, mit dem Ziel ein Basismuster festzustellen, anhand dessen Täter einfacher identifiziert werden können. Als Kriterien wurden die berufliche Tätigkeit und die Beziehung zu dem betroffenen Unternehmen genommen, sowie die Persönlichkeit und potenzielle Motive einbezogen. Die Studie hat ergeben, dass Täter in der Regel zwischen 36 und 55 Jahren alt sind, tendenziell eher männlich als weiblich, seit mindestens 3 Jahre bei dem Unternehmen tätig sind und von anderen Kollegen sehr respektiert werden. Die Täter sind keine Teamplayer, sondern Einzelkämpfer, die langsam und durchdacht arbeiten. Am stärksten betroffen sind die Wirtschaftsbereiche des Rechnungs- und Finanzwesens, danach folgt der Vertriebsbereich. Neben den unternehmensinternen Mitarbeitern, können auch Externe einen Betrug tätigen. Die Studien zeigen, dass es sich im Normalfall um Menschen handelt, die dem Unternehmen sehr nah sind, und deren Erfolg von diesen Unternehmen abhängt. Die größte Gefahr stellen dabei die Lieferanten (35%) dar; gefolgt von Kunden (26%) und Subunternehmen (19%). Die externen Berater, Aktionäre und Joint-Venture-Partner hingegen, begehen wesentlich seltener Finanzbetrüge (Melcher, 2009, S. 8-9).

In Österreich dient das Finanzstrafgesetz (FinStrG) als gesetzliche Grundlage für die Bekämpfung jeglicher Finanzbetrüge und definiert diese als „von Strafe bedrohten Taten (Handlungen oder Unterlassungen) natürlicher Personen. Finanzvergehen sind auch andere ausdrücklich mit Strafe bedrohte Taten, wenn sie in einem Bundesgesetz als Finanzvergehen

oder als Finanzordnungswidrigkeiten bezeichnet sind." Als Verstoß gegen FinStrG ist auch ein Versuch des Finanzbetrugs strafbar. FinStrG ist aber nur anwendbar, wenn das Verbrechen geographisch auf Österreich begrenzt ist. Für alle Delikte die darüber hinausgehen, bzw. schwerere gesetzliche Verbrechen darstellen, kommt das Strafgesetzbuch (StGB) zur Anwendung (Bundeskanzleramt, 2017).

Eine weitere sehr verbreitete Form der Wirtschaftskriminalität ist die Geldwäsche. Das Konzept der Geldwäsche entwickelte sich in den Vereinigten Staaten in den 30er Jahren des zwanzigsten Jahrhunderts zum Zeitpunkt des Verbots von alkoholischen Getränken und Glücksspielen (Morris-Cotterill, 1999). Alle Gelder, die seitens der Alkoholproduzenten und Schmuggler verdient wurden, haben diese trügerischer Weise an amerikanischen Behörden beispielsweise als Gewinn aus eigener Autowäscherei gemeldet. Schneider definiert den Begriff Geldwäsche folgendermaßen: „Geldwäsche ist der Prozess, durch den Erlöse, die aus kriminellen Tätigkeiten stammen, transportiert, überwiesen, konvertiert oder mit legalen Geschäften vermischt werden, in der Absicht, die wahre Herkunft, die Beschaffenheit, die Verfügung über oder das Eigentum an solchen Erlösen zu verschleiern oder zu verheimlichen (Schneider, 2009, S. 4).“ Durch diese kriminellen Tätigkeiten werden alle anderen Wirtschaftssubjekte negativ beeinflusst. Geldwäsche, sowie andere Arten der organisierten Kriminalität, zielen darauf ab, eine „Schattenwirtschaft“ in allen Staaten zu etablieren und dadurch alle Wirtschaftsprozesse zu beeinflussen. Das gewaschene Geld lässt sich wesentlich leichter verdienen als das legale, und dadurch wird ein fairer Wettbewerb im Vorhinein bereits verhindert (IPFS, 2018). Das europäische Parlament lässt diesbezüglich verlautbaren: „ohne eine Koordinierung auf Gemeinschaftsebene könnten Geldwäscher und Geldgeber des Terrorismus versuchen, Vorteile aus der Freiheit des Kapitalverkehrs und der damit verbundenen finanziellen Dienstleistungen, die ein einheitlicher Finanzraum mit sich bringt, zu ziehen, um ihren kriminellen Tätigkeiten leichter nachgehen zu können (Amtsblatt der Europäischen Union, 2005).“ Die organisierte Kriminalität und Geldwäsche können schnell und einfach die Finanzsysteme weltweit erschüttern (Sejfulovic, 2012, S. 10-11). Das Europäische Parlament und der Rat der Europäischen Union betonen die Wichtigkeit der Geldwäscheprävention, insbesondere durch die Richtlinie 2005/60/EG, Artikel 47 und Artikel 95: „Massive Schwarzgeldströme können die Stabilität und das Ansehen des Finanzsektors schädigen und sind eine Bedrohung für den Binnenmarkt; der Terrorismus greift die Grundfesten unserer Gesellschaft an... (Amtsblatt der Europäischen Union, 2005).“ Die

österreichische Justiz setzt sich mit der Frage der Geldwäsche intensiv auseinander. Die Absätze 1 des §165 und §278c des österreichischen Strafrechts setzen zu diesem Zweck die EU-Richtlinien 2005/60/EG und 2006/70/EG in das österreichische Recht um (Bundeskanzleramt, 2017).

2.1.1. Bestimmung des Begriffs „Betrug“

Die Literatur notiert zahlreiche Versuche, den Begriff des Betrugs genau zu bestimmen. Die österreichische Gesetzgebung definiert den Betrug als „Vorsatz, durch das Verhalten des Getäuschten sich oder einen Dritten unrechtmäßig zu bereichern, jemanden durch Täuschung über Tatsachen zu einer Handlung, Duldung oder Unterlassung verleitet, die diesen oder einen anderen am Vermögen schädigt... (Strafgesetzbuch , 2017).“ Die Finanzbetrüge entstehen vor allem dann, wenn eigene Interessen dem Unternehmensinteresse übergestellt werden (Aleksic, Uloga i znacaj forenzickog racunovodjstva u otkrivanju finansijskih prevara, 2015, S. 235; Dimitrijevic, 2015, S. 150; Leisinger, 2008, S. 174-175).

Die ACFE definiert Betrug in den Abschlüssen als „absichtliche, vorsätzliche, ungenaue Behauptung oder Unterlassung von materiellen Aussagen oder Buchhaltungsdaten, die mit anderen Informationen als Ganzes beobachtet wird, zeigt an, dass der Leser sein Urteil oder seine Entscheidung ändert oder neu ordnet.“ Laut den internationalen Revisionsstandards wird der Betrug im Rechnungslegungsprozess als vorsätzliche Handlung, die von einer oder mehreren Personen, mit leitenden Funktionen, die für das Management, die Arbeitnehmer oder Dritte verantwortlich sind, begangen, um unlautere oder rechtswidrige Leistungen zu erhalten (Dimitrijevic, 2015, S. 139; Rezaee, 2002, S. 2).

Eine weitere Definition des Betruges im Jahresabschluss haben Julie Marget und Geoffrey Peck bekannt gegeben: „Betrug in Abschlüssen ist eine Handlung vorsätzlicher Täuschung, die zu einer irreführenden Darstellung, einer wesentlichen falschen Darstellung oder einem beabsichtigten Ausschluss in den Finanzkonten eines Unternehmens führt. Die Täuschung wird mit der Absicht begangen, Aktionäre und andere Stakeholder über den Finanzstatus der Geschäftseinheit irrezuführen. Der Betrug kann irreführend finanzielle Umstände oder einen nicht finanziellen Sachverhalt mit sich bringen (Margret & Peck, 2015, S. 1).“

2.1.2. Betrugsarten

Betrüge in der Finanzberichterstattung werden in unterschiedliche Kategorien unterteilt. Die übliche Aufteilungsweise von Betrügen in der Finanzberichterstattung ist durch ihre Gruppierung im Rahmen der folgenden fünf Rechnungslegungszyklen, in denen sie mit hoher Wahrscheinlichkeit zumindest eine Form von Prüfungsspur hinterlassen, gegliedert:„

1. Verkaufs- und Abrechnungszyklus

2. Kauf- und Zahlungszyklus

3. Lohnlisten- und Kaderzyklus

4. Bestands- und Lagerungszyklus

5. Erwerb von Kapital und Geldrückerstattung (Silverstone & Sheetz, 2007, S. 26)."

Der Verkaufs- und Abrechnungszyklus ist der mächtigste Bargeld-Rechnungslegungszyklus. Die häufigsten Missbräuche in diesem Zyklus sind die Aneignung von täglichen Verkäufen, Nicht-Evidentierung von Verkäufen, Verkauf zu niedrigeren Preisen als vorgeschrieben, Darstellung von Verkäufen an fiktive Kunden u.Ä. Dieser Zyklus ist wesentlich mehr als die anderen Zyklen mit Bargeldgeschäften verknüpft.

Der Kauf- und Zahlungszyklus umfasst Zahlungen für Waren, Ausrüstung und Dienstleistungen für den Geschäftsbetrieb der juristischen Person. Dieser Zyklus ist folgenden Betrugsarten ausgesetzt: Zahlungen an fiktive Kunden, Zahlung von Waren und Dienstleistungen zu überhöhten Preisen, Kauf von Waren in unnötig großen Mengen u.Ä. In Abhängigkeiten von der Natur des Betrugs, arbeiten die Täter als Einzelgängern, oder zusammen mit anderen Kollegen und/oder Geschäftskunden und Partner.

Der Lohnlisten- und Kaderzyklus beschäftigt sich mit der Anstellung und Entlassung von Mitarbeitern sowie mit deren Löhnen, Arbeitszeiten, Kostenvergütungen und Krankheit. In diesem Zyklus ist es möglich, fiktive Mitarbeiter zu bezahlen, Arbeitszeiten zu erhöhen, Kosten zu überschätzen u.Ä. Meistens sind sowohl die Mitarbeiter aus der Personalabteilung einer Firma involviert, als auch die Bewerber.

Der Bestands- und Lagerungszyklus kontrolliert die Beschaffung, die Lagerung und den Verbrauch von Rohstoffen und Materialien. Die Betrüge im Zusammenhang mit den Beständen sind Bestellungen von unnötigen Materialien, Aneignung von Mitteln u.Ä. Die Täter

sind im Normalfall die Fahrer, Lagerkontrollen und die unternehmensunabhängigen Personen, die die gestohlenen Güter annehmen (Silverstone & Sheetz, 2007, S. 26-33).

Betrug entsteht auch bei der Finanzierung von Schulden. Diese Schuldenfinanzierung kann durch Kapital und Geldrückerstattungen erfolgen. Dies beinhaltet beispielsweise Aktienkapital, Zahlungen von Zinsen oder Dividenden. All diese Transaktionen werden für gewöhnlich auf hohen Managementebenen ausgeführt. Somit können auch alle Betrüge, die in Zusammenhang mit solchen Transaktionen stehen, nur von den Leitern des Unternehmens ausgeführt werden. Beispiele für derartige betrügerische Aktivitäten können unter anderem Geldanleihen für persönliche Bedürfnisse durch eine juristische Person, Missbrauch von Dividenden und Erträgen aus Finanzierungen, oder die Manipulation von Aktienkursen an der Börse sein. Der Erwerb von Kapital und Geldrückerstattung beinhaltet die Finanzierung von Schulden auch mit Aktienkapital, Zahlungen von Zinsen und Dividenden (Silverstone & Sheetz, 2007, S. 26-33).

Zu den Tätern der illegalen Handlungen von Führungskräften (Management-Betrug) gehören Geschäftsführer, Führungskräfte und andere Manager. Illegale Handlungen von Arbeitnehmern (Arbeitnehmer-Betrug) werden von Arbeitnehmern und Mitarbeitern in ausführenden Funktionen durchgeführt. Als Beispiel für illegale Handlungen von Arbeitnehmern kann die rechtswidrige Aneignung von Vermögen angegeben werden – Stehlen von Bargeld durch den Kassierer/Schatzmeister, Stehlen von Waren durch den Lagermitarbeiter usw.

Besonders charakteristisch sind Betrüge im Zusammenhang mit der Amtstätigkeit (Amtsbetrug). Dabei handelt es sich um die Ausnutzung der eigenen amtlichen Position bei der Arbeit/Beruf mit der Absicht, sich eigenen materiellen Nutzen in einer unwürdigen Weise anzueignen. Die Art des Betrugs ist industrieabhängig, aber Betrüge entstehen überwiegend durch Lügen, falschen Darstellungen, Datenverfälschung und Korruption (Zahra et al. 2005, S. 803-806).

Illegale Handlungen zur Bereicherung der Organisation werden überwiegend von Mitgliedern des Top-Managements ausgeführt, um Aktionäre, Gläubiger, Staatsbehörden und andere Personen in Hinsicht auf die Vermögens- und Ertragslage des Unternehmens zu täuschen. Die Opfer illegaler Handlungen zur Bereicherung der Organisation können Verbraucher, Aktionäre, Gläubiger, Mitbewerber, Banken, Versicherungsinstitute und

Staatsbehörden sein. Die charakteristischen Arten von illegalen Handlungen zum Schaden der Verbraucher sind: Nicht wahrheitsgetreue Bewerbung und Darstellung in der Öffentlichkeit, nicht wahrheitsgetreue Markenzuteilung, Lieferung von kleineren Mengen, Gewicht und anderer quantitativer Maßeinheiten als bestellt, Ersatz von Qualität, billige Imitationen, fehlerhafte Produkte und Fixierung der Preise. Die Beispiele für illegale Handlungen zur Bereicherung der Organisation aber zum Schaden der Banken sind nicht wahrheitsgetreue Jahresabschlüsse und nicht wahrheitsgetreue Anträge auf die Gewährung von Darlehen.

Beispiele für die Täuschung von Versicherungsinstituten sind falsche Schadensersatzansprüche, Brandlegung, unwahre Anmeldung für die Versicherungen usw. Die genannten Täuschungen führen zu Vertrauensverlust in die Führungskräfte und die Institutionen. Die Institutionen wiederum verlieren das Vertrauen in das Staatssystem. Sobald das Staatssystem droht instabil zu werden, erfolgt eine Einmischung seitens der Politik und somit auch seitens der Öffentlichkeit. Folglich verlangt die Regierung strengere Sicherheitsmaßnahmen in Unternehmen, was wiederum einen direkten Einfluss auf die Unternehmenskosten hat (Easterly, 2005; Aghion & Durlauf, 2005) Moore und Mills (1990) haben dieses Phänomen als „ein allgemeines Wachstum des Zynismus in einer Gesellschaft“ bezeichnet. Autoren wie Fukuyama (1995) sind der Meinung, dass „der wirtschaftliche Erfolg kapitalistischer Gesellschaften auf dem Niveau des Vertrauens und des daraus resultierenden kooperativen Verhaltens in diesen Gesellschaften beruht.“ Folge daraus ist die sogenannte Zerstörung des Sozialsystems und Markts (Zahra et al. 2005, S. 815-819).

Die illegalen Handlungen vor der Eintragung und illegalen Handlungen nach der Eintragung in den Geschäftsbüchern lassen sich folgendermaßen erläutern: Geschäftsbücher stellen einheitliche Aufzeichnungen über den Stand und die Änderungen des Vermögens, der Verbindlichkeiten, des Kapitals sowie der Einnahmen und Ausgaben von juristischen Personen und Unternehmern dar. Die Geschäftsbücher bestehen aus dem Buchungsjournal, dem Hauptbuch und den Hilfsbüchern. Illegale Handlungen, die vor der Eintragung in den Geschäftsbüchern durchgeführt werden, werden vor der Verarbeitung und Buchung eines Geschäftsereignisses in der Rechnungslegung durchgeführt. Empfangene Mittel (häufig Bargeld) werden nicht dokumentiert, sondern versteckt und für sich behalten, und so wird deren Eintragung vermieden. Diese illegalen Handlungen sind am schwierigsten aufzudecken, weil sie keine schriftliche Spur hinterlassen. Die häufigsten Täter dieser Art von illegalen Handlungen sind Personen, die auf irgendeine Weise mit Bargeld in Kontakt gekommen sind,

wie beispielsweise Schalter-Mitarbeiter, Tresor-Mitarbeiter, Kassierer/Schatzmeister, Verkäufer und alle anderen Mitarbeiter, die unmittelbar von Kunden und Käufern Bargeld empfangen. Die illegalen Handlungen, die nach der Eintragung in den Geschäftsbüchern getätigt werden, werden nach der Verarbeitung und Buchung im Rechnungslegungssystem durchgeführt. Diese Arten von illegalen Handlungen sind seltener im Vergleich zu den vorher angeführten, und sie sind leichter aufzudecken, da im Rechnungslegungssystem eine schriftliche Spur über das veruntreute Vermögen zu finden ist (Dimitrijevic, 2015, S. 143-145).

2.1.3. Cyberkriminalität

Wir leben in einer Zeit, in der es dank neuer Technologien schnell und einfach möglich ist, Informationen aus diversen Quellen weltweit abzurufen, sich mit anderen Menschen innerhalb von Sekunden verbinden zu können, online Einkäufe zu tätigen, etc. Die Rechner und Internetanschlüsse sind relativ billig und zum Alltag für viele Menschen geworden. Technologie wurde als Luxus Europas und Amerikas angesehen, aber mittlerweile steigt auch die Anzahl der Internetnutzer aus Afrika und Asien massiv an (Brodowski & Freiling, 2011, S. 31).

Die andere Seite der Technologie-Medaille weist auch negative Folgen auf. Durch die Verwendung des Internets entwickelt sich auch die Cyberkriminalität sehr leicht und schnell (Nykodym et al., 2005). Sie ist auch zu einem Teil des Alltags geworden, obwohl das Bewusstsein dafür oft nicht vorhanden ist (Babu & Parishat, 2004).

Insbesondere hoch entwickelte Länder legen viel Wert auf die Bekämpfung von Cyberkriminalität. Diese Problematik hat sich zu einer relevanten Sicherheitsfrage für viele Nationen entwickelt. Nicht nur die Regierung und Gesetzgebung muss sich mit Cyberkriminalität auseinandersetzen, sondern die gesamte Bevölkerung. Wird in Betracht gezogen, dass in Deutschland im Jahr 1992 bereits 12.435 Fälle von Cyberkriminalität registriert worden sind, lässt sich nur ansatzweise schätzen, wie hoch diese Zahl heutzutage sein muss (Kompjuterski i cyber kriminal, S. 158-162).

Der Begriff der Cyberkriminalität weißt bis heute keine klar abgegrenzte Definition auf. Laut der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) umfasst sie „jegliche illegale, unethische oder unerkannte Verhalten mit automatischer Datenverarbeitung und/oder Datenübertragung“. Computerkriminalität wird auch als

belastendes Verhalten definiert, in dem der Rechner als ein Mittel zur Ausführung oder Gegenstand der Tat erscheint. Manche Akteure definieren diese Art von Kriminalität als jede Art von Angriff, die mit elektronischer Datenbearbeitung eng verknüpft ist.

Folgende Tätigkeiten fallen unter den Bereich der Computerkriminalität:„

- nicht autorisierter Zugriff auf einen geschützten Computer
- unbefugtes Abfangen von elektronischen Daten, die von einem zu einem anderen Computer gesendet werden
- Zerstörung, Änderung und Löschung von elektronischen Daten
- Beeinträchtigung oder Sperrung der Funktionsweise des Computersystems durch Beschädigen, Löschen, Ändern oder Einfügen von elektronischen Daten
- Verteilung nicht autorisierter Inhalte
- Erstellung und Verbreitung von Viren und bösartiger Software (Kompjuterski i cyber kriminal, S. 161)."

Österreichische Behörden haben eine ähnliche Sichtweise wie die OECD. Sie differenzieren Delikte der Computerkriminalität in sechs Kategorien: „

- Widerrechtlicher Zugriff auf ein Computersystem (§ 118a StGB)
- Datenbeschädigung (§ 126a StGB)
- Störung der Funktionsfähigkeit eines Computersystems (§ 126b StGB)
- Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126c StGB)
- Betrügerischer Datenverarbeitungs- missbrauch (§ 148a StGB)
- Datenfälschung (§ 225a StGB) (Bundesministerium für Justiz, 2016, S. 46).“

Regierungen und Unternehmen sehen sich heutzutage mit einer höchst technologisierten Formen der Cyber-Kriminalität konfrontiert: Verletzung des geistigen Eigentums, Piraterie und Computerdiebstahl durch Internetnetzwerke. In vielen Ländern sind neue strickte Gesetze in Kraft getreten, die jegliche Art von Verletzung des geistigen Eigentums bekämpfen (Kompjuterski i cyber kriminal, S. 158-162; Der österreichische Zoll, 2013).

Die österreichische Gesellschaft und Regierung sind mit den Gefahren von Cyberkriminalität durchaus vertraut und sich dieser zum Teil auch bewusst, da sie neue Technologien und die damit verbundenen Risiken schon vor Jahren akzeptiert haben. Sie

unterstützen die technologische Weiterentwicklung jedoch, da diese trotzdem auch viele Vorteile mit sich bringt. Konsumenten treffen mittlerweile beinahe alle Kaufentscheidungen mit Hilfe des Internets. Ohne ein Handy ist der Alltag kaum vorstellbar. Unternehmen haben Schwierigkeiten mit diesem Entwicklungstempo stand zu halten und ihre Geschäfte z.B. an die „Industrie 4.0¹“ anzupassen. Langsam aber sicher ändert sich das gesamte Wirtschaftsleben. Alle Branchen ändern sich unter dem Druck der neuen Entwicklungen. Konservative Branchen, die traditionell aufgestellt sind, wie etwa am Beispiel des Bankwesens erkennbar, zeigen trotzdem noch immer großen Widerstand und wollen sich nicht „digitalisieren lassen“, sie haben sich aber dennoch den Entwicklungen der Zeit mehr oder weniger gefügt. Viele Mitarbeiter haben Angst vor Veränderungen und glauben, dass die Digitalisierung mit einer reinen Automatisierung gleichzusetzen ist und ihnen in Folge dieser, der Verlust ihrer Arbeitsplätze droht. Trotzdem sind die Vorsitzenden in der österreichischen Wirtschaftskammer davon überzeugt, dass Österreich bis 2020 eines der besten europäischen Länder in Hinsicht auf die IT-Sicherheit und Digitalisierung werden kann (CCM-TV, 2017).

Es hat sich gezeigt, dass Unternehmen die negativen Seiten des Internets unterschätzten und Opfer von Cyberkriminalität geworden sind (Der Standard, 2017). Offiziell ist in einem Jahr, von 2015 bis 2016, die Anzahl der Cyberangriffe von 10.010 auf 13.103 gesprungen. Diese Zahlen entsprechen einem Anstieg von fast 31%. Experten sind aber der Meinung, dass die Dunkelziffer wesentlich höher ist und, dass in Österreich mit ca. 25.000 Angriffen am Tag gerechnet werden kann (CCM-TV, 2017). Die Wirtschaftsprüfungsgesellschaft KPMG hat ebenso eine Studie durchgeführt, mit dem Ziel, festzustellen, wie viele Unternehmen in Österreich mit der Cyberkriminalität konfrontiert werden. Ihre Ergebnisse zeigen, dass „72% aller Unternehmen in Österreich in den letzten 12 Monaten Opfer einer Cyberattacke waren und, dass davon jedes zweite Unternehmen als Folge unter einer Unterbrechung der Geschäftsprozesse litt.“ KPMG betont, dass jedes Unternehmen zum Opfer werden kann, unabhängig von Branche, aber, dass die Industrieunternehmen am häufigsten betroffen sind (KPMG, 2017).

¹ Vernetzung von industrieller Produktion mit moderner Informations- und Kommunikationstechnik (Bundesministerium für Wirtschaft und Energie, 2018)

KPMG hat sich weiter mit der Frage „Was sind die Ursachen von Cyberangriffen?“ beschäftigt und die Ergebnisse lauten: 90% Malware², 89% Phishing³ und 47% Social Engineering⁴. Das lässt vermuten, dass sich Unternehmen auf die interne Kultur und Sicherheiten fokussieren müssen, wenn sie zukünftig die Anzahl der Angriffe reduzieren wollen. KPMG hat auch die Meinung von Experten bestätigt, dass sie die österreichischen Unternehmen zu wenig mit dem Thema „Industrie 4.0“ beschäftigen und sogar 40% der befragten Unternehmen haben zugegeben, dass sie keinen Überblick über „Internet of Things“⁵ (IoT) und ähnlichen Themen haben. Folglich ist der Schutz vor Angriffen kaum bis gar nicht vorhanden und alle Unternehmen sollten diesem Thema deshalb so schnell wie möglich eine hohe Priorität zuweisen (KPMG, 2017).

In der Fachliteratur spielt in Bezug auf die Cyberkriminalität der Begriff des geistigen Eigentums eine wichtige Rolle: Das geistige Eigentum bezieht sich auf die literarischen, künstlerischen und wissenschaftlichen Arbeiten, und den daraus resultierenden Rechten. Jegliches Kopieren und/oder unberechtigtes Nutzen dieser ist eine Strafrechtstat. Unter geistiges Eigentum fallen weiter Industriedesign, Marken, Entdeckungen, etc. Der Staat ermöglicht den Schutz des geistigen Eigentums, um weitere Innovationen zu fördern. Es kann demnach festgehalten werden, dass das geistige Eigentum zum Wirtschaftswachstum, sowohl in den entwickelten Ländern, als auch in Entwicklungsländern führt (Kompjuterski i cyber kriminal, S. 162-163). „Das Urheberrecht ist das Recht des „Schöpfers“ an dem „Werk“, das er geschaffen hat. Er ist der Einzige, der bestimmen kann, was mit diesem „Werk“ geschieht. Es gibt drei Möglichkeiten eines Eingriffs in die Werkintegrität, denen der Urheber zustimmen muss:

1) eine Bearbeitung als qualitative Veränderung des Werks, bei der ein neues Werk entsteht (z. B. die Übersetzung eines Textes in eine andere Sprache);

2) eine Werksänderung als quantitative Veränderungen des Werks (Kürzungen, Zusätze) oder eine Beeinträchtigung des Werks; und schließlich

² Computerprogramm das dem Benutzer einen Schaden zufügen will - z.B. Virus (Aschermann, 2014)

³ Versuch durch gefälschte Emails oder Internetseiten geheime, persönliche Benutzerdaten zu erbeuten – z.B. Online-Banking Zugangsdaten (Bundeskanzleramt Österreich, 2018)

⁴ Trickbetrug durch zwischenmenschliche Beeinflussung (Rouse, 2006)

⁵ Internet der Dinge: Vernetzung von Geräten in Industrie und privatem täglichen Leben durch Sensoren. Die Geräte werden durch die Sensoren in gewisser Weise „intelligent“ (Computerwoche, 2018)

3) die Verbindung des Werks mit einem anderen Werk (z. B. das Unterlegen eines Films mit einer bestehenden Musikaufnahme), oder Auflösen einer bestehenden Werkverbindung (Die österreichische Justiz, 2017)."

Computertechnologien ermöglichen eine Verletzung dieses Gesetzes durch z.B. unrichtiges Zitieren und die Verwendung fremder Aussage für eigene wissenschaftliche Arbeiten. Eine weitere und weit verbreitete Art der Computer- und somit der Cyberkriminalität ist Piraterie. Es handelt sich dabei um eine Computer-Straftat, deren Basismerkmal die Verwendung oder Vervielfältigung von Programmen, Software oder anderen elektronischen Daten ist. Es kann zwischen unterschiedlichen Grundarten der Piraterie unterscheiden werden. Hierbei kann zunächst einmal die Endbenutzer Piraterie genannt werden. Diese tritt auf, wenn ein Mitarbeiter eine Software benutzt, die mit Hilfe einer illegalen Kopie des Originals auf dem Computer installiert wurde und für dessen Ausführung er keine Genehmigung hat. Als Zweites kann die Mehrfachnutzung von Client-Server Software genannt werden. Bei dieser Art der Piraterie greifen mehr Benutzer gleichzeitig auf eine zentrale Softwarekopie zu, als dies durch eine Lizenz erlaubt ist. Internet Piraterie, als dritte Form, tritt auf, wenn Software, die illegaler Weise aus dem Internet heruntergeladen wurde, genutzt wird. Eine vierte Möglichkeit ist die Aufzeichnung auf der Festplatte. Hierbei verkauft ein Unternehmen illegale Software als Teil ihres Angebotes für Computer. Durch vor dem Verkauf aufgespielte bzw. mitgelieferte Software kann die Attraktivität des angebotenen Rechners eventuell deutlich gesteigert werden. Zu guter Letzt kann im Zusammenhang mit Piraterie die gewerbsmäßige illegale Vervielfältigung angeführt werden. Dabei wird eine geschützte Software eins-zu-eins kopiert und verkauft (Kompjuterski i cyber kriminal, S. 162-163; Babu & Parishat, 2004).

Computerdiebstahl ist eine gesetzeswidrige Tätigkeit, in der das bewegliche Eigentum von dem Eigentümer illegal angeeignet wird, mit der Absicht, Gewinn zu erzielen. Unter dem Begriff Computerdiebstahl wird nicht nur Diebstahl von Rechnern und deren Komponenten verstanden, sondern auch Diebstahl von Passwörtern oder der Missbrauch von Zahlungskarten. Experten halten fest, dass letztere eine sehr gefährliche Art von Computerkriminalität darstellt und sich diese mit der Weiterentwicklung des elektronischen Handels immer mehr verbreiten wird (Kompjuterski i cyber kriminal, S. 162-163).

In Österreich unterscheidet man zwischen zwei großen Arten von Cyberkriminalität: Cyberkriminalität im engeren und im breiteren Sinne. Unter die erste Kategorie fallen unterschiedliche unerlaubte Zugriffe auf ein Computersystem. Alles was darüber hinausgeht, und Kinderpornografie, Betrugsdelikte, etc. umfasst, fällt unter die Kriminalität im weiteren Sinne. Die Cyberkriminalität im engeren Sinne ist in Österreich zwischen 2015 und 2016 um 55,1 % gestiegen. Die zweite Kategorie wurde nicht präzise erfasst. Mag. Leopold Löschl, Leiter des Cybercrime Competence Center C4 des Bundesministeriums für Inneres (BMI), ergänzt: „Ebenso haben das Unterschätzen von Cyberkriminalität und die Mängel an Präventionsmaßnahmen maßgeblichen Anteil an der zunehmenden Anzahl an Cyberattacken (CCM-TV, 2017).“

2.1.4. Motivationsfaktoren, die zum Betrug führen

Da sich Betrüger im Prozess der Finanzberichterstattung von anderen Menschen in ihren demografischen oder psychologischen Eigenschaften kaum unterscheiden, erschwert dies dem Wirtschaftsprüfer die Aufdeckung von Betrügen erheblich, da es keine herausstechenden Merkmale gibt, die ihm wichtige Hinweise zur Aufdeckung liefern könnten. Dementsprechend ist es notwendig, dass der Wirtschaftsprüfer über das Wissen von drei Schlüsselementen verfügt, die das Zustandekommen von Betrügen ermöglichen: bestehender Druck oder Anreize, offensichtliche Möglichkeit und Bestehen von rechtfertigenden Einstellungen-Rationalisierung (Stanisic, Interna kontrola i revizija, 2014, S. 339).

Es gibt verschiedene Gründe, die die Unternehmensleitung dazu veranlassen, Betrüge im Jahresabschluss zu begehen. Einer von ihnen ist die Notwendigkeit, die Gewinn- und Verlustrechnung besser aussehen zu lassen, als sie tatsächlich ist. Ebenso können die Führungskräfte falsche Jahresabschlüsse abgeben, um Fremdfinanzierung voranzutreiben. Eine schlechte Finanzleistung kann die Fähigkeit des Unternehmens reduzieren, das Kapital durch Finanzierung und andere Arten von Aktienangeboten zu erhöhen. Betrugereien entstehen auch, wenn die Unternehmensleitung versucht finanzielle Schwierigkeiten vor Kunden zu verbergen, da sie diese sonst verlieren würde. Dementsprechend kann es durchaus auch vorkommen, dass die Unternehmensleitung mit der Absicht das eigene Unternehmen besser aussehen zu lassen als es tatsächlich ist, einen Betrug im Jahresabschluss begeht (Petrovic et al. Revizijska regulativa, 2016, S. 78-80; Albrecht et al. 2009, S. 366-368).

Betrüge werden auch mit der Absicht begangen, dass das Unternehmen versucht seine eigene Unfähigkeit zu verbergen, die in den Obligationsklauseln festgelegten Bedingungen zu erfüllen. Das Betrugsmotiv kann auch Gier sein, wenn die Unternehmensleitung falsche Jahresabschlüsse vorlegt, damit das Unternehmen fortschreitet und die Unternehmensleitung ihre Positionen behält, die Gehälter und andere Managementbezüge erhöht, und damit die Vertragsbedingungen erfüllt werden, die auf diesen Vorteilen basieren. Der Wunsch nach einem höheren Lebensstandard, oder die entdeckte Möglichkeit des leichten Verdienstes führen dazu, dass Mitarbeiter oft Betrug begehen, und als Anreiz für die Betrugshandlungen können auch das Gefühl der mangelnden Wertschätzung oder der ungenügenden Bezahlung für die geleistete Arbeit auftreten, sowie die Angst des Arbeitsplatzverlustes oder der Wunsch zur Verwirklichung von unrealistischen Zielen. Betrugselemente beinhalten bereits die bloße Möglichkeit für das Begehen irgendeiner Betrugsart oder deren Verbergung bzw. Vermeidung und stehen unter Strafe (Dimitrijevic, 2015, S. 137-138; Albrecht et al. 2009, S. 366-368; Zahra et al. 2005, S. 805).

2.1.5. Faktoren und Indikatoren des Betrugsrisikos

Das Betrugsrisiko wird auf der Ebene des gesamten Unternehmens, auf der Ebene der Geschäftseinheit und auf der Ebene eines bedeutenden Postens im Jahresabschluss oder der Behauptung bewertet. Die Natur und der Umfang der Aktivitäten im Zusammenhang mit der Risikobewertung sollten der Größe des Subjekts und der Komplexität des durch ihn ausgeübten Geschäfts entsprechen. Die Faktoren des Betrugsrisikos auf der Ebene des Jahresabschlusses können anhand von drei Bedingungen aufgeteilt werden, die dann vorliegen, wenn als Folge des Betrugs im Jahresabschluss falsche Angaben auftauchen. Dies sind Anreize oder Druck, Möglichkeit für die Begehung des Betrugs, und rechtfertigende Einstellung und Rationalisierung nach dem Betrug selbst. Jeder der angeführten Faktoren enthält mehrere vorhandene Risikofaktoren, und für jeden Risikofaktor können bestimmte Indikatoren identifiziert werden, die auf einen stattgefundenen Betrug hinweisen können. Diese drei Bedingungen sind subjektiv und daher abhängig von der Persönlichkeit des Betrügers. Trotzdem wird oft argumentiert, dass „Gelegenheit Diebe macht (Glaser, 2015, S. 313).“ Nachfolgend findet sich eine Übersicht der Risikofaktoren und Indikatoren (Stanisic, Interna kontrola i revizija, 2014, S. 339-340; Albrecht et al. 2009, S. 75-76):

Die finanzielle Stabilität und Profitabilität von Subjekten sind von wirtschaftlichen, marktspezifischen oder branchenspezifischen Bedingungen bedroht, in der das Subjekt geschäftstätig ist. Die Indikatoren sind: Ein hohes Maß an Wettbewerb oder Marktsättigung, begleitet von sinkenden Profiten, hoher Sensibilität gegenüber raschen Veränderungen wie z.B. technologischen Änderungen, Produktveralterung oder Änderung der Zinssätze sowie deutlicher Rückgang der Käufernachfrage, Betriebsverluste, die zum Bankrott oder Konkurs führen können, das Subjekt kann zum Ziel einer feindlichen Übernahme werden (Stanisic, Interna kontrola i revizija, 2014, S. 343; 359-360).

Ein weiterer Faktor ist der große Druck auf das Management, die Erwartungen und Forderungen von Dritten zu erfüllen. Es gibt Erwartungen hinsichtlich der Profitabilität durch Investoren, Gläubiger und andere Stakeholder, die übermäßig aggressiv sind, oder unrealistische Erwartungen durch das Management, die in Pressemitteilungen und anderen Berichten veröffentlicht wurden. Ebenso besteht ein Bedarf an zusätzlichen Finanzierungsquellen, damit das Subjekt wettbewerbsfähig bleibt, einschließlich Finanzierung größerer Forschungs- und Entwicklungsprojekte oder Kapitalanlagen (Albrecht et al. 2009, S. 366-369; Schwanfelder, 2017).

Der Faktor des Betrugsrisikos besteht, wenn ein hoher Druck auf das Management und die Mitarbeiter in operativen Geschäften besteht, die durch die Unternehmensleitung gesetzten finanziellen Ziele zu erreichen, einschließlich Ziele in Bezug auf Verkauf und Erhöhung der Profitabilität. Die Natur der Branche und das Geschäft des Unternehmens bieten die Möglichkeit, sich auf eine falsche Finanzberichterstattung einzulassen. Auf diesen Faktor weisen Transaktionen hin, die nicht dem üblichen Geschäftsverlauf entsprechen, in denen die betroffenen Seiten nicht der Wirtschaftsprüfung unterliegen oder die von einer anderen Firma geprüft werden (Albrecht et al. 2009, S. 366-369).

Ineffiziente Rechnungslegungs- und Informationssysteme führen zu Fehlern in der Funktionsweise der aufgestellten Kontrollen. Das Management schafft es nicht, die bedeutenden internen Mängel der internen Kontrolle zu beseitigen. Das Erkennen von Warnzeichen ist ein entscheidender Faktor für eine erfolgreiche Betrugsaufdeckung. Diese führen zur Ausarbeitung effektiver Methoden und Verfahren für das Aufdecken von Betrugsfällen. Oft kann ein gutes Verfahren zur Betrugsaufdeckung auch als gutes

Kontrollverfahren dienen (Stanisic, Interna kontrola i revizija, 2014, S. 20-25; Albrecht et al. 2009, S. 143).

Die angeführten Indikatoren können jedoch keine ausreichende Grundlage für das Ableiten von Schlussfolgerungen sein, die sie sich darauf beziehen ob das Risiko für das Entstehen des Betrugs im Jahresabschluss hoch oder niedrig ist. Um das Betrugsrisiko zu bewerten, sind eine tiefgreifende Analyse der Geschäftsprozesse und eine detailliertere Untersuchung aller sich im Unternehmen ereignenden Geschehnisse notwendig (Stanisic, Interna kontrola i revizija, 2014, S. 20-25).

2.2. Internationale Prüfungsstandards

Die Internationalen Prüfungsstandards (International Standards of Auditing - ISA) werden seit 1977 angewendet. Mit ihnen hat sich vorerst der Ausschuss für internationale Prüfungsstandards (Auditing Practices Committee – IAPC) befasst. 1978 wurde das International Auditing and Assurance Standard Board (IAASB) gegründet, und die Verantwortung über ISA übernommen. Die Internationalen Prüfungsstandards beziehen sich auf die Internationalen Prüfungsstandards (ISA) und die damit verbundenen Statements und Standards, in demjenigen Umfang, in dem sie für die gesetzlich vorgeschriebene Wirtschaftsprüfung relevant sind (Petrovic, Medjunarodni standardi revizije, 2010, S. 14-20). Die ISA Standards legen fest, was die Verantwortlichkeiten von Prüfern bei einer Prüfung sind (ISAAB, 2018).

Mit den Problemen des Betrugs im Jahresabschluss befasst sich der Internationale Prüfungsstandard – ISA 240 – *Verantwortung des Wirtschaftsprüfers* ist die Erörterung von kriminellen Handlungen und Fehlern bei der Wirtschaftsprüfung des Jahresabschlusses. Die im Standard enthaltene Grundvoraussetzung ist die Anforderung, dass „der Wirtschaftsprüfer bei der Planung und Durchführung der Wirtschaftsprüfung, im Ziele der Verringerung des Prüfungsrisikos auf ein annehmbar niedriges Niveau, das Risiko von materiell falschen Angaben im Jahresabschluss infolge von kriminellen Aktivitäten in Betracht zieht.“ Mit dem Standard sind Regeln und Richtlinien für Fragen gegeben, die sich mit den Eigenschaften der kriminellen Handlungen, Verantwortlichkeiten der Personen mit Führungsaufgaben, Identifizierung und Bewertung des Betrugsrisikos, Beurteilung von Prüfungsnachweisen usw. befassen (Petrovic et al. Revizijska regulativa, 2016, S. 234; Scholz, 2017, S. 87).

Der Internationale Prüfungsstandard – ISA 260 – *Bekanntgabe der Prüfungsbefunde an verwaltungsbefugte Personen* wurde 2015 vom „International Auditing and Assurance Standards Board“ (IAASB) verabschiedet. Den ISA 260 wenden externe Wirtschaftsprüfer bei der Prüfung von allgemeinen Jahresabschlüssen an. Die Anforderungen des ISA 260 beziehen sich in erster Linie auf die Kommunikation der Wirtschaftsprüfer mit den verwaltungsbefugten Personen, mit einem darin eingeschlossenen umfassenden Rahmen dieser Kommunikation und den zu kommunizierenden Fragen (Petrovic et al. Revizijska regulativa, 2016, S. 183). „Dieser Standard wird unabhängig von der Führungsstruktur oder der Größe des Prüfungskunden verwendet“ sowie „bei denjenigen Prüfungskunden, bei denen alle verwaltungsbefugten Personen an der Führung des Prüfungskunden beteiligt sind, sowie bei Subjekten, deren Inhaber-Wertpapiere an der Börse sind (Petrovic, Medjunarodni standardi revizije, 2010, S. 107-109; IFAC ISA 260, 2009, S. 214).“

Der Internationale Prüfungsstandard – ISA 570 – *Grundsatz der Unternehmensweiterführung des Prüfungskunden* wurde ebenso 2015 verabschiedet. Er wird von externen Wirtschaftsprüfern bei der Durchführung der Prüfung von allgemeinen Jahresabschlüssen angewendet. ISA 570 befasst sich mit den Verantwortlichkeiten der Wirtschaftsprüfer im Zusammenhang mit der Anwendung der Annahme des zeitlich unbegrenzten Geschäftsbetriebs zum Zeitpunkt der Erstellung des vom Prüfungskunden festgelegten Jahresabschlusses (IFAC ISA 570, 2018, S. 545-547).

Die Standards legen folgende Ziele des Wirtschaftsprüfers fest:

1. dass er ausreichend zufriedenstellende Prüfungsnachweise sammelt, die eine objektive Annahme für die Prüfung des Managements, des Prüfungskunden über die zeitliche Unbegrenztheit des Geschäftsbetriebs des Prüfungskunden, die bei der Erstellung des Jahresabschlusses angewendet werden, rechtfertigen;
2. dass er aufgrund der vorgelegten Prüfungsnachweise die Schlussfolgerung ziehen kann, ob eine bedeutende Unsicherheit im Zusammenhang mit Ereignissen oder Umständen besteht, die eine erhebliche Unsicherheit im Zusammenhang mit der Möglichkeit des Prüfungskunden verursachen können, mit dem zeitlich unbegrenzten und langdauernden Geschäftsbetrieb fortzusetzen; und

3. dass er den Bestätigungsvermerk und die Stellungnahme unter Beachtung der Anforderungen des Standards erstellt (Petrovic et al. Revizijska regulativa, 2016, S. 293; IFAC ISA 570, 2018, S. 545-547).

ISA 570 schreibt vor, dass der Wirtschaftsprüfer bei der Wirtschaftsprüfung und Beurteilung der erhaltenen Ergebnisse die Richtigkeit der Annahme des Grundsatzes des kontinuierlichen Geschäftsbetriebs des Prüfungskunden erörtern muss, auf Basis derer die Unternehmensleitung den Jahresabschluss erstellt hat (Petrovic et al. Revizijska regulativa, 2016, S. 293; IFAC ISA 570, 2018, S. 545-547).

Der Standard *ISA 700 – Bildung der Stellungnahme und Berichterstattung über den Jahresabschluss* regelt die Verantwortlichkeit des Wirtschaftsprüfers bei der Erstellung der Stellungnahme zum Jahresabschluss. Er regelt auch die Form und den Inhalt des Bestätigungsvermerks, der auf der Grundlage der Prüfung des Jahresabschlusses ausgestellt wurde. Das Ziel von ISA 700 ist es, Normen zu bilden und Anweisungen zu den Berichten unabhängig von der Stellungnahme des Wirtschaftsprüfers zu geben, sowie Anweisungen zu denjenigen Fragen zu geben, die der Wirtschaftsprüfer bei der Bildung seiner Stellungnahme zum Jahresabschluss erörtern wird (Petrovic et al. Revizijska regulativa, 2016, S. 15; 44; 203; Petrovic, Medjunarodni standardi revizije, 2010, S. 41; IFAC ISA 700, 2018, S. 2-6).

Der Bestätigungsvermerk zum Jahresabschluss sollte eine klar ausgedrückte Stellungnahme des Wirtschaftsprüfers zum Jahresabschluss enthalten. Die abgegebene Stellungnahme, ob der Jahresabschluss wahrheitsgetreu dargestellt ist, schließt auch die Beurteilung der objektiven Darstellung des Jahresabschlusses ein. Der Bestätigungsvermerk muss den Hinweis enthalten, dass es die Verantwortung des Wirtschaftsprüfers ist, aufgrund der durchgeführten Prüfung eine Stellungnahme zum Jahresabschluss zu erteilen. Eine positive Stellungnahme des Wirtschaftsprüfers wird erteilt, nachdem der Wirtschaftsprüfer festgestellt hat, dass der Jahresabschluss wahrheitsgetreu dargestellt ist (Petrovic et al. Revizijska regulativa, 2016, S. 203-206; IFAC ISA 700, 2018, S. 2-6).

Statements on Auditing Standards 99 (SAS 99) hat neue Anforderungen für Wirtschaftsprüfer im Zusammenhang mit der Aufdeckung von Betrügen eingeführt (AICPA, 2018). Sein Ziel ist der „Wiederaufbau des Vertrauens der Anleger in die Kapitalmärkte und dass der revidierte Jahresabschluss die Finanz- und Ertragslage des Unternehmens präzise widerspiegelt.“ SAS 99 erinnert die Wirtschaftsprüfer daran, dass sie sich nicht zu sehr auf die

Aussagen der Kunden stützen dürfen und dass sie die Wirtschaftsprüfung skeptisch und wie Ermittler angehen sollten. Darüber hinaus wird vom Wirtschaftsprüfer eine Bewertung des Betrugsrisikos verlangt (Pearson & Brickner, 2003).

Eines der berühmtesten Gesetze im amerikanischen Raum wurde am 30. Juli 2002 verabschiedet. Von seiner Reichweite her, ist es eines der umfangreichsten nach dem „Securities Exchange Act of 1934“. Es wurde nach seinen zwei Autoren, Paul Sarbanes und Michael Oxley, benannt- „Sarbanes-Oxley Act“ (SOX). Dieser Act stellt eine Ergänzung der Gesetzgebung aus den Jahren 1933 und 1934 dar und entstand als Konsequenz der großen Unternehmensskandale in den Vereinigten Staaten (z.B. Enron Skandal – vgl. Kapitel 3.1. - oder MCI Worldcom⁶) (Moritz & Gesse, 2005, S. 5). Es sieht die persönliche Verantwortlichkeit der Unternehmensleitungen für den Jahresabschluss ihrer Unternehmen vor. Darüber hinaus unterstützt es die verantwortungsvolle Leitung des Geschäftsbetriebs der Unternehmen und öffnet auf diese Weise die Möglichkeit für die Stärkung des Vertrauens der Kapitaleigentümer und der Gesellschaft, in der das Unternehmen geschäftstätig ist. Das Sarbanes-Oxley Gesetz definiert die Kontrollinstrumente in öffentlichen Unternehmen, in denen die Unternehmensleitung die höchstmögliche Transparenz der Berichterstattung über die Geschäftsergebnisse anstrebt. Laut diesem Gesetz tragen der Geschäftsführer und der Finanzdirektor des Unternehmens die Verantwortung für die Richtigkeit der Angaben in den Unternehmensberichten. Mit dem Ziel der Stärkung der Unabhängigkeit der Wirtschaftsprüfung und der Vermeidung von neuen korporativen Skandalen verbietet der Sarbanes-Oxley Act manche Nicht-Prüfungsleistungen und erfordert gleichzeitig eine Prüferrotation sowie Regelungen zur Sicherstellung der Prüfungsqualität (Menzies, 2004, S. 7; Gros, 2005). Das oberste Ziel dieses Acts ist der „Schutz von Anlegern durch genauere und verlässlichere wertpapierrechtliche Publizitätspflichten (Moritz & Gesse, 2005, S. 6).“

Um jegliche Missverständnisse zu vermeiden, definiert der SOX ganz klar die für die Organisation und die Prüfung relevanten Begriffe (z.B. Prüfung, Prüfungskomitee, Board, Standards, etc.). Die SOX Regelungen umfassen alle börsenorientierten amerikanischen Unternehmen, sowie alle internationalen Unternehmen, die an den amerikanischen Börsen

⁶ MCI Worldcom: Ehemals drittgrößtes Telekommunikationsunternehmen der Welt, dem im Zuge einer Insolvenz 2002 Fehlbuchungen in Höhe von USD elf Mrd. nachgewiesen wurden (Manager Magazin, 2005).

gehandelt werden wollen (Controlling-Portal, 2017). Der SOX-Act ist in 11 Themengebiete unterteilt:

1. Organisation und Aufgaben des Aufsichtsgremiums
2. Unabhängigkeit der Wirtschaftsprüfer
3. Verantwortlichkeiten der Unternehmen
4. Veröffentlichungspflichten für Finanzinformationen
5. Verhinderung von Interessenkonflikten bei Finanzanalysten
6. Befugnisse der Securities and Exchange Commission (SEC)
7. Studien und Berichte
8. Informanten Schutz und Aufbewahrungspflichten
9. Strafrechtliche Bestimmungen
10. Steuererklärung
11. Verantwortung der Geschäftsführung (Public Law 107-204-JULY 30,2002; 116 STAT. 745, 2002).

Das Gegenstück des amerikanischen SOX-Gesetzes in Europa bildet die auf Vorschlag der Europäischen Kommission vorgestellte "Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates". Die Richtlinie bestimmt, wie Abschlussprüfungen von den Jahresabschlüssen und den konsolidierten Abschlüssen durchgeführt werden sollen. Die Motivation für die Erstellung dieser Richtlinie liegt in der fehlenden Harmonisierung der Regelungen für eine Abschlussprüfung. In dem Gesetzestext wird der Zweck der Richtlinie ausführlich angegeben: „Zweck der vorliegenden Richtlinie ist eine Harmonisierung der Anforderungen an die Abschlussprüfung auf hohem Niveau, wenn auch eine vollständige Harmonisierung nicht angestrebt wird. Der Mitgliedstaat, der eine Abschlussprüfung vorschreibt, kann strengere Anforderungen aufstellen, sofern in dieser Richtlinie nichts Anderes vorgesehen ist (Amtsblatt der Europäischen Union , 2006).“ Diese Richtlinie umfasst zudem die Mindestqualitätsanforderungen für die Abschlussprüfung innerhalb der Europäischen Union. Wird diese Richtlinie mit dem Sarbanes-Oxley Act verglichen, kann eine inhaltliche Ähnlichkeit und eine Übereinstimmung der Ziele festgestellt werden.

Die neuen Gesetze, die die ISA Standards ablösen sollen sind die International Financial Reporting Standards (IFRS) in Europa und die werden langsam auch in Japan, China und Indien umgesetzt. In den Vereinigten Staaten wird IFRS nicht umgesetzt, sondern es gilt weiterhin nur das Generally Accepted Accounting Principles Gesetz (US GAAP) (Peavler, 2017). Laut dem Absatz 7 der EU Richtlinie EG Nr. 1606/2002 des Europäischen Parlaments und des Rates „werden die „International Accounting Standards" (IAS) vom „International Accounting Standards Committee" (IASC) entwickelt, deren Zweck darin besteht, ein einheitliches Regelwerk weltweiter Rechnungslegungsstandards aufzubauen. Im Anschluss an die Umstrukturierung des IASC hat das neue Board als eine seiner ersten Entscheidungen am 1. April 2001 das IASC in „International Accounting Standards Board" (IASB) und die IAS mit Blick auf künftige internationale Rechnungslegungsstandards in „International Financial Reporting Standards" (IFRS) umbenannt. Die Anwendung dieser Standards sollte, so weit wie irgend möglich und sofern sie einen hohen Grad an Transparenz und Vergleichbarkeit der Rechnungslegung in der Gemeinschaft gewährleisten, für alle kapitalmarktorientierten Gesellschaften in der Gemeinschaft zur Pflicht gemacht werden (Verordnung (EG) Nr. 1606/2002 des Europäischen Parlaments und des Rates vom 19. Juli 2002 betreffend die Anwendung internationaler Rechnungslegungsstandards, 2002)." Trotz dieses Vereinheitlichungsversuchs, haben österreichische Unternehmen, die vom EG Nr. 1606/2002 nicht betroffen sind, noch immer das Recht, ihren Jahresabschluss wie im Unternehmensgesetzbuch (UGB) beschrieben, zu machen (UGB, 2017).

2.3. Ausgewählte EU-Statistik

Dieses Kapitel liefert eine kurze Übersicht zu der Anzahl der in der EU eingereichten Anmeldungen von verdächtigen Aktivitäten und Transaktionen. Bevor jedoch eine Analyse der abgebildeten Grafik erfolgt, soll angemerkt werden, dass die nationalen Gesetzgebungen der EU-Mitgliedstaaten in ihren Begriffen für allgemein verdächtige monetäre Aktivitäten nicht übereinstimmen. In Hinsicht auf das Angeführte gibt es in den nationalen Gesetzgebungen drei Bezeichnungen für verdächtige monetäre Aktivitäten: SAR – Bericht über verdächtige Aktivitäten (engl. Suspicious Activity Reports); STR – Bericht über verdächtige Transaktionen (engl. Suspicious Transactions Reports); und UTR – Bericht über ungewöhnliche Transaktionen (engl. Unusual Transaction Reports). Ein Bericht über verdächtige Aktivitäten ist ein Informationsblatt, das Strafverfolgungsbehörden darauf hinweist, dass bestimmte Kunden

oder deren Aktivitäten in irgendeiner Weise verdächtig sind und auf Geldwäsche oder Terrorismusfinanzierung hindeuten könnten (National Crime Agency, 2018, S. 2). Alle Aktivitäten, die untypisch oder illegal erscheinen, bei denen kein wirtschaftlicher Zweck einsehbar ist und die nicht zum Kundenprofil passen, sind durchgehend an die zuständigen Behörden zu melden, weil sie vermuten lassen, dass der Kunde möglicherweise in Geldwäsche- oder Terrorismusfinanzierungstätigkeiten involviert ist. Das offizielle Dokument, in dem die Behörden davon verständigt werden, ist der Bericht über verdächtigen Transaktionen (Anti Money Laundering & Counter Financing of Terrorism, 2018). Die ungewöhnlichen Transaktionen umfassen die Transaktionen, wenn der Kunde sehr hohe Beträge in Bar von seinem Konto abzieht oder auf sein Konto einzahlt. Solche Transaktionen sind mit dem Bericht über ungewöhnliche Transaktionen zu erfassen (Business Government Netherlands, 2018).

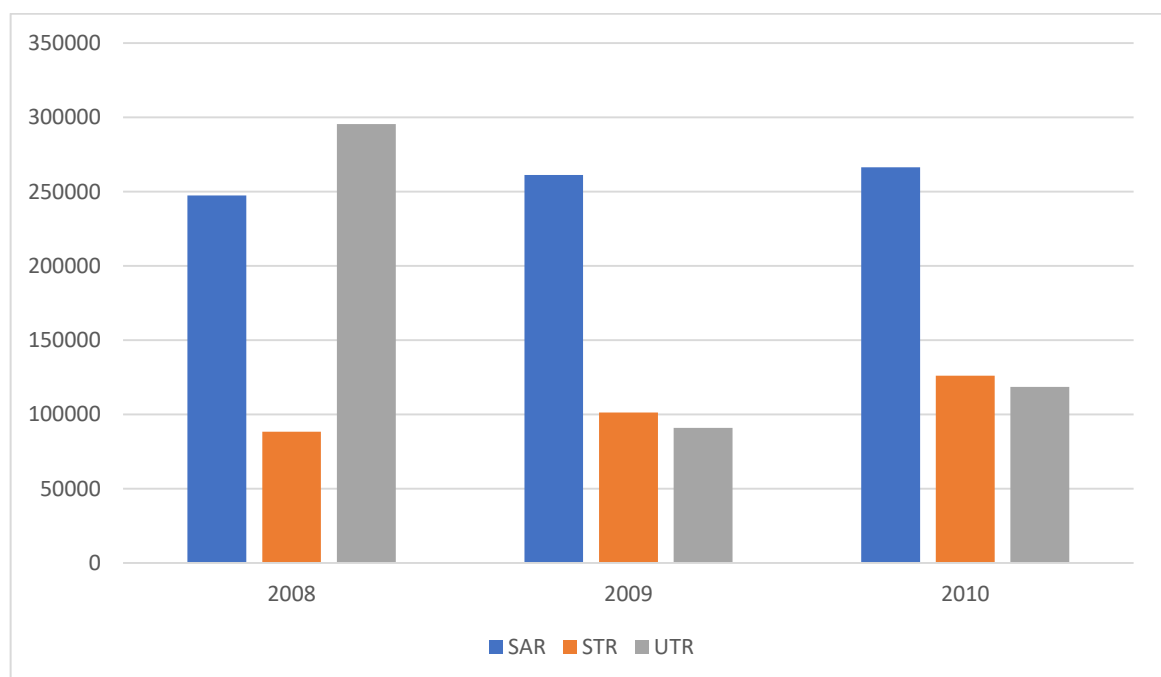


Abbildung 1- SAR, STR, UTR

(Commission, 2013, S. 25)

Die obige Abbildung verdeutlicht, dass die Anzahl der eingereichten Anmeldungen von verdächtigen Aktivitäten einen ersichtlichen Wachstumstrend verzeichnet, der im Jahr 2010 den Wert von 125.000 Anmeldungen überschritten hat. Die Anzahl der eingereichten Anmeldungen von ungewöhnlichen Transaktionen verzeichnete im Jahr 2009 einen starken

Rückgang. Allerdings kommt es zum leichten Anstieg der Anzahl der Berichte über ungewöhnliche Transaktionen, die erneut den Wert von 100.000 überschritten haben. Die Anzahl der Berichte über verdächtige Transaktionen hat einen sehr leichten Wachstumstrend im Beobachtungszeitraum verzeichnet. Die Anzahl der Berichte über verdächtige Transaktionen lag im analysierten Zeitraum bei ca. 260.000.

Die folgende Grafik zeigt den Anteil der EU-Berichte über verdächtige Aktivitäten, die von Kreditinstituten stammen.

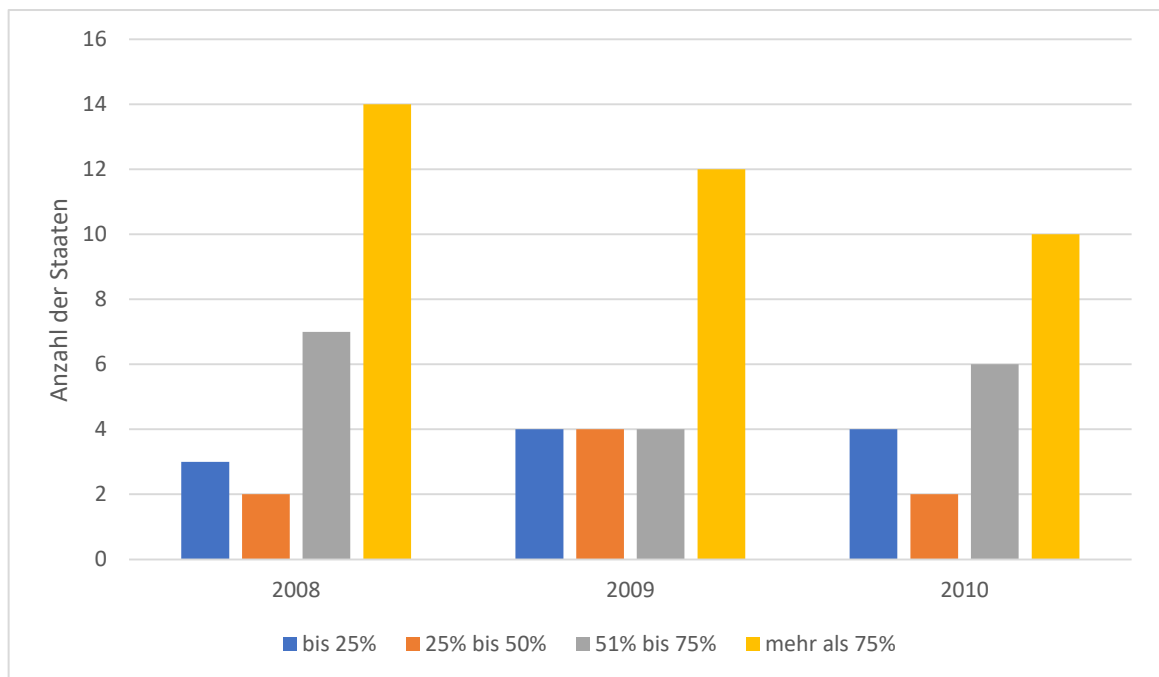


Abbildung 2- EU Berichte über verdächtige Aktivitäten

(Commission, 2013, S. 49)

Kreditinstitute sind in der Branche als Verursacher von verdächtigen Transaktionen (STRs) bekannt. Die Graphik zeigt den Prozentsatz aller verdächtigen Aktivitäten und Transaktionen, sowie den Anteil ungewöhnlicher Transaktionen, die aus den Kreditinstituten stammen. Aufgrund der dargestellten Daten in der obigen Grafik wird die Schlussfolgerung gezogen, dass sich in den meisten EU-Staaten die Anzahl der Berichte über verdächtige Aktivitäten in mehr als 75% der Fälle auf die Einreichung der Berichte von Kreditinstituten zurückführen lässt.

Die großen Wirtschaftsprüfungsgesellschaften haben sich mit der Frage der Wirtschaftskriminalität immer wieder auseinandergesetzt und einige Studien dazu erstellt. Werden unter Wirtschaftskriminalität alle Delikte verstanden, die sich auf Handelsrecht,

Rechnungslegungsvorschriften, Steuerrecht, Wertpapier-, Banken- und Versicherungsgesetze, Arbeitsrecht, Gesetz gegen den unlauteren Wettbewerb beziehen, dann ist eine genaue Abschätzung der Anzahl der Fälle sehr schwierig. Die schwere Ermittlung ist durch die Unmöglichkeit, die Wirtschaftskriminalität genau zu definieren, verursacht. Es kann mit einer Dunkelziffer von 80% bis 90% gerechnet werden. Die in Deutschland vom Bundeskriminalamt (BKA) registrierten Schäden bewegen sich jährlich zwischen EUR 3,5 Mrd. und EUR 6,9 Mrd. Die Wirtschaftsprüfungsunternehmen KPMG und PwC kommen jährlich gesehen auf ein ähnliches Ergebnis. Es wird aber davon ausgegangen, dass viele "Top-Management" Schäden erst gar nicht entdeckt werden. Gleichzeitig wird eine gewisse Anzahl an entdeckten Delikten nicht veröffentlicht, damit der Ruf der betroffenen Unternehmen nicht beeinträchtigt wird. Deshalb wird geschätzt, dass sich die tatsächlichen Schäden zwischen EUR 20 Mrd. und EUR 80 Mrd. im Jahr bewegen (Melcher, 2009, S. 3-8).

Für die USA ermittelt die ACFE die Schadenshöhe. Laut amerikanischen Statistiken verursachen Untreue und Diebstähle ca. USD 150 Tsd. im Jahr. Sogar dreizehn Mal höhere Schäden werden durch die Manipulation der Rechnungslegung verursacht. Das Committee of Sponsoring Organizations of the Treadway Commission (COSO) hat bestätigt, dass 51% der untersuchten amerikanischen Firmen, die Rechnungslegungssysteme manipulieren, insolvent gehen oder den Eigentümer wechseln müssen (Melcher, 2009, S. 3-8).

Weiterst zeigen Studien, dass viele Wirtschaftsbetrüge durch die interne Revision oder reinen Zufall entdeckt werden. Die einzigen Methoden, die erfolgreicher als der Zufall sind, sind die Management Reviews und die Hinweisgebersysteme, die 46% der Betrüge auffinden. Insgesamt werden um 90% aller Betrugsereignisse selbst durch das Unternehmen entdeckt. Die restlichen 10% werden dank der Kooperation mit externen Prüfern identifiziert. Die folgende Grafik zeigt die typischsten Aufdeckungsursachen und die Häufigkeit in der sie auftreten.

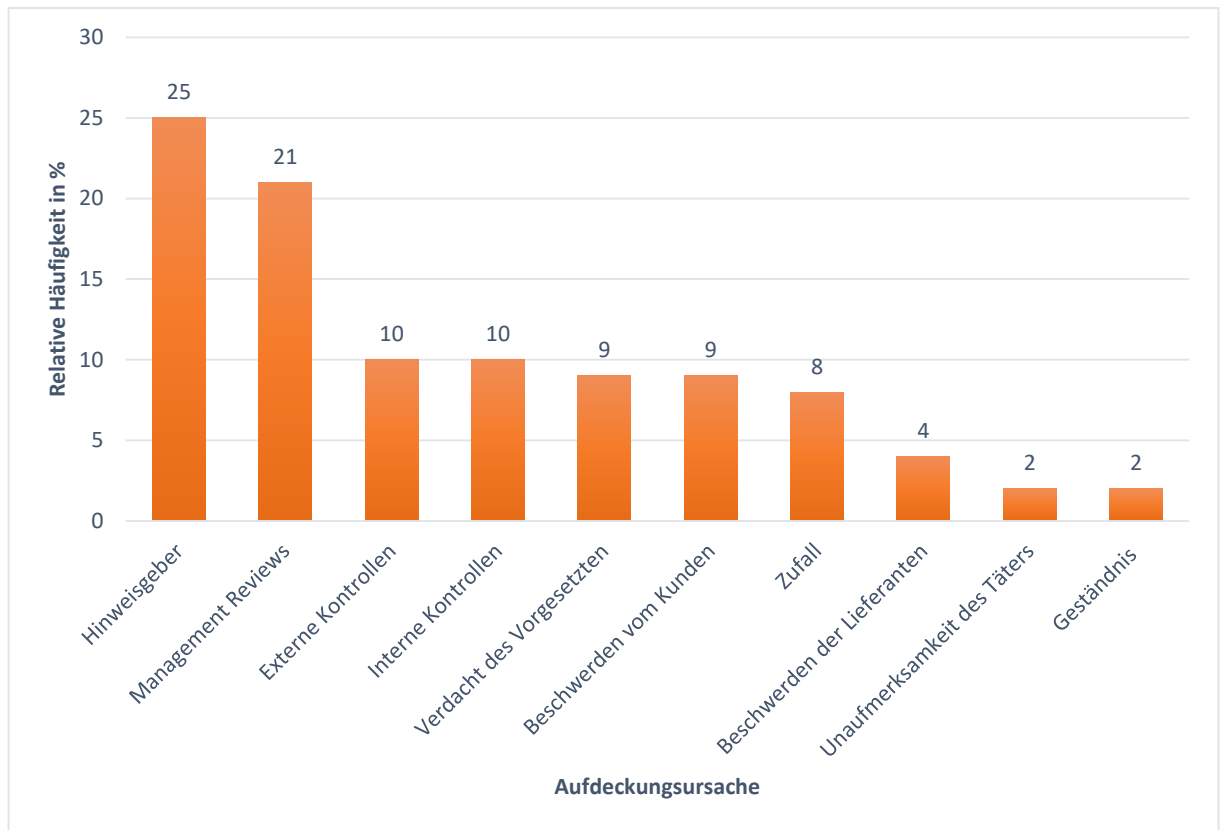


Abbildung 3- Aufdeckungsursachen

(Melcher, 2009, S. 10)

3. Kampf gegen Betrug

3.1. Enron-Skandal

Beim Thema Rechnungsbetrug, kommt vielen als erster Gedanke das Unternehmen „Enron“ in den Sinn. Dieses Unternehmen, bekannt für seine innovativen Ideen und signifikanten Gewinne, weckt aber auch negative Erinnerungen in der Öffentlichkeit: die größten Rechnungswesen Malversationen und die Gier seines Managements. Im Jänner 2002 erscheinen in allen berühmten Zeitungen weltweit Schlagzeilen: „Enrons Collapse: der Überblick; Arthur Andersen entlässt Exekutive“ (The New York Times), „Enrons Sturz zeigt das Genie des Kapitalismus“ (BBC News), „Enron-Skandal: Das große Schreddern“ (SPIEGEL Online), u. ä. Diese Schlagzeilen weisen auf den Zusammenhang zwischen dem Wirtschaftssystem und den Malversationen hin. Im folgenden Abschnitt dieser Arbeit wird ein historischer Überblick über die Firma "Enron" gegeben, mit der detaillierten Beschreibung ihrer Betrüge und den dadurch entstandenen Konsequenzen. Des Weiteren werden Maßnahmen aufgezeigt, wie sich solche Ereignisse verhindern lassen können.

3.1.1. Unternehmensgeschichte

Der Zusammenbruch des amerikanischen Unternehmens Enron Corporation (Enron) ist durch einen Kostenrechnungsskandal ins negative Licht der Öffentlichkeit gerückt worden und gilt schon seit Jahren als die „Mutter aller Skandale“. Das Unternehmen wurde mehrmals zur innovativsten Firma Amerikas erklärt und stand auf der Liste der „Most Admired Companies“. Der Energiekonzern Enron wurde 1985 durch die Fusion der zwei Unternehmen - Houston Natural Gas und Internorth – gegründet. Die Haupttätigkeitsgebiete Enron's waren das Absichern durch Wetterrisiken und der Handel mit Energien und Rohstoffen (Möller & Sigillo, Der Enron-Andersen-Skandal und dessen Einfluss auf das Reputationskapital der Institution Wirtschaftsprüfung, 2010, S. 5).

Schon kurz nach der Gründung ist Enron in große Schulden geraten. In Folge des Regulierungsmangels hat Enron zusätzlich das exklusive Recht auf eigene Pipelines verloren. Das Unternehmen musste dringend eine Lösung finden um sich zu retten und wieder profitabel arbeiten zu können. Mit Unterstützung der bekannten Beratungsfirma McKinsey & Co, hat Enron versucht, eine neue Strategie zu entwickeln. Der damalige Enron CEO, Kenneth Lay, war begeistert von den Ideen und dem Enthusiasmus des jungen Beraters Jeffrey Skilling, den er bald als festen Angestellten übernahm (The Guardian, 2002). Skilling hat sich die sogenannte „Erdgas-Bank“ ausgedacht. Die Idee dahinter war, dass Enron als Zwischenhändler auf dem Erdgasmarkt agiert, in dem es Erdgas von Lieferanten kauft und an die Konsumenten weiterverkauft wird. Enron hat die Macht übernommen und ein Monopol in diesem Markt erschaffen. Es wurde sogar eine neue Abteilung gegründet- Enron Finance Corp- die ausschließlich auf die Derivatverträge fokussiert war (Thomas, 2002).

Die Erfolge veranlassten viele Veränderungen und es wurde die gesamte Unternehmenskultur schnell angepasst: Die Mitarbeiter wurden ordentlich für die Unternehmenserfolge belohnt, genossen Unternehmensvorteile in hohem Maß, aber die Fluktuationsrate stieg massiv, denn nur die Stärksten konnten überleben - alles war ausschließlich darauf ausgelegt soviel Geld wie möglich zu generieren. Dabei wurden die langfristigen Ziele außer Sicht gelassen. Motivation und Arbeitsfreude wurden langsam zu Stress (Thomas, 2002; Pratap, 2016).

Während sich die Situation im Unternehmen langsam in eine negative Richtung entwickelte, erlebte die Wirtschaft der Vereinigten Staaten eine Hochkonjunktur.

Investitionsmöglichkeiten waren überall vorhanden. Die Wall Street meldete ein signifikantes Wachstum. Skilling und Lay erweiterten das Enron Hauptgeschäft um Strom. Sie knüpften wertvolle Kontakte zur Politik und schafften es, den Strommarkt dereguliert zu halten. Mit der erfolgreichen Akquise von "Portland General Electric Corp" hat Enron die absolute Macht im amerikanischen Strommarkt übernommen. Die Profite sind um USD 5 Mrd. gestiegen und die Anzahl der Mitarbeiter stieg von 200 auf 2000. In der gleichen Art und Weise hat Enron seine Geschäfte auf Kohle, Papier, Eisen, Wasser und Wetter ausgedehnt. Im Jahr 1999 kreierte das Unternehmen Enron Online (EOL). EOL war eine internetbasierte Plattform für Handel mit Rohstoffen. Unabhängig vom Handelsgegenstand war Enron als eine Partei beim Ablauf des Handels involviert. Enrons Erfahrung und seine lange Tradition haben bei Anlegern einen guten und sicheren Eindruck hinterlassen. Die Anleger waren dazu bereit, große Summen über die Plattform zu handeln. Mit der weiteren Technologieentwicklung ist Enrons online Konzept in die Höhe gestiegen. Im Jahr 2000 hat Enron den Rekordaktienpreis von USD 90,65 erreicht (Thomas, 2002; Myatt, 2013).

3.1.2. Betrügerisches Geschäftsmodell

Die amerikanischen Buchhaltungsgesetze haben die Unternehmen verpflichtet, für alle ausstehenden Verträge, sowohl für die Forderungen als auch für die Verbindlichkeiten, am Ende des jeweiligen Quartals, auch die Wertänderungen zu berücksichtigen; d.h. sie müssen diese Produkte zu einem fairen Marktwert bewerten bzw. die nicht realisierten Gewinne und Verluste ausweisen. Für jene Unternehmen, die mit Erdöl handeln, sind diese Vorschriften aber unmöglich umzusetzen, da die langfristige Preisentwicklung für Erdöl nicht im Voraus bekannt ist, und jegliche Preisabschätzungen nicht möglich sind. Somit können Öl-Unternehmen, wie auch Enron, selbstständig Prognosen erstellen und die Buchhaltung auf Basis eigener Vorstellungen durchführen. Es hat sich im Nachhinein herausgestellt, dass Enron mindestens 30% höhere Gewinne meldete hat, als realistisch gesehen gemacht wurden (Thomas, 2002).

Die „selbstständige Anpassung“ der Bilanz wurde auch weiterhin ausgenutzt: Enron hat die harten Aktivposten in seiner Bilanz künstlich reduziert und die Gewinne aus Finanzgeschäften durch die nicht realisierten Gewinne erhöht. Dadurch wurde die Vermögensrendite ebenfalls künstlich erhöht und die Schuldenquote gleichzeitig reduziert. Die attraktiven Schuldenquoten weckten das Vertrauen von fremden Investoren und das

Unternehmen hatte sich in den Augen der Öffentlichkeit gut positioniert. Die Höhe des Betrugs wurde mit USD 0.7 Mrd. berechnet (Thomas, 2002).

Alle seinen künstlichen Wertänderungen hat Enron in den eigenen Finanzberichten nie veröffentlicht. Es wurde alles an die Konten von Enron's Zweckgesellschaften, bekannt unter dem englischen Namen „special-purpose entities“ oder SPEs, gebucht. Enrons externe Partner wurden gleichzeitig auch an diese Zweckgesellschaften gebunden. Die, durch Enron gegründeten Zweckgesellschaften, wurden nie als Enrons Tochtergesellschaften aufgelistet. Dank des amerikanischen „Financial Standards Accounting Board“ (FASB) und dessen Regulierung, die besagt, dass wenn nur 3% der Zweckgesellschaft dem anderen Konzern nicht gehören (in diesem Fall Enron), die Zweckgesellschaft nicht als Tochterunternehmen betrachtet werden soll, sondern als unabhängige Einheit. Das hat Enron ermöglicht, dass alles, was in den Bilanzen seiner Zweckgesellschaften auftaucht, nie in der eigenen Bilanz konsolidiert werden muss. Dadurch buchte Enron nur die Gewinne und alle Schulden wurden an die Zweckgesellschaften umgebucht. Dann verlangte Enron von seinen externen Partnern finanzielle Unterstützung für die hochverschuldeten Zweckgesellschaften (in diesem Fall ist die Bank der externe Partner), mit dem Versprechen, im Notfall selbst für diese Kredite zu garantieren. Jede Bank war bereit, einem großen und unverschuldeten Unternehmen wie Enron, einen Kredit zu gewährleisten. Sobald das Geld bei der Zweckgesellschaft lag, hat sie es an Enron weitergegeben. So kam Enron laufend zu neuem Geld, und seine Zweckgesellschaften verschuldeten sich immer stärker (Thomas, 2002; Fischer, 2003).

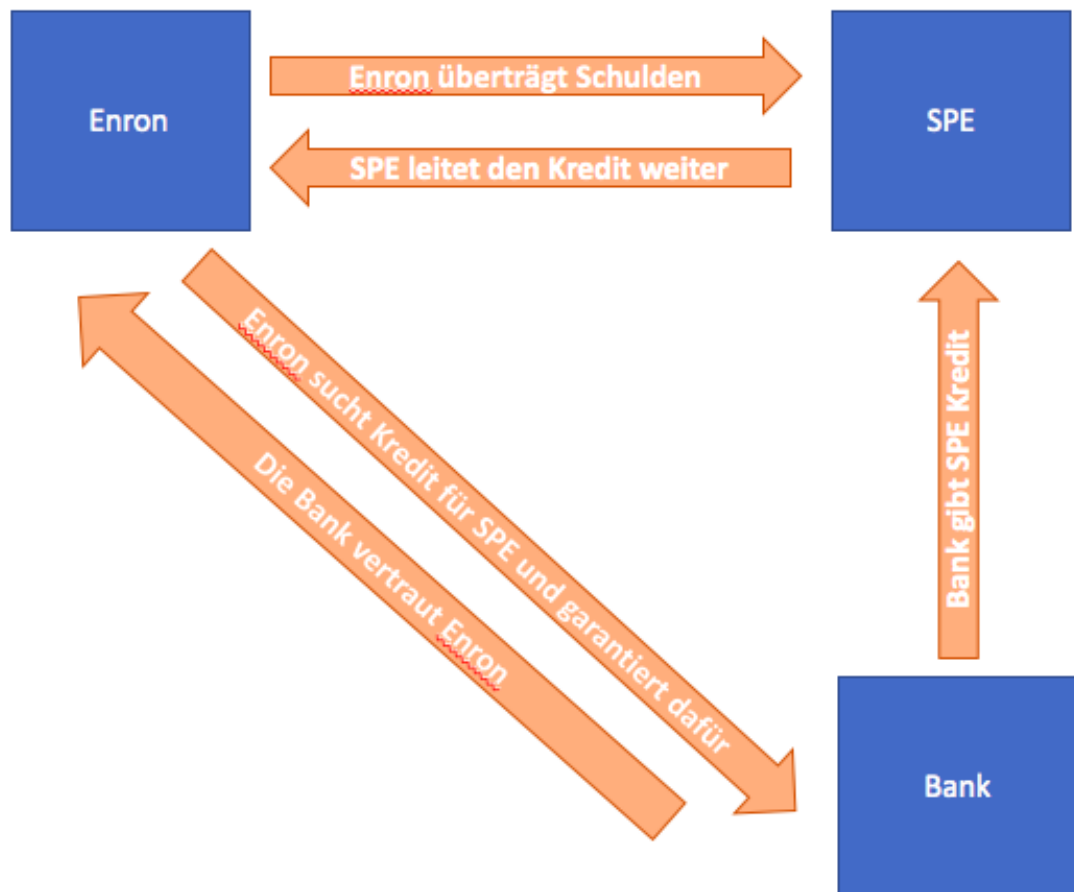


Abbildung 4- Enron SPE

Ein ähnliches Konzept wendete Enron auch mit Partnergesellschaften an, nur dass diese in diesem Fall die Zweckgesellschaften gegründet haben, die Enron wiederum für die eigenen Geldtransaktionen genutzt hat. Im Gegensatz zu dem vorherigen Model, wurde kein Kredit von der Bank verlangt, sondern die Zweckgesellschaften bezahlten Enron Geld ein, und zwar jedes Mal, wenn Enrons Finanzen nicht sonderlich positiv waren. Praktisch hat sich Enron sein eigenes Geld über diese Zweckgesellschaften wieder als Gewinn einbezahlt. Als Gegenleistung für die Gründung der Zweckgesellschaften hat Enron seinen externen Partnern seine Aktien gegeben. Die nachfolgende Abbildung verdeutlicht diesen Vorgang (Prashant, 2015).

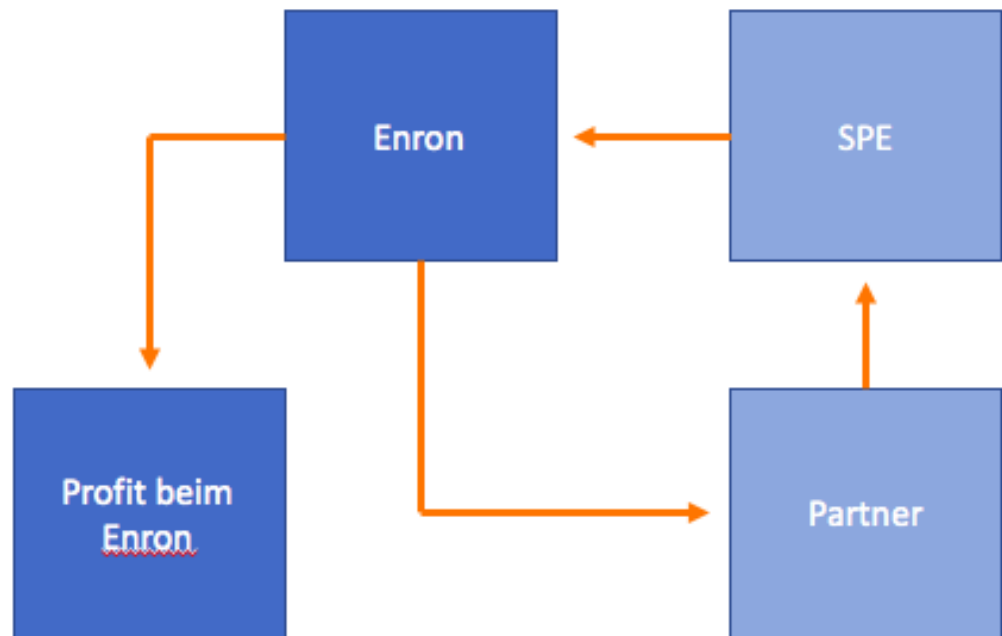


Abbildung 5- Enron SPE.2

(Prashant, 2015)

Enron spezialisierte sich mit der Zeit immer mehr in diesem Geschäft, und nutzte die Zweckgesellschaften für alle Geschäfte, die nicht profitabel liefen (bspw. Energieanlagen in Übersee, die Aktien die an die Öffentlichkeit abgegeben wurden, etc.). Im Endeffekt schienen alle Geschäfte, die von Enron getätigt wurden, komplett ohne Schulden zu sein. Um alle dafür benötigten Partnerschaften aktiv zu halten, versprach Enron immer wieder, weitere Unternehmensaktien auszugeben. Die Anzahl der Zweckgesellschaftstätigkeiten wurde mit der Zeit immer größer, die Versprechen immer umfangreicher und der Verschuldungsgrad höher. Da nur schlechte Geschäfte ausgelagert wurden, sanken auch die Aktiva der Zweckgesellschaften. Das setzte Enron unter Druck, immer mehr Aktien auszugeben. Aus diesen Geschäften wurde ein Managergehalt von USD 30 Mio. herausgezogen. Neben den berühmtesten Zweckgesellschaften- „LJM Cayman LP“ und „LJM2 Co-Investment LP“- wurde das „verdiente“ Geld in neue Gesellschaften investiert, in sogenannte „Raptor vehicles“, die eine Fehlinvestition verschleiern sollten. Um die „Raptor vehicles“ zu finanzieren, benötigte Enron einen Wechsel, für den es frische Aktien mit einem Wert von USD 1.2 Mil. ausgegeben hat. Als Konsequenz hätte eigentlich die Eigenkapitalquote sinken müssen, aber Enron gelang es, diese künstlich zu erhöhen. Dadurch wurden die Buchhaltungsgrundsätze stark verletzt.

Der gesamte Plan mit der „Raptor“ Finanzierung lief schief und die Konsolidierung aller Konten schlug fehl (Holtzman et al. 2003).

Das Management Board ließ Enron im Stich, indem die Mitglieder ihre eigenen Aktien verkauften. Dieses Verhalten wurde im Nachhinein als Insiderhandel beurteilt. In Folge dessen, trat Skilling von seinem Posten zurück. Der Aktienpreis fiel schnell auf USD 40 pro Stück und ist im Folgenden weiter gesunken. Die ersten Bilanzuntersuchungen fanden statt. Im Oktober 2000 musste Enron einen Verlust veröffentlichen. Die „Raptor“ Verträge wurden storniert, weil sie sonst Kosten in Höhe von USD 58 Mio. in Form von Enron Aktien verursachen würden. Die amerikanische Börsenaufsicht (United States Securities and Exchange Commission - SEC) hat sich in Folge dessen zum ersten Mal für den Enron Fall interessiert (F.A.Z., 2008). Die SEC hat weitere Prüfungen gestartet. Die Unternehmensschulden sind von allen Seiten aufgetaucht und im November 2000 wurde Enron als „junk“ (Ramsch) Unternehmen bewertet, mit einem Aktienwert von USD 0,26. Am 2. Dezember 2000 beantragte Enron schließlich den Gläubigerschutz "nach Chapter 11" (Thomas, 2002).

„Chapter 11“ beschreibt das Insolvenzrecht in den USA. Unternehmen mit Problemen und einer hohen Verschuldung beantragen Insolvenz, um sich im darauffolgenden Prozess wieder zu sanieren. Dabei wird ein Großteil des Fokus auf die Fortführung des Unternehmensgeschäfts gelegt, sowie darauf durch eine Reorganisation nach dem Abschluss des Verfahrens erneut erfolgreich Geschäfte betreiben zu können. Der Reorganisationsplan beinhaltet Maßnahmen für die Entschuldung und die zukünftige Ausrichtung des Unternehmens. Das Tagesgeschäft läuft mehr oder weniger normal weiter, wobei gewisse Aktivitäten (z.B. Zahlung von Forderungen) eine Genehmigung seitens des Gerichts benötigen. Eine wichtige Rolle für Chapter 11 spielt das Kreditorenkomitee (creditors' committee). Dieses überwacht die Aktivitäten des Unternehmensmanagements und ist ebenfalls am Reorganisationsplan beteiligt. Mit Genehmigung des Gerichts dürfen hierfür auch Anwälte oder andere Experten zu Rate gezogen werden. Die Verwaltung der Insolvenzmasse erfolgt in der Regel durch das beantragende Unternehmen bzw. dessen Management selbst. Nur in seltensten Fällen wird ein Treuhändler dafür eingesetzt. Kreditoren müssen dem Plan mit einer Zweidrittelmehrheit zustimmen, damit das Gericht diesen final genehmigen kann. Es ist hierbei auch möglich einen Plan für die Liquidierung des Unternehmens vorzulegen. Es können

mehre Pläne zur Abstimmung vorlegt werden. Hat sich die Lage des Unternehmens verbessert, kann Chapter 11 beendet werden (United States Courts, 2018).

Im Unterschied zu Österreich (Insolvenzordnung – IO) oder Deutschland (Insolvenzordnung – InsO) bleibt hierbei in der Regel das Management bzw. das Unternehmen selbst für das Tagesgeschäft verantwortlich, wobei gewisse Transaktionen durch ein Gericht genehmigt werden müssen. In Österreich oder Deutschland wird häufig ein Insolvenzverwalter eingesetzt. Der Insolvenzverwalter übernimmt die Verantwortung für das ganze Unternehmen bzw. steigt ins Unternehmen als Führungskraft ein. In Österreich ist eine hohe Überschuldung mit negativer Fortbestehungsprognose schon ein ausreichender Grund für das Insolvenzverfahren. Zahlungsunfähigkeit des betroffenen Unternehmens ist natürlich der zweite Grund für die Einleitung eines Insolvenzprozesses (Rechtsanwalt Dr. Markus Kaltseis, 2016).

3.1.3. Gesetzgebung

Die wichtigsten Enron Manager wurden nach dem Zusammenbruch des Unternehmens verhaftet und verurteilt. Ihr Handeln hat alle Compliance- und Risikomanagementgesetze aus den 90er Jahren verletzt. Diese wurden im Sarbanes Oxley Act aufgefrischt und verstärkt. Im europäischen Raum hätte ihr Handeln gegen das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) von 1998 verstoßen, welches „fehlendem Risikobewusstsein und unzureichenden Kontroll- und Informationsmechanismen unternehmensseitig entgegenwirken soll (Sure, 2016, S. 125).“ Weiterst wurde das Wertpapiergesetz (USA Securities Act) verletzt. Im Grunde genommen handelt es sich dabei um ein relativ altes Gesetz, das seit 1933 ohne Änderungen in Kraft trat. Die Börsenaufsicht in den Vereinigten Staaten wurde 1934 gegründet. Fest zu halten ist hierbei, dass nicht alle amerikanischen Skandale diese Gesetze verletzten und es dadurch auch keine Veranlassungen gab, die Gesetzgebung in den Vereinigten Staaten zu überprüfen und zu verschärfen. Enron war das erste Unternehmen, das diese Gesetze brach (SPIEGEL Online, 2002).

Skilling wurde zu USD 45 Mio. Schadenersatz und 24 Jahren Gefängnis verurteilt. Er wurde für Verschwörung, Betrug, verfälschte Bilanzdarstellung und das Belügen der Öffentlichkeit verurteilt (McNulty, 2006). Ihm ist es nicht gelungen, das Gericht davon zu überzeugen, nichts von den Zweckunternehmen gewusst zu haben. "Er hat das Geschäft eines

der größten Unternehmen der Welt systematisch und umfangreich korrumpiert", sagte der stellvertretende Justizminister Larry Thompson in Washington. "Er hat Geld gestohlen, um sich selbst, seine Familie und seine Freunde zu bereichern (Die Welt, 2002)."

Zu der Zeit als Enron der weltweit größte Energiehändler und das siebtgrößte Unternehmen Amerikas war, brach es zusammen. In den Jahren vor seinem Zusammenbruch, hat Enron es geschafft, seine Erträge um USD 600 Mio. künstlich zu erhöhen, ohne dass sein Wirtschaftsprüfer Arthur Andersen diese Ereignisse gemeldet hat. Es wurde eine starke Abhängigkeit und Zusammenarbeit beider Unternehmen vermutet. Dieses Ereignis hat den Glauben an die Fähigkeiten des Managements und der Wirtschaftsprüfung stark beeinträchtigt.

Der bereits erwähnte Sarbanes Oxley Act of 2002 ist als Antwort auf den Enron Skandal in Kraft getreten. Es wurden die internen Kontrollen der Großunternehmen nochmals überprüft. Auf einmal wurde der internen Prüfung und dem Berichtswesen eine wesentlich wichtigere Rolle als je zuvor zugeschrieben. Die Unsicherheit und das verlorene Vertrauen haben auch die europäischen Länder beeinflusst. In der Schweiz wurde unmittelbar ein neues Gesetz veröffentlicht – das Revisionsgesetz (RAG), das ähnlich wie der Sarbanes Oxley Act aufgebaut worden ist. Dies war gleichzeitig das erste Mal, dass der Begriff eines internen Kontrollsystems in Europa verwendet wurde (Möller & Sigillo, Der Enron-Andersen-Skandal und dessen Einfluss auf das Reputationskapital der Institution Wirtschaftsprüfung, 2010, S. 1-2). Dieser Fall hat gezeigt, wie wichtig die Wirtschaftsprüfung, bzw. die forensische Wirtschaftsprüfung sind, und welche Konsequenzen entstehen können, wenn es zu einem Scheitern dieser kommt. Der Enron Fall ist der größte „weißer Kragen“ Skandal aller Zeiten (Finance laws, 2017). Die heutigen internen Kontrollen und das Risikomanagement wären in der Lage gewesen, das Unternehmen damals besser vor allen Manipulationen zu schützen. Besonders die unabhängige forensische Wirtschaftsprüfung hätte die Malversationen rechtzeitig entdecken und den Betrug verhindern können.

3.2. Kampf gegen Betrug

Es gibt mehrere Möglichkeiten, wie Unternehmen das Betrugsrisiko minimieren können. Die Basis sollte bereits im Inneren des Unternehmens entwickelt werden: Es soll eine Betrugskampfkultur aufgebaut und gepflegt werden. Zudem sollten verschiedene Trainings für Mitarbeiter zur Verfügung gestellt werden, sodass sie selber die Gefahr rechtzeitig

erkennen können. Es muss ein hohes Augenmerk in der Auswahl von Partnern und Lieferanten gelegt werden (Bailey, 2015). Eine weitere Maßnahme bezieht sich auf die internen Kontrollsysteme (IKS). Das Ziel ist „die Bewahrung des Vermögens des Unternehmens, Gewährleistung der Zuverlässigkeit des Rechnungswesens und der Einhaltung der Geschäftspolitik (Klokar, 2017, S. 1)“. IKS basieren auf Überwachungsmaßnahmen, Richtlinien und der internen Revision. Somit wäre die interne Revision eine Erweiterung des IKS, die seine Effizienz kontrolliert (Klokar, 2017, S. 1). Weitere Maßnahmen, die die interne Kontrolle ergänzen, sind das Risikomanagement und die Compliance. Große Unternehmen im Sinne von §221 Abs. 1 UGB sind gesetzlich verpflichtet (§268 UGB), eine externe Wirtschaftsprüfung zu bestellen, bevor sie ihren Jahresabschluss machen (§ 268 UGB, 2017). Somit kann die externe Wirtschaftsprüfung als eine weitere Methode zur eventuellen Betrugsentdeckung dienen. Wirtschaftsprüfer können Fehler im Jahresabschluss nachvollziehen und falls ein konkreter Betrugsverdacht vorliegt und somit eine tiefgreifende Prüfung notwendig wird, die forensischen Rechnungsprüfer hinzuziehen, die auf die Betrugsentdeckung spezialisiert sind (Gray, 2008, S. 117).

Eine Wirtschaftsprüfung ist definiert als ein systematischer Überblick über die Geschäftsbücher und die Rechnungslegungs-Berichte, die von Wirtschaftsprüfern und Experten mit dem Ziel durchgeführt wird, eine kompetente, fachliche und unabhängige Stellungnahme über deren Ordnungsmäßigkeit, Richtigkeit und Genauigkeit abzugeben. Wenn gesetzlich aufgefördert, sind die verwendeten Formulierungen für die Erteilung der Stellungnahme des Wirtschaftsprüfers „gibt ein wahrheitsgetreues und objektives Bild“ (engl. gives true and fair view) oder „stellt in allen bedeutenden Aspekten ordnungsmäßig dar“ (engl. present fairly, in all material respects) (IFAC, 2009, S. 106).

Eine allgemein anerkannte Definition der Wirtschaftsprüfung hat der Ausschuss für grundlegende Prüfungskonzepte der Amerikanischen Vereinigung der Buchführer gegeben, wonach die Wirtschaftsprüfung ein „systematisches Verfahren der objektiven Erfassung und Beurteilung von Nachweisen im Zusammenhang mit den Aussagen zu Geschäftsaktivitäten und Ereignissen ist, um die Stufe der Kompatibilität zwischen den Aussagen und den festgelegten Kriterien zu bestimmen, sowie die Ergebnisse den interessierten Nutzern zu präsentieren (Stanisic & Nikolic, Kontrola i revizija hotelskog poslovanja, 2009, S. 7).“

Das Institut der forensischen Wirtschaftsprüfer (*Institute of forensic auditors- IFA*) versteht unter der forensischen Wirtschaftsprüfung die Handlungen zur Erfassung, Bestätigung, Verarbeitung, Analyse und Berichterstattung von Daten, mit dem Ziel des Erhalts von Daten und Nachweisen, die infolge von kriminellen Handlungen bei Jahresabschlüssen und präventiven Beratungsleistungen entstanden sind und die in gerichtlichen und finanziellen Streitigkeiten verwendet werden können. Die forensische Wirtschaftsprüfung wird in Verdachtsfällen von Veruntreuung und Betrügen angewendet, wenn eine steuerliche Verpflichtung zu bestimmen ist, bei der Untersuchung des Ehegatten im Scheidungsprozess oder bei der Untersuchung von Angaben im Zusammenhang mit Bestechung sowie aus anderen Gründen. Die Kenntnisse und Fähigkeiten umfassen Folgendes: Ermittlungsfähigkeiten, Untersuchung, Recht, quantitative Methoden, Finanzen, Wirtschaftsprüfung, Rechnungslegung und Umsetzung der gesetzlichen Regelungen. Organisatorisches Verhalten und angewandte Psychologie sind Kenntnisse und Fähigkeiten von wesentlicher Bedeutung (Bartulovic & Filipovic, 2016, S. 45-46; ICFA, 2016).

Unternehmen sind verpflichtet, Programme umzusetzen, die das Auftreten von Betrügen verhindern und im Laufe des Jahres durch die interne und externe Prüfung bewertet werden. In diesem Zusammenhang werden im anschließenden Teil dieser Arbeit die Prüfungsverfahren zur Aufdeckung und Verhinderung von Betrügen dargelegt, bzw. die Verfahren der internen Prüfung und die spezifischen Verfahren der externen Prüfung erläutert.

3.2.1. Interne Prüfung

Das Wertpapieraufsichtsgesetz (WAG) 2007 verpflichtet die im WAG aufgelisteten Institute (Wertpapierfirmen, Wertpapierdienstleistungsunternehmen, Kreditinstitute und Versicherungen) zur Einhaltung gewisser Regelungen, mit dem Ziel bei der Abwicklung von Finanzgeschäften sowohl Kunden als auch das Institut vor finanziellen Schäden zu bewahren. Die Regeln sind in drei Kategorien unterteilt: Compliance (§18 WAG 2007), Risikomanagement (§19 WAG 2007) und interne Revision (§20 WAG 2007). Bei diesen Unternehmen, genau wie bei allen anderen, sind die „angemessene interne Kontrollmechanismen, welche die Einhaltung von Beschlüssen und Verfahren auf allen Ebenen sicherstellen, einzurichten und laufend aufrecht zu erhalten sowie diese zu überwachen, regelmäßig zu bewerten und die zur Behebung etwaiger Mängel erforderlichen Maßnahmen zu ergreifen (Wirtschaftskammer

Österreich- Die Finanzdienstleister, 2012, S. 2).“ Das bezieht sich auf die regelmäßige Kontrolle des IKS. Die Aufgaben der internen Revision können von der Geschäftsleitung übernommen werden, oder an die externen Institutionen (z.B. Wirtschaftsprüfungsgesellschaften) ausgelagert werden (Wirtschaftskammer Österreich- Die Finanzdienstleister, 2012, S. 1-3). Neben Finanzinstituten sind auch Unternehmen zur Compliance verpflichtet. Unter Compliance in diesem Sinne sind alle Maßnahmen zu verstehen, die wirtschaftliche Schäden, nichtige Verträge, etc. vermeiden sollen (JEANNEE Rechtsanwalt GmbH, 2014). In Österreich wird diese Thematik durch das Unternehmensrechtsänderungsgesetz URÄG 2008 abgedeckt und es wird betont, dass „bei börsennotierten Unternehmen und den sogenannten „XL- Unternehmen“ (Bilanzsumme > EUR 96,25 Mio. oder Umsatzerlöse > EUR 192,5 Mio.) in Zukunft ein Prüfungsausschuss einzurichten ist. Zu seinen erweiterten umfangreichen Aufgaben gehört u.a. die Überwachung der Wirksamkeit des internen Kontrollsystems (IKS), eines allfälligen internen Revisionssystems (IRS), und des Risikomanagementsystems (RMS) (Arbeiterkammer Österreich, 2017).“

3.2.1.1. Interne Revision

Die interne Prüfung ist das Verfahren der Beurteilung oder Überwachung der in der Organisation aufgestellten Aktivitäten. Sie arbeitet unter anderem durch die Prüfung, Beurteilung und Berichterstattung an das Management und die Unternehmensleitung über die Angemessenheit und Effektivität der Komponenten des Rechnungslegungssystems und des internen Kontrollsystems (BDO Deutschland, 2017).

Die Definition nach dem Deutschem Institut für Interne Revision e.V. (IIR) lautet: „Die interne Revision erbringt unabhängige und objektive Prüfungs- und Beratungsdienstleistungen, welche darauf ausgerichtet sind, Mehrwerte zu schaffen und die Geschäftsprozesse zu verbessern. Sie unterstützt die Organisation bei der Erreichung ihrer Ziele, indem sie mit einem systematischen und zielgerichteten Ansatz die Effektivität des Risikomanagements, der Kontrollen und der Führungs- und Überwachungsprozesse bewertet und diese verbessern hilft (Interne Revision, 2017).“

Das Institut interner Prüfer (The Institute of Internal Auditors) definiert die interne Prüfung als „unabhängige, objektive, versichernde und beratende Tätigkeit, deren Ziel die Verbesserung und Optimierung der Operationen einer Organisation ist. Sie hilft der Organisation bei der Erreichung ihrer Ziele, indem sie eine systematisch disziplinierte

Beziehung zur Bewertung und Optimierung der Effektivität im Verfahren des Risikomanagements, Kontrollsystem und im Unternehmen selbst einführt (Stanisic, Interna kontrola i revizija, 2014, S. 158).“

Die interne Prüfung ist die vollständigste und modernste Form der Überwachung des finanziellen und materiellen Geschäftsbetriebs des Unternehmens sowie die Form der Überwachung, die die Rechnungslegung und administrativen Kontrollen im internen Kontrollsystem betreffen. Die interne Prüfung ist eine systematische, objektive Beurteilung durch interne Prüfer von verschiedenen Operationen sowie die Kontrolle innerhalb der Organisation zur Feststellung, ob finanzielle und operative Informationen präzise und zuverlässig sind, die Unternehmensrisiken identifiziert und minimiert wurden, die externen Regelungen und akzeptablen internen Richtlinien und Verfahren eingehalten wurden, die zufriedenstellenden operativen Kriterien angenommen wurden, die Quellen erfolgreich und ökonomisch genutzt wurden, und ob die Ziele der Organisation erfolgreich umgesetzt wurden – alles zum Nutzen der Hilfsmitglieder der Organisation in der effektiven Entlastung deren Verpflichtungen.

Es kann allgemein beschlossen werden, dass die Hauptaufgaben der internen Revision folgende sind:„

- Erstellung und dauerhafte Umsetzung eines Revisionsprogramms mit dem Ziel, die Angemessenheit und Wirksamkeit der Systeme, internen Kontrollmechanismen und Vorkehrungen des Unternehmens zu prüfen und zu bewerten;
- Ausgabe von Empfehlungen auf der Grundlage der Ergebnisse der ausgeführten Aufgaben;
- Überprüfung der Einhaltung dieser Empfehlungen und
- Erstellung von Tätigkeitsberichten (Wirtschaftskammer Österreich- Die Finanzdienstleister, 2012, S. 3)."

Das Ziel der internen Kontrolle bei der Aufdeckung von Betrügen ist es, der Unternehmensleitung bei der effizienten Durchführung ihrer Arbeit zu helfen, indem sie mit Analysen, Einschätzungen, Empfehlungen und Ratschlägen zu diesem Thema versorgt wird. Es ist notwendig, dass der interne Prüfer jederzeit die Möglichkeit eines Betrugs verfolgt und schlussendlich feststellt, ob im Zweifelsfall eine weitere Untersuchung erforderlich ist. Dies wird durch den Erwerb des Verständnisses der Indikatoren erreicht, die darauf hindeuten,

dass sich ein Betrug abgespielt hat, und dann durch die Durchführung von Untersuchungen mit dem Ziel der Identifizierung von Mängeln des internen Kontrollsystems, die zum Betrug führen können. Obwohl die Aufdeckung von Betrügen nicht die Hauptverantwortung des internen Prüfers ist, sollte er immer die Möglichkeit der Betrugsentstehung im Auge behalten, und falls ihm etwas für einen Betrug verdächtig ist, sollte er die verantwortlichen Personen darüber verständigen (Stanisic, Interna kontrola i revizija, 2014, S. 162-164; Rat der Europäischen Union (Brüssel), 2017, S. 68-69).

Internen Prüfer führen eine Reihe von Verfahren durch, um eine vernünftige Sicherheit darüber zu erhalten, ob das Betrugsrisiko auf ein annehmbar niedriges Niveau reduziert wurde. Es ist wichtig, dass in der Abteilung der internen Prüfung die Verfahren der proaktiven Prüfung und Überwachung der Transaktionen entwickelt werden, um Betrüge rechtzeitig aufzudecken (Hayes et al. 2005, S. 232-235).

Die interne Revision wird durch die Implementierung von Internen Kontrollsystemen unterstützt. Interne Kontrollsysteme sind mit dem Insolvenzrechtsänderungsgesetz aus dem Jahr 1997 zu einem pflichtigen Bestandteil jeder Gesellschaft geworden. Das Unternehmensänderungsgesetz 2008 (URÄG 2008) hat die bereits bestehenden Vorschriften noch deutlicher definiert und ausgedehnt. Die Idee von IKS stammt aus den Vereinigten Staaten und kommt als Folge unterschiedlicher Betrugsfällen in der Wirtschaftssphäre. Das American Institute of Certified Public Accountants (AICPA) hat die allererste Definition für IKS veröffentlicht: „Unter IKS werden sämtliche Maßnahmen und Vorkehrungen verstanden mit dem Ziel:

- zur Bewahrung des Vermögens des Unternehmens
- zur Gewährleistung der Zuverlässigkeit des Rechnungswesens
- zur Verbesserung der Effizienz betrieblicher Abläufe
- zur Sicherung der Einhaltung der Geschäftspolitik zu verstehen (Löffler & Nayer, 2011, S. 3)."

Wie schon erwähnt, in Europa gelten die 4., 7. und 8. EU-Richtlinie zur Verstärkung der Corporate Governance in den Unternehmen. Die einzelnen europäischen Länder haben diese Richtlinien in das Staatsrecht umgesetzt. Was die USA betrifft, haben die Richtlinien besonders stark an Bedeutung gewonnen, begründet durch mehrere Unternehmenszusammenbrüche,

unter anderem den von Enron. Nach dem Enron Skandal ist der schon erwähnte Sarbanes-Oxley Act in Kraft getreten, um die internen Kontrollen besser aufzustellen.

Neben der Tatsache, dass IKS eine gesetzliche Verpflichtung darstellen, helfen sie den Unternehmen, eine erfolgreiche und nachhaltige Unternehmensführung zu realisieren. Sie unterstützen die Gesellschaften dabei, rechtzeitig potentielle Risiken zu identifizieren. Die IKS sind durch mehrere Merkmale bestimmt: Organisation, Scoping, Dokumentation, Prüfung und Aktualität, Berichterstattung, gesetzliche Richtlinien und Kosten-Nutzen-Verhältnis. Damit die IKS erfolgreich sind, müssen alle genannten Merkmale unter Kontrolle gehalten werden. Im ersten Schritt müssen alle Prozesse klar definiert werden. Für alle Unternehmen, die grenzübergreifend tätig sind, besteht die zusätzliche Herausforderung, die länderübergreifenden Gesetze im Griff zu halten. Studien haben nachgewiesen, dass Firmen mit einer spezialisierten IKS-Abteilung, erfolgreicher sind, als jene ohne eine solche Abteilung. Im weiteren Schritt müssen alle Unternehmensrisiken gescoped und analysiert werden. Nur durch eine effiziente Risikopolitik kann ein effizientes IKS aufgebaut werden. Obwohl die Gefahr besteht, dass es nicht als sonderlich relevant einzustufen ist, ist die Dokumentation ein wesentlicher Bestandteil jedes IKS. Die Studien zeigen, dass viele Unternehmen eine nicht einheitliche und komplizierte Dokumentation haben, was zu Schwierigkeiten dabei führt, Unternehmensprozesse abzubilden und richtig zu verstehen. Nur Transparenz und Klarheit schaffen hier einen Mehrwert. IKS müssen regelmäßig geprüft und gewartet werden. Mindestens einmal im Jahr muss eine detaillierte Prüfung durchgeführt werden. Ohne ständige Wartung, können leicht unbemerkt Fehler auftreten. Es sollen alle im Unternehmen informiert werden, wie die Systeme funktionieren. Nur durch eine transparente Berichtserstattungskultur ist es möglich die wahre Effizienz zu erreichen. Wichtig ist auch, dass alle neuen Richtlinien, rechtzeitig in die Unternehmensstruktur eingebaut werden. Die ineffizienten IKS hindern die Unternehmensreaktionsfähigkeit und Prozessgeschwindigkeit. Die Studien zeigen, dass die meisten Unternehmen den Nutzen von IKS gegenüber den Kosten priorisieren (Detecon (Schweiz) AG in Zusammenarbeit mit der Handelshochschule Leipzig und der Wirtschaftsuniversität Wien, 2010, S. 4-5).

Es ist gesetzlich vorgeschrieben, dass Unternehmen gewisse wichtige Merkmale anhand eigener interner Prozessketten definieren und für die Wirtschaftsprüfung transparent machen. Leider hat das Gesetz diese „wichtigen Merkmale“ bisher nicht definiert, was den Unternehmen einen idealen Spielraum für diversen Manipulationen offenlässt (Detecon

(Schweiz) AG in Zusammenarbeit mit der Handelshochschule Leipzig und der Wirtschaftsuniversität Wien, 2010, S. 6). Um diese Lücken zu decken und die Manipulationen zu verhindern, müssen die Wirtschaftsprüfer sorgfältig alle Unternehmensberichte prüfen und falls dabei Fehler entdeckt werden, Forensiker hinzuziehen.

3.2.1.2. Risikomanagement

Das Risikomanagement hilft dem Unternehmen, die richtigen Entscheidungen zu treffen, indem es ihm ermöglicht, alle potenziellen Risiken zu erfassen und zu erläutern. Eine konstante Steuerung des Risikos ist hierbei notwendig. Risikomanagement beinhaltet sowohl die externen (z.B. Naturkatastrophen), als auch die internen (z.B. Zahlungssicherung) Risiken (Unterhauser, 2007).

Die österreichische Gesetzgebung deckt durch unterschiedliche Vorschriften das Risikomanagement ab. Die Unternehmen sind laut § 243 UGB verpflichtet, beim Jahresabschluss auch einen Lagebericht zu veröffentlichen, der die Geschäftsverläufe abbildet (§243 UGB Lagebericht). Das UGB zwingt die Unternehmen weiter, in diesem Lagebericht, alle Risiken und Ungewissheiten, zu erfassen. Weiterst müssen Unternehmen die angewendeten Finanzinstrumente und Systeme des Risikomanagements darlegen. Das Risikomanagement überschneidet sich teilweise mit den internen Kontrollsystemen und kontrolliert diese dabei gleichzeitig. Laut GmbH-Gesetz (GmbHG) müssen Geschäftsführer sicherstellen, dass das Unternehmen ein adäquates IKS hat und, dass die Risiken somit kontrollierbar sind. In einer Aktiengesellschaft muss der Vorstand die Verantwortung für das IKS und das Risikomanagement übernehmen. Dafür sorgt § 82 Aktiengesetz (AktG) (Unterhauser, 2007; RIS §82 AktG).

Obwohl es in Österreich kein allgemeines Gesetz gibt, das das Risikomanagement zur Gänze bestimmt, gibt es eine Reihe von Vorschriften, die die Unternehmen verpflichten, sich mit dem Thema „Risikomanagement“ zu beschäftigen. Grundsätzlich lässt sich festhalten, dass österreichischen Unternehmen strenge Normen beachten müssen (Unterhauser, 2007).

3.2.1.3. Compliance

Der Begriff „Compliance“ umfasst einerseits die internen Regelungen eines Unternehmens (z.B. Korruptionsvermeidung) und andererseits die Beziehungen des Unternehmens zum Markt und seiner Konkurrenz (z.B. Verstöße gegen Wettbewerbs- und

Kartellrecht) (Bartelsmann, 2018). Dies bedeutet also, dass Compliance „die Einhaltung aller Gesetze, Verordnungen und Richtlinien sowie von vertraglichen Verpflichtungen und freiwillig eingegangenen Selbstverpflichtungen (KPMG, 2011, S. 4-6)“ umfasst. Compliance bezieht sich auf alle Unternehmensprozesse. Es gibt keine Einschränkungen bezüglich der Geschäftsbereiche. Die Compliance ist länder- und personenübergreifend. Falls das Unternehmen als Konzern agiert, bezieht sich die Compliance auf den gesamten Konzern. Eine berühmte Bezeichnung für Compliance ist „Code of Conduct“ (KPMG, 2011, S. 4-6).

Aus Non-Compliance folgen die Verstöße gegen Kapitalmarkt-, Arbeits- und Steuerrecht, das Lebensmittelrecht, das Umwelt- und Produkthaftungsrecht. Bei einem Missachten der Compliance-Regelungen werden sowohl Unternehmen als auch Mitarbeiter zum Strafsubjekt. Die Strafe kann in Form einer Geldstrafe erfolgen (Bußgelder), für Verstöße gegen öffentlich-rechtliche Vorschriften, oder durch eine finanz-strafrechtliche Verantwortung. Die Unternehmen riskieren dabei, ihren eigenen Ruf zu verletzen und schlecht bewertet zu werden. Bereits ein Vorwurf der Ordnungswidrigkeiten verursacht enorme externe Kosten und einen erheblichen internen Aufwand (KPMG, 2011, S. 4-6; Audit Committee Institute, 2007, S. 5).

So wie für das Risikomanagement, gibt es auch für Compliance keine präzise Gesetzeslage. Trotzdem lassen sich die Regeln aus unterschiedlichen Gesetzen abbilden, die dann im Endeffekt auch die Compliance regeln. Beispielsweise sind die Vorstandsmitglieder einer Aktiengesellschaft nach § 70 Abs.1 AktG verpflichtet, die Unternehmensorganisation und Kultur so zu gestalten, dass die Gesellschaft rechtskonform (compliant) ist (KPMG, 2011, S. 4-6).

3.2.1.4. Bewertung des Betrugsrisikos

Die Bewertung des Betrugsrisikos stützt sich stärker auf die möglichen Betrugsszenarien als auf die Risikobewertung. Die Bewertung berücksichtigt verschiedene Weisen, auf welche Betrüge und Täuschungen innerhalb und außerhalb des Unternehmens passieren können. Ebenso wird die Sensibilität des Unternehmens für die Möglichkeit der Umgehung der Kontrollen seitens der Unternehmensleitung erörtert. Ein Verfahren der Bewertung des Betrugsrisikos endet mit einer Beurteilung des möglichen Einflusses des Betrugsrisikos auf die Richtigkeit und die faire Darstellung des Jahresabschlusses.

Die Bewertung des Betrugsrisikos durch den internen Prüfer besteht aus folgenden Schritten:

- Identifizierung der relevanten Faktoren für das Betrugsrisiko
- Identifizierung der potenziellen Betrugsschemen und Festsetzung der Prioritäten auf der Grundlage des Risikos
- Vergleich der bestehenden Kontrollen mit den potenziellen Betrugsschemen und Identifizierung von Löchern
- Prüfung der Effektivität der präventiven Kontrollen und der Aufdeckungskontrollen in Bereichen mit einer bestehenden Möglichkeit der Betrugsentstehung
- Dokumentation und Berichterstattung über die Bewertung des Betrugsrisikos (Kacanski, 2012, S. 43-44).

Jedes Unternehmen vergleicht für sich selbst die Kosten der internen Kontrolle und die Vorteile von der Minderung oder Beseitigung der Risiken. Dennoch sollte das Verfahren der Bewertung des Betrugsrisikos adäquat dokumentiert werden. Das bedeutet, dass die internen Prüfer und der Prüfungsausschuss eine offene Kommunikation mit den externen Prüfern haben sollen, insbesondere zu Fragen der Ausgesetzttheit gegenüber falscher Finanzberichterstattung, Missbräuchen, sowie zur Frage, ob im Berichtszeitraum Fälle von tatsächlichen oder potentiellen Betrügen aufgedeckt wurden (Europäische Kommission Generaldirektion Regionalpolitik und Stadtentwicklung, Leifdaten zur Bewertung des Betrugsrisikos und zu wirksamen und angemessenen Betrugsbekämpfungsmassnahmen, Programmplanzeitraum 2014-2020, 2014, S. 9-11).

3.2.1.5. Beurteilung der Umsetzung interner Kontrollen

Die interne Kontrolle kann helfen, eine zuverlässige Finanzberichterstattung sowie die Konformität mit Gesetzen und Vorschriften zu sichern. Die Definition des internen Kontrollsystems ist im Standard ISA 400 gegeben – *Risikobewertung und interne Kontrolle*, in welchem das interne Kontrollsystem „alle von der Unternehmensleitung der juristischen Person angenommenen Richtlinien und Verfahren zur Erreichung ihrer Ziele (interne Kontrollen) kennzeichnet. Sinn ist die Sicherstellung, dass der Geschäftsbetrieb der juristischen Person ordnungsmäßig und effizient durchgeführt wird (International standard on auditing 400, 2018, S. 358-360).“ Dies umfasst die Einhaltung der Richtlinien der Unternehmensleitung, die Erhaltung der Integrität der Vermögensmittel, die Verhinderung

und Aufdeckung von kriminellen Handlungen und Fehlern, die Richtigkeit und Vollständigkeit der Rechnungslegungs-Evidenzen sowie die rechtzeitige Zusammenstellung zuverlässiger finanzieller Informationen (Stanisic, Interna kontrola i revizija, 2014, S. 8; International standard on auditing 400, 2018, S. 358-360).

Die Unternehmensleitung trägt die Hauptverantwortung für die Gestaltung und Umsetzung des internen Kontrollsystems, dessen Aufgabe die Verhinderung von Betrügen ist, und die Rolle des internen Prüfers ist die Unterstützung der Unternehmensleitung durch die Untersuchung und Beurteilung der Angemessenheit und des Erfolgs der umgesetzten Kontrollen. Die internen Prüfer erörtern, ob die Kontrollumgebung die entsprechenden Einstellungen und Aktionen in der Richtung der internen Kontrolle aufstellt, ob die juristische Person realistische Ziele sowie einen Verhaltenskodex eingeführt hat, der die verbotenen Handlungen und deren Bestrafung festlegt. Darüber hinaus kontrolliert der interne Prüfer, ob die entsprechenden Richtlinien zur Bevollmächtigung und Genehmigung umgesetzt werden und ob Verfahren zur Überwachung der Geschäftstätigkeit und zur Sicherung von Vermögenswerten aufgestellt wurden. Der interne Prüfer kann bei der Beurteilung der internen Kontrollen das Betrugsrisiko identifizieren (Stanisic, Interna kontrola i revizija, 2014, S. 158-160; International standard on auditing 400, 2018, S. 358-360).

Bei der Erörterung des Betrugsrisikos bietet der interne Prüfer eine vernünftige Sicherheit über die erkannten und materiell bedeutenden Mängel der internen Kontrollen, Fehler oder absichtlichen Handlungen. Die internen Prüfer müssen sich bewusst sein, welche Möglichkeiten infolge von Schwächen in den internen Kontrollen unter anderem entstehen können: nicht genehmigte Transaktionen, unerwartete Variationen von Transaktionen, Fälle der Umgehung der internen Kontrollen, unerklärliche Abweichungen der Preise und ungewöhnlich hohe Verluste. In solchen Fällen führt der interne Prüfer eine Bewertung der Indikatoren durch und entscheidet, ob die Notwendigkeit für weitere Maßnahmen und die Einleitung einer Untersuchung besteht. Falls die Notwendigkeit für eine Untersuchung besteht, muss der interne Prüfer dies offenlegen, indem er die ausführenden Geschäftsführer verständigt und eine fachliche Untersuchung empfiehlt (Stanisic, Interna kontrola i revizija, 2014, S. 158-160). Die Aufgabe des internen Prüfers ist die Überprüfung der Angemessenheit der Funktionsweise des internen Kontrollsystems in jeder Berichtsperiode, sowie die Verständigung der zuständigen Behörden über die eventuell erkannten Mängel dieses Systems (Stanisic, Interna kontrola i revizija, 2014, S. III).

Wie bereits dargelegt, besteht das interne Kontrollsystem in der Organisation aus mehreren Komponenten, wie beispielsweise: Kontrollumgebung, Risikoabschätzung, Kontrollprozesse, Informationen und Kommunikation und Monitoring. Diese beinhalten Richtlinien und Verfahren, deren Ziel nicht nur die Verhinderung und Aufdeckung von illegalen Handlungen in der Organisation ist, sondern auch die Verwirklichung anderer Ziele wie z.B. effizienter Geschäftsbetrieb, Bestehen eines zuverlässigen Systems der Finanzberichterstattung, Schutz des Vermögens u.Ä. Die internen Prüfer sollen feststellen, in welchem Maß die Unternehmensleitung adäquate Kriterien für die Feststellung der Zielerfüllung aufgestellt hat (Pickett, 2005, S. 71-72; Rautenstrauch, 2016).

Einige Prüfungsabteilungen verwenden Fragebögen über die interne Kontrolle für die Beurteilung der Kontrollen. Es gibt einige Standardsysteme, mithilfe derer der Wirtschaftsprüfer eine Frageliste erstellen kann, die zwecks der Beurteilung erarbeitet sind, ob die erwartete Anwesenheit der Kontrollen überhaupt gegeben ist. Die Antworten sind in einer ja/nein-Form gestaltet, wobei „nein“ auf das Bestehen eines Problems hindeutet, das weiter untersucht werden soll. „Standardisierte Ansätze zur Beurteilung durch den Wirtschaftsprüfer sparen Zeit und sorgen für Konsistenz, können aber für eine risikobasierte Wirtschaftsprüfung weniger geeignet sein, wo Risiken sich ändern und Standardantworten weniger sinnvoll sein können (Pickett, 2005, S. 193-194; 229-231).“

Die Bewertung der Kontrollen sollte so gestaltet sein, dass sie die Aspekte der risikobedrohten Systeme betont, um am Ende des Verfahrens die zu unternehmenden Aktivitäten zur Beseitigung dieser Risiken vorzuschlagen. Das Nicht-Bestehen, Mängel oder Schwächen der Kontrollen sollten für die Prüfungsphase der Überprüfung richtungsweisend sein. Die Schlüsselkontrollen, auf die sich die Unternehmensleitung stützt, charakterisieren auch die Prüfungspläne, die vom internen Prüfer durchzuführen sind. Die Überprüfungen der Kontrollen zielen darauf ab, die operative Effektivität der Kontrollen bei der Verhinderung, Aufdeckung und Besserstellung von materiell bedeutenden Fehlern auf dem Niveau der Behauptung in den Jahresabschlüssen zu beurteilen.

3.2.1.6. Betrugsuntersuchungen

Wenn im Unternehmen Bedenken wegen Fehlern in der internen Kontrolle auftauchen oder der Verdacht entsteht, dass Betrüge vorhanden sind, wird eine Untersuchung eingeleitet. Die Untersuchung von Betrügen durch den internen Prüfer besteht aus: Sammlung von

Informationen und Erkenntnissen, ob es zum Betrug gekommen ist, Identifizierung von Verlusten, Identifizierung der am Betrug teilnehmenden Akteure, Identifizierung des Betrugsplans/-szenarios, Befreiung vom Verdacht von unschuldigen Personen und Vorbereitung von ausreichender Dokumentation für die Einleitung eines Gerichtsverfahrens.

Die Schlüsselphasen der durchgeführten Untersuchung des Betrugs sind:

1. Einreichung von Beschwerden
2. Festlegung der grundlegenden Fakten vor der Untersuchung selbst
3. Untersuchungsplan
4. Frage der Überwachung
5. Durchführung der vollen Untersuchung
6. Befragung
7. Bericht über die durchgeführte Untersuchung (Pickett, 2005, S. 168-172).

Einreichung von Beschwerden bedeutet, dass die Beschwerden oder Meldungen über potentielle Betrüge aus mehreren Quellen stammen können, wie beispielsweise Berichte über Mängel der internen Kontrolle, formale Beschwerden von Käufern, Lieferanten oder Banken, anonyme Meldungen oder Meldungen über das Meldesystem für festgestellte Unregelmäßigkeiten, sofern dieses im Unternehmen besteht (Pickett, 2005, S. 168-172).

Festlegung der grundlegenden Fakten vor der Untersuchung selbst bedeutet, dass der interne Prüfer die Person oder die Personen befragt, von denen Meldungen über den Betrug stammen, was ihm die Sammlung anderer notwendiger Informationen ermöglicht. Der Wirtschaftsprüfer erstellt dann eine Liste der gesammelten Details, die ihm als Ausgangsgrundlage für die Durchführung einer Betrugsuntersuchung dienen (Pickett, 2005, S. 168-172).

Der Untersuchungsplan sollte aus den Gesprächen mit der Unternehmensleitung abgeleitet werden. Dieser legt den Ansatz der Untersuchung selbst fest, den geplanten Arbeitsumfang, die notwendigen Ressourcen und die klare Definition der Rolle jedes Teilnehmers in der Untersuchung (Pickett, 2005, S. 168-172).

Die Frage der Überwachung stellt das Beobachten der Aktivitäten einzelner Personen ohne deren Wissen dar. Das Beobachten und Sammeln von Nachweisen ist eine nützliche Methode zur Sicherung von Informationen während der Untersuchung (Pickett, 2005, S. 168-172; Puhani, 2018).

Die Durchführung der vollen Untersuchung besteht aus der Sammlung von Nachweisen. Dies beinhaltet die Durchsicht der Dokumentation, Befragung, Überwachung, Analyse und Verfolgung von Transaktionen. Um festzustellen, ob ein Betrug begangen worden ist, müssen relevante Nachweise gesammelt werden (Pickett, 2005, S. 168-172).

Die Befragung stellt eines der wichtigsten Verfahren während der Durchführung der Untersuchung dar, weil die meisten Fragen durch die Befragung der entsprechenden Personen gelöst werden können. Die Gespräche können mit Personen geführt werden, die den Betrug gemeldet haben, mit Schlüsselzeugen, Managern, Verdächtigen u.Ä. Am wichtigsten sind Befragungen von Zeugen, von denen verlangt werden kann, eine formale Aussage zu unterzeichnen (Pickett, 2005, S. 168-172).

Der Bericht über die durchgeführte Untersuchung stellt alle Befunde dar, zu denen der interne Prüfer gekommen ist. Es kann auch die Empfehlung für weitere Handlungen gegeben werden. Falls genügend Nachweise gesammelt werden, die den aufgetretenen Betrugsfall in der Organisation bestätigen, sind zwei Szenarien möglich. Die erste Möglichkeit ist, den Fall dem zuständigen Gericht zu melden und ein offizielles Gerichtsverfahren einleiten. Die zweite Möglichkeit ist, dass die an dem Betrug beteiligten Mitarbeiter vor die Disziplinarkommission des Unternehmens selbst gebracht werden und auf diese Weise die Sanktionen für sie bestimmt werden (Pickett, 2005, S. 168-172; Leitlinie V 201: Zur Berichterstellung in der Internen Revision, 2012).

3.2.2. Externe Prüfung: Wirtschaftsprüfung

Die jährliche Wirtschaftsprüfung des Jahresabschlusses soll von einem unabhängigen und qualifizierten Wirtschaftsprüfer durchgeführt werden, mit dem Ziel der Bereitstellung von objektiven Nachweisen, die zeigen, dass der Jahresabschluss die tatsächliche finanzielle Lage der juristischen Person darstellt. Laut dem Internationalen Prüfungsstandard ISA 240 *Verantwortung des Wirtschaftsprüfers für die Erörterung von kriminellen Handlungen und Fehlern bei der Prüfung des Jahresabschlusses* wird dem Prüfer die Anforderung gestellt, bei

der Planung und Durchführung der Wirtschaftsprüfung mit dem Ziel der Reduzierung des Prüfrisikos auf ein annehmbar niedriges Niveau, das Risiko von materiell falschen Angaben im Jahresabschluss zu berücksichtigen, die infolge von Betrug oder anderen kriminellen Aktivitäten entstanden sind (International Standard on Auditing, 2009, S. 157-158). Der Prüfer kann keine absolute Sicherheit erlangen, dass materiell falsche Angaben im Jahresabschluss aufgedeckt werden, und zwar aufgrund von Faktoren wie der Anwendung der Beurteilung, Anwendung von Überprüfungsverfahren, inhärenten Beschränkungen und der Tatsache, dass die meisten verfügbaren Nachweise zwar überzeugend, aber nicht definitiver Natur sind (Petrovic et al. Revizijska regulativa, 2016, S. 77-81).

Bei der Planung der Wirtschaftsprüfung sollte der Wirtschaftsprüfer das Risiko bewerten, dass Betrüge und Fehler materiell bedeutende, falsche Angaben im Jahresabschluss verursachen können, und er sollte die Unternehmensleitung zum Bestehen des aufgedeckten Betrugs oder der materiell bedeutenden Fehler befragen. Auf der Grundlage der Risikobewertung sollte der Wirtschaftsprüfer das Prüfungsverfahren so entwickeln, um Sicherheit zu erlangen, dass die falschen Angaben wegen Betrügen und Fehlern, die in Bezug auf die in Gänze betrachteten Jahresabschlüsse materiell bedeutend sind, aufgedeckt werden. Wenn mit der Anwendung der Prüfungsverfahren ein Verdacht auf einen möglichen Betrug vorliegt, sollte der Wirtschaftsprüfer die möglichen Auswirkungen auf den Jahresabschluss erörtern. Im Falle der Aufdeckung des Bestehens von bedeutenden Betrügen und Fehlern sollte der Wirtschaftsprüfer die Unternehmensleitung, die Nutzer des Berichts und die gesetzgebenden Behörden und Regierungsbehörden über die Ergebnisse seiner Arbeit verständigen. Der Wirtschaftsprüfer bewertet zwangsmäßig in Übereinstimmung mit den Prüfungsstandards und –verfahren, welche Bereiche der Gegenstand der Wirtschaftsprüfung sein werden, und er setzt die Natur, den Zeitablauf und den Umfang der Untersuchungen fest. Die Wirtschaftsprüfer nutzen darüber hinaus die Beurteilungen sowohl bei der Interpretation der Ergebnisse ihrer Arbeit als auch bei der Beurteilung der Nachweise (Petrovic et al. Revizijska regulativa, 2016, S. 77-81).

Die Prüfungsverfahren sind mit den Prüfungszielen abgestimmt. Daher sind die Erwartungen der Öffentlichkeit nicht als realistisch zu bewerten, wenn es darum geht, dass Wirtschaftsprüfer jeden Fehler und jeden Betrug aufdecken, der eventuell im Jahresabschluss vorliegt. Der Ausschuss der Wirtschaftsprüfer sollte den Prüfungsplan überwachen und sicherstellen, dass die Wirtschaftsprüfer unabhängig, fachlich kundig und mit dem

Geschäftsbetrieb des Kunden vertraut sind. Die unabhängigen Wirtschaftsprüfer sollten die Entstehung jeglicher Interessenskonflikte mit der Unternehmensleitung des Prüfungskunden vermeiden, weil sie nur auf diese Weise ihre Unabhängigkeit in ihren Aktivitäten beibehalten können, was auch die Grundlage für den Beruf des Wirtschaftsprüfers ist. Jeder Wirtschaftsprüfer muss die Grundprinzipien der Prüfungsethik einhalten, vor allem aber die Grundsätze der Verantwortlichkeit, des öffentlichen Interesses, der Integrität, der Objektivität und der notwendigen Sorgfalt. Laut dem Ethik-Kodex der International Federation of Accountants (IFAC) sind „die Ziele der Rechnungsprüfung, auf höchster Ebene des Professionalismus zu arbeiten, die vorgeordneten Ziele effizient zu erreichen und das öffentliche Interesse zufrieden zu stellen (Aleksic, Revizija i Kontrola, 2012, S. 19-20; 26; Petrovic et al. Revizijska regulativa, 2016, S. 6-9; 77-81; Handelsblatt, 2003).“

Der gewissenhafte Wirtschaftsprüfer sollte die Theorie und die Praxis der Wirtschaftsprüfung kennen. Das Niveau der Bildung, Erfahrung und Fähigkeiten des durchschnittlichen Wirtschaftsprüfers haben, zur Erkennung von Signalen der Existenz von Unregelmäßigkeiten fähig zu sein, sowie mit den Erkenntnissen über die Arten der Durchführung und Aufdeckung von Unregelmäßigkeiten Schritt zu halten. Vom Wirtschaftsprüfer wird verlangt, die notwendigen Kenntnisse über den geprüften Kunden, über die Arten seines Geschäftsbetriebs und über die herrschenden Bedingungen in der Geschäftsbranche, in der sich der Prüfungskunde befindet, zu erwerben. Der Wirtschaftsprüfer sollte das interne Kontrollsystem des Prüfungskunden durchblicken und beurteilen können, eventuelle Rechnungslegungs- und Finanzprobleme erkennen, denen der Auftraggeber ausgesetzt ist, auf ungewöhnliche Ereignisse reagieren sowie bei der Beseitigung aller Zweifel an der Regelmäßigkeit der Nachweise beharren, die im Laufe der Wirtschaftsprüfung auftreten können (Aleksic, Revizija i Kontrola, 2012, S. 39-40). Besteht bei Wirtschaftsprüfern der Verdacht, dass unter den unrichtigen Zahlen in Bilanzen, mehr als ein unabsichtlicher Fehler vorliegt, sind sie dazu verpflichtet die Thematik umgehend an die forensischen Rechnungsprüfer weitergeben.

4. Forensische Rechnungsprüfung

4.1. Klassische forensische Rechnungsprüfung

Das starke Unternehmenswachstum in den letzten Jahren hat die Überprüfung und das Auditing erschwert. Zudem haben sich die Management-Ebenen auf Malversationen

„spezialisiert“, um eigene Interessen befriedigen zu können. Die Politik wird bei vielen Unternehmen eingebunden. Dadurch ist Betrug auf eine höhere Ebene gehoben worden und traditionelle Wirtschaftsprüfer können dagegen nicht mehr ankämpfen. Der Notwendigkeit danach, dass sich Unternehmen erfolgreich und effizient mit solchen Problemen auseinandersetzen, hat eine neue Expertise in das Wirtschaftsleben gebracht- die forensische Rechnungsprüfung (Owojori & Asaolu, 2009, S. 183).

Die Aufdeckung, sowie Aufklärung und der Nachweis von kriminellen Handlungen ist mit ihren spezifischen Besonderheiten verbunden, die die Möglichkeit zur Gelangung der Erkenntnis beeinflussen, ob und wie eine Straftat begangen wurde. Da die Verhinderung und Bekämpfung krimineller Aktivitäten häufig die Kapazitäten und Fähigkeiten der Rechts- und Steuerbehörden übersteigt, ist die Unterstützung und Zusammenarbeit von Experten, bzw. des Wirtschaftsprüfers für die Aufdeckung von Betrügen notwendig.

Die forensische Rechnungsprüfung verwendet das Rechnungswesen, die Wirtschaftsprüfung und Ermittlungsfähigkeiten, um Jahresabschlüsse eines Geschäftsunternehmens zu überprüfen. Forensische Rechnungsprüfer analysieren, interpretieren und fassen komplexe Finanz- und Geschäftsangelegenheiten zusammen. Sie können durch Versicherungsgesellschaften, Banken, Polizei, staatliche Agenturen oder öffentliche Wirtschaftsprüfungsgesellschaften angestellt werden. Forensischen Buchhalter erstellen finanzielle Nachweise, entwickeln Computerprogramme zur Verwaltung gesammelter Informationen und übermitteln ihre Befunde in Form von Berichten oder Präsentationen (Forensic CPA Society, 2018).

Es gibt mehrere Gründen wieso die forensische Rechnungsprüfung immer mehr an Bedeutung gewinnt:

- Die interne Kontrolle und die traditionelle Wirtschaftsprüfung können verschiedene Fakten und andere versteckte Aspekte von Unternehmensbetrug nicht nachvollziehen.
- Die Rotation der Wirtschaftsprüfer ist oft nicht ausreichend, damit sie keine Beziehung zum prüfenden Unternehmen aufbauen können. Zudem besteht die Gefahr von Lobbyismus.
- Die Wirtschaftsprüfer sind nicht sorgfältig überprüft und ausgewählt. Es kann ein Mangel an Qualifikation auftreten.

- Obwohl Wirtschaftsprüfer und interne Prüfer den Betrug rechtzeitig entdecken können, haben sie meistens keine Möglichkeit, mit ihm umzugehen, weil sie in diesem Bereich mangelnde Erfahrung und Kenntnisse haben (Owojori & Asaolu, 2009, S. 185).

Neben Zeugenaussagen vor Gericht kann vom forensischen Rechnungsprüfer möglicherweise verlangt werden, visuelle Hilfsmittel zur Unterstützung der Nachweise vorzubereiten. „Die forensischen Rechnungsprüfer sind beim Federal Bureau of Investigation (FBI), Central Intelligence Agency (CIA), Internal Revenue Service (IRS), Federal Trade Commission (FTC), Inneren Sicherheit, Kanzlei für Alkohol, Tabak und Feuerwaffen, in der Zuständigkeit der Regierung und anderer Regierungsbehörden angestellt (Gray, 2008, S. 115).“ Der Schwerpunkt liegt auf den sogenannten „Weißen-Kragen“ Verbrechen.

Forensische Rechnungsprüfer sind häufig Zeugen in zivil- und strafrechtlichen Gerichtsverhandlungen. In dieser Eigenschaft dienen sie als Gutachter. Sie bezeugen nicht, ob Betrüge entstanden sind. Der Gutachter legt die Nachweise vor. Die forensischen Rechnungsprüfer haben eine Vielzahl von Organisationen, die ihre Arbeit unterstützen. Dies deckt sich auch mit der forschungsleitenden Fragestellung, wonach die forensische Rechnungsprüfung einen Schlüsselmechanismus in der Verhinderung von Betrügen darstellt (Möller & Sigillo, Der Enron-Andersen-Skandal und dessen Einfluss auf das Reputationskapital der Institution Wirtschaftsprüfung, 2010).

4.1.1. Umfang und Arten forensischer Rechnungsprüfung

Laut Dahili Gray, Mitglied des American Institute of Authorised Public Accountants, „erbringen forensische Buchhalter Dienstleistungen in Streitverfahren bei verschiedenen Situationen wie z.B. Betriebsanschaffungen, Vermögensbewertung in Scheidungsverfahren, Schadensersatzanträgen, entgangenen Gewinnen aufgrund von Veruntreuung und anderen gesetzlichen Handlungen, Steuerhinterziehung und Geldwäsche (Gray, 2008, S. 116).“

Einige Autoren betonen, dass „das forensische Rechnungswesen folgenden Zweck hat:

1. Erkennung der Bereiche für mögliche Unregelmäßigkeiten oder Betrüge – bedeutet die Einschränkung des Suchfelds nach bestimmten Unregelmäßigkeiten bzw. Lokalisierung des Bereichs, in dem die Unregelmäßigkeit oder der Betrug stattfindet.

2. Erkennung von konkreten Unregelmäßigkeiten oder Betrügen - bedeutet die Aufdeckung einer bestimmten Unregelmäßigkeit oder eines Betrugs und die Feststellung der Art und Weise, wie sie begangen wurden.
3. Bewertung der Höhe des Risikos der identifizierten Unregelmäßigkeiten oder Betrüge - bedeutet die Bewertung der Gefahr der begangenen Straftat (absichtlich, unbeabsichtigt, Ausmaß der Unregelmäßigkeiten, Gefahr des begangenen Betrugs usw.).
4. Beweisführung – bedeutet die Sicherung der materiellen und anderen Nachweise, die beweisen, dass die Straftat begangen und wie sie begangen wurde (Udruzenje racunovodja, forenzičara i revizora, 2017).“

Im Einklang mit dem Arbeitsbereich umfasst das forensische Rechnungswesen zwei große Bereiche: untersuchendes Rechnungswesen und gerichtliche Unterstützung.

Das untersuchende Rechnungswesen wird dann beauftragt, „wenn der Verdacht einer kriminellen Handlung in Jahresabschlüssen besteht, oder wenn der Betrieb des Unternehmens als vorbeugende Maßnahme überprüft wird (Aleksic, Uloga i značaj forenzičkog racunovodstva u otkrivanju finansijskih prevara, 2015, S. 230).“ Die Funktion des untersuchenden Rechnungswesens besteht aus der Sammlung von eventuellen Nachweisen über Rechtswidrigkeiten und der Zustellung dieser an den Prüfungskunden und falls erforderlich an die Rechtsbehörden, um die Einleitung eines Gerichtsverfahrens zu ermöglichen. Die Dienstleistungen des untersuchenden Rechnungswesens sind finanzstrafrechtliche Ermittlungen und die unabhängige forensische Wirtschaftsprüfung der Jahresabschlüsse (Udruzenje racunovodja, forenzičara i revizora, 2017; Larry et al. 2005).

Gerichtliche Unterstützung bezieht sich auf professionelle Dienstleistungen, die Gerichtsprozesse unterstützen sollen. Diese Sparte kann als eine Form von Beratung verstanden werden (Udruzenje racunovodja, forenzičara i revizora, 2017). Zudem hat das ökonomisch-finanzielle Gutachten als Form des forensischen Rechnungswesens in Strafverfahren eine besondere Bedeutung im Beweisverfahren, bei der Ermittlung von Tatsachen (Cudan, 2015).

4.1.2. Forensische Rechnungsprüfung- berufliche Tätigkeit

Da die forensische Rechnungslegung eine Mischung aus Rechnungslegung, Wirtschaftsprüfung und Gesetz darstellt, lässt sich ableiten, dass der forensische Buchhalter

seine Kenntnisse der Rechnungslegung mit den Ermittlungsfähigkeiten in verschiedenen statutarischen Daten und Ermittlertätigkeiten im Rechnungswesen kombiniert. Weiter muss der forensische Rechnungsprüfer einen hohen Grad an Kommunikationsfähigkeiten, sowohl verbal, als auch schriftlich, besitzen, um von Kunden und Verdächtigen, alle notwendigen Informationen bekommen zu können. Ein Auge fürs Detail muss er dabei ebenfalls haben.

Die forensischen Rechnungsprüfer arbeiten nach dem Grundsatz gründlich, zuverlässig, hochkomplex und professionell zu sein. Wie im letzten Paragraph erwähnt, müssen alle ihre Befunde potenziell als Beweise vor Gericht verwendbar sein können. Deswegen stützt sich das oben beschriebene Wissen stark auf Gesetze und Vorschriften (Buhse, 2013).

Forensischen Buchhalter führen die Wirtschaftsprüfung, Untersuchung und Ermittlung der Richtigkeit der Dokumente der Finanzberichterstattung durch, oft im Zusammenhang mit einem geplanten oder laufenden Gerichtsverfahren. Sie werden mit der Vorlage verdächtiger Finanzdaten beauftragt. Sie können mit Unternehmen, gemeinnützigen Organisationen (einschließlich Regierungen und Strafverfolgungsbehörden) und anderen Subjekten zusammenarbeiten, welche die Dienstleistungen des forensischen Rechnungswesens beantragen. Die forensischen Prüfer unterscheiden sich von den traditionellen Prüfern, dadurch, dass sie eine besonders tiefe Analyse durchführen und diese Analyse mit konkreten Ergebnissen abschließen. Im Gegensatz zu den traditionellen Prüfern, wird von Forensikern erwartet auch komplexe Zusammenhänge verstehen zu müssen und diese so auszuwerten, dass sie zur Not als Gerichtsbeweise verwendet werden können (Owojori & Asaolu, 2009, S. 183-184).

Objektivität ist ein Schlüsselmerkmal, das ein forensischer Prüfer mitbringen muss. Diese Fachleute sind als „Schöpfer der unabhängigen und objektiven Informationen über die Wirtschaft“ angesehen. Laut Experten wird dieser Beruf in den nächsten 20 Jahren eine der Jobbeschreibungen mit der höchsten Nachfrage sein (Vilendecic & Vilendecic, 2014, S. 172-173).

4.1.3. Eigenschaften und Verfahren der Forensik

Betrüge in Jahresabschlüssen können manchmal unbemerkt bleiben, wenn sich auf verschiedene Interpretationen der verwendeten Rechnungslegungsstandards bei der

Erstellung der Jahresabschlüsse gestützt wird. Sobald es einen Verdacht gibt, dass ein Finanzbetrug vorliegt, untersuchen Prüfer den vorliegenden Sachverhalt folgendermaßen: Inspektion, Beobachtung, Befragung und Konfirmation, Kontrolle und das analytische Verfahren (Jovkovic, 2014, S. 53-55). Die Ergebnisse aller dieser Aktivitäten fließen in das Gesamtbild und stellen eine klare und transparente Darstellung des befragten Unternehmens dar. Somit können diese Aktivitäten auch als „Forensic Due Diligence“ bezeichnet werden (KPMG Deutschland, 2017).

Die Inspektion umfasst die Überprüfung aller Dokumente eines Unternehmens, unabhängig davon ob diese in Papier- oder elektronischer Form sind, und sowohl die internen Berichte und Dokumente, als auch die externen. Alle diese Dokumente zeigen dem Prüfer, welche Verträge das Unternehmen hat und wie viele liquide Mittel es besitzt. Durch die Inspektion wird auch ein Einblick in Aktien und Darlehen des Unternehmens gewährt. Oft kann es vorkommen, dass der Prüfer zufällig, im Laufe der Prüfung, noch gewisse verdächtige Positionen in Bilanzen entdeckt. Dieser Schritt ist ein wichtiger Meilenstein für einen eventuellen Beweisprozess im Falle eines Gerichtsverfahrens (Jovkovic, 2014, S. 53-55). Die Prüfung der Unterlagen deutet außerdem auf die Schwachstellen im Unternehmen hin. Rechtzeitige Entdeckung dieser Schwachstellen ist wichtig, da sie leichter durch Betrug oder Angriff ausgenutzt werden können. Zusätzlich kommt es auch oft vor, dass die bereits realisierten Verstöße entdeckt werden (KPMG Deutschland, 2017).

Die Befragung besteht aus der Suche von gut informierten Mitarbeiter des zu prüfenden Unternehmens. Es werden sowohl die Compliance Mitarbeiter zum Gespräch eingeladen, als auch jene aus den betroffenen Abteilungen. Auf diese Weise können gleichzeitig zwei Ansichten zu demselben Problem gesammelt und darauffolgend analysiert werden (KPMG Deutschland, 2017). Diese Technik wird implementiert, wenn Beweise über die Funktionsweise des internen Kontrollsystems gebraucht werden. Die Befragung kann sowohl schriftlich (formal) als auch mündlich (informell) erfolgen, wobei die schriftliche Variante zu empfehlen ist, weil die schriftlich aufgenommenen Informationen später als Beweise dienen können (Jovkovic, 2014, S. 53-55). Die Konfirmation ist eine Bestätigung der vorhandenen Informationen durch Dritte, die keine Verbindung zum Unternehmen haben. Wichtig ist zu beachten, dass die Befragung erheblich durch den Interviewer beeinflusst werden kann. In Abhängigkeit davon, welche Einstellung der Interviewer annimmt, wird der Befragte dazu bereit sein zu kooperieren und die richtigen Antworten zu geben. Die Sozialforschung hat

mehrmals bewiesen, dass gefälschte Interviews öfter passieren als gedacht (Baur & Blasius, 2014, S. 50).

Die Alternativlösung zur Befragung ist die Beobachtung. Diese Methode ist besonders gut geeignet, wenn bereits im Voraus mit einer schlechten Kommunikation zu rechnen ist, oder die Befragung aus einem anderen Grund nicht möglich ist. Durch Beobachtung bekommt der Prüfer einen Einblick in die aktuellen Prozesse und Verfahren des Unternehmens. Weiterst kann ein gutes Verständnis von Interaktionen und Beziehungen zwischen Mitarbeiter gewonnen werden (Baur & Blasius, 2014, S. 56). Ein großer Nachteil dieser Technik ist, dass sie nur eine Momentaufnahme zu einem bestimmten Zeitpunkt abbildet. Der Prüfer bekommt weder die historischen Daten noch die Prognosen (Jovkovic, 2014, S. 53-55). Besteht der Bedarf mit historischen Daten zu arbeiten, können Hintergrundrecherchen durchgeführt werden, indem die bestehenden öffentlichen Quellen analysiert werden. Dadurch ist es möglich nachzuvollziehen, wie hoch das Risiko ist, dass Korruption, Geldwäsche, Kartellausmachungen u.Ä. vorkommen (KPMG Deutschland, 2017).

Die Kontrolle bezieht sich auf eine mathematische Überprüfung der Richtigkeit von Dokumenten oder Berichten. Meistens wird ein Revisions-Software abgespielt, und der Prüfer wird automatisch benachrichtigt, falls die vertraglichen Verbindlichkeiten und Forderungen mit den Summen im Hauptbuch nicht übereinstimmen (Jovkovic, 2014, S. 53-55).

Die analytischen Verfahren sind auf die Untersuchung der Trends und Prognosen bezogen. Oft werden hierbei auch die gegenseitigen Einflüsse von unterschiedlichen Konten und Verträgen überprüft (Jovkovic, 2014, S. 53-55). Analytische Verfahren können auch auf einer technischen Ebene durchgeführt werden. Dafür kommen spezifische IT-Tools zum Einsatz. Es wird zwischen drei unterschiedlichen Methoden der technischen Analyse: KDAT, E-Discovery und Snapshot Collections unterschieden. Eine umfangreiche Gesamtanalyse des Hauptbuches, der Prozesse, der Zahlungsströme und der Kreditorenstammdaten wird im Laufe der KDAT-Analyse durchgeführt. E-Discovery wird erst dann angewendet, wenn ein konkreter Verdacht vorliegt. Diese Analyse umfasst die Prüfung aller E-Mails und elektronischen Dokumente. Bei der Snapshot Collection werden die Daten speziell abgesichert, sodass keine Daten geändert oder gelöscht werden können. Abhängig von der Situation, können forensische Experten 24/7 Zugriff auf die Daten des Unternehmens haben

und beobachten diese, aber im begrenzten Ausmaß, ohne dass sie die Daten in das eigene System für die weitere Analyse abspeichern dürfen (KPMG Deutschland, 2017).

4.1.3.1. Persönlicher Kontakt besser als Lügendetektor

Ein Interview mit dem FBI-Agenten Joe Navarro erzählt von seinen langjährigen Erfahrungen und betont wie ein Gespräch bei der Entdeckung der Kriminalität wichtig ist. Herr Navarro hat mehr als 25 Jahre Arbeitserfahrung beim FBI und mehr als 10000 Verhöre hinter sich.

Laut Navarro muss man die ganze Zeit höchstachtsam sein, wann sich beim Gesprächspartner etwas in der Stimme oder Mimik ändert. Sogar eine Kleinigkeit, die normalen Menschen nicht auffallen würde, kann auf eine Lüge hindeuten. Eine klare und tragende Stimme, gefolgt von einem tiefen und langsamen Atmen deutet die Wahrheit an.

„Eine der allerersten Gesten, die ich bemerkte“, sagt er, „war, dass viele Menschen ihren Hals berühren, wenn sie lügen.“ Den allgemeinen Glauben, dass die Leute wegschauen, wenn sie lügen, hat Navarro widerlegt. „Gerade wenn Menschen lügen, halten sie eher Augenkontakt“, so Navarro, „denn für sie ist es sehr wichtig, möglichst schnell herauszufinden, ob man ihnen ihre Lüge auch wirklich abkauft (Jimenez, 2013).“

Das wichtigste ist, gleich am Anfang Stress zu beseitigen und eine lockere Atmosphäre zu schaffen, denn der Stress blockiert das Denken. Es muss auf alle Körperteile des Befragten geachtet werden. Die Literatur hält fest, dass das Gesicht ein Spiegel menschlicher Emotionen ist und der Interviewer besonderes viel Wert auf dieses legen sollte. Herr Navarro meint aber, dass der ganze Körper gleich wichtig ist, besonders die Füße, da sie „das ehrlichste Körperteil des Menschen seien. Denn sie sind diejenigen, die unsere Spezies über Millionen von Jahren am Leben erhalten haben – weil sie auf Flucht oder Kampf vorbereiten. Drehen die Füße sich weg, fühlt man sich unsicher, zeigen die Zehen nach vorne, ist man souverän und zuversichtlich (Jimenez, 2013).“

Mit „Weißen-Kragen“ Betrügern sind die Interviews besonderes schwer, da solche Menschen es gewohnt sind „Raum einzunehmen, beobachtet zu werden und ihre Reaktionen schnell zu regulieren“. Bei diesen Menschen muss man besonderes auf die kleinsten Zeichen von Erstaunen, Aufregung oder Sorge achten. Diese können nur in wenigen Millisekunden geschehen (Jimenez, 2013).

4.1.3.2. Mittel zur Untersuchung der Handlung

Für die Aufdeckung von Betrug ist es von außerordentlicher Wichtigkeit, die „roten Fahnen (red flags) rechtzeitig zu identifizieren, die von der Anwesenheit des Betrugsrisikos sprechen, nicht aber notwendigerweise damit verbunden sein müssen (Belopavlovic, 2014, S. 129).“

Nach der Identifizierung der roten Fahnen verwenden Wirtschaftsprüfer verschiedene forensische Techniken, um Betrüge aufzudecken. Die gängigsten Methoden sind die horizontale und vertikale Analyse der Bilanzen. Neben den Erkennungs- und Untersuchungstechniken von Betrug gibt es auch Methoden zur Verhinderung von Manipulationen in Jahresabschlüssen, wie z.B. die unerwartete externe Wirtschaftsprüfung, die Teilnahme der internen Wirtschaftsprüfung in den proaktiven forensischen Aktivitäten, sowie wirksame interne Kontrollen (Belopavlovic, 2014, S. 129-130).

Da ein Unternehmen nicht alle Betrüge verhindern kann, müssen seine Wirtschaftsprüfer, Buchhalter und Kontrolleure sich mit einigen Aufdeckungstechniken vertraut machen. Die Wirtschaftsprüfer und Betrugsermittler untersuchen Betrüge, indem sie die Zeichen und Signale von Betrügen bemerken, und dann die Spuren der fehlenden oder betrügerischen Dokumente verfolgen, die einen Teil der Vertuschung der Rechnungslegungsdaten darstellen.

Wichtig ist, dass die Prüfer bestimmten Regeln folgen. Es ist lediglich ein Anfangsverdacht notwendig, um eine forensische Überprüfung zu starten. Alle Aktivitäten werden vertraglich geregelt (Budimir, 2017, S. 107-110; Universität Erlangen, 2018).

Im ersten Schritt muss der forensische Prüfer einen kompletten Plan vor Augen haben: wonach wird gesucht, in welchem Zeitrahmen, welche Beweise werden gebraucht, etc. Der Plan ermöglicht eine effiziente und zeitsparende Untersuchung. Der forensische Prüfer wird oft durch ein gemischtes Team unterstützt: anderen Experte, Drittpersonen unabhängig vom Unternehmen und interne Mitarbeiter aus dem zu prüfenden Unternehmen (Budimir, 2017, S. 107-110; Forensic Accounting Today, 2017).

Der schwierigste und gleichzeitig der wichtigste Teil dieses Untersuchungsprozesses ist das Sammeln von Beweisen. Man unterscheidet zwischen zwei Hauptkategorien von Beweisen: interne Beweise (Bilanzen, Videoaufnahmen durch Sicherheitskameras, E-Mails)

und externe Beweise (Informationen gewonnen durch Lieferanten oder Kunden, Berichte von Externen). Alle diese Beweise müssen auf legale Art gesammelt werden; sonst gelten sie nicht vor dem Gericht (Budimir, 2017, S. 107-110).

Wenn der forensische Prüfer glaubt, er hat genug Beweise gesammelt, fängt die zweite Phase der Untersuchung an: das Interview. Man unterscheidet zwischen zwei Arten von Interviews: Das Verhör, wenn man mit Verdächtigen das Gespräch führt, und das Interview, wenn man mit den Zeugen redet. Alle Interview-Ergebnisse können vor Gericht gebracht werden (Budimir, 2017, S. 107-110).

4.1.3.3. Nachweisarten

Für eine effektive Durchführung der Betrugsuntersuchung ist es notwendig, dass der forensische Rechnungsprüfer alle Regeln des Gerichts kennt und die Abläufe versteht. Im Normalfall wird davon ausgegangen, dass der Prozess vor Gericht endet. Daher, wie schon erwähnt, ist es notwendig, dass von Anfang an, alle Tätigkeiten und gesammelte Dokumente den juristischen Anforderungen entsprechen. Unwissenheit „on front end“ bzw. am Anfang der Untersuchung kann relativ leicht die Beweise desavouieren (Singleton, 2006, S. 299).

Erstmal muss ein Verständnis dafür vorhanden sein, was überhaupt als Beweis gilt, und welche Beweise relevant sind. „Im weitesten Sinne ist der Beweis durch die fünf Sinne und jede Art von Beweisen wahrnehmbar, wie Zeugenaussagen, Aufzeichnungen, Dokumente, Tatsachen, Daten oder konkrete Gegenstände, die rechtlich in einer Verhandlung vorgelegt werden, um eine Behauptung zu beweisen und bei dem Gericht oder der Jury Vertrauen zu wecken (Singleton, 2006, S. 300).“ Somit kann ein Beweis demonstrativ, theoretisch oder umständlich sein. Damit ein Beweis auch juristisch akzeptabel wird, muss er Zeugenaussagen, Gegenstände und Tatsachen beinhalten, die relevant, sachlich und kompetent sind (Singleton, 2006, S. 300; Jahn, 2001).

Die folgenden Punkte gelten als relevant und juristisch akzeptabel:„

- Motiv für das Verbrechen
- Die Fähigkeit des Angeklagten, das Verbrechen zu begehen
- Die Gelegenheit des Angeklagten, das Verbrechen zu begehen
- Bedrohungen oder Böswilligkeit der Angeklagten

- Mittel zur Begehung der Straftat (Besitz einer Waffe, Werkzeug, oder Fähigkeiten zur Begehung des Verbrechens)
- Körperliche Beweise an der Szene, die den Angeklagten mit dem Verbrechen verbinden
- Verhalten und Kommentare des Verdächtigen zum Zeitpunkt der Festnahme
- Versuch, die Identität zu verbergen
- Versuch, Beweise zu zerstören
- Gültige Geständnisse (Singelton, 2006, S. 300).“

Egal um welche Art von Beweisen es sich handelt, Originaldokumente sind immer die besten und müssen dem Gericht vorgelegt werden. Kopien sind immer als sekundär zu bezeichnen (Singelton, 2006, S. 303; Project Consultant, 2013; Steuerberater.net, 2016).

4.2. Digitale forensische Rechnungsprüfung

Die digitale Forensik umfasst „die Aufdeckung und Sammlung, Bewahrung, Beweisführung und das fachliche Gutachten der digitalen Nachweise vor Gericht, in Fällen des Missbrauchs von IKS und Verwaltung von Computer-Vorfällen, Computerkriminalität, Zivilklagen oder administrativen Anforderungen (Milosavljevic & Grubor, 2009, S. 10).“ Sie ist auch unter dem Namen „IT-Forensik“ bekannt. Wie schon erwähnt, bringt die Verwendung der IT-Systeme den Unternehmen Kosten- und Zeitersparnisse, aber gleichzeitig bietet sich durch die IT-Technologie auch ein sehr hohes Missbrauchspotenzial. Die digitale Forensik umfasst die Anwendung von Techniken der Computerwissenschaften zur Unterstützung der Ermittlungen von Diebstahl, Änderung oder Zerstörung von Daten, Betrügen, organisierten kriminellen Handlungen, Mord, Drogenhandel und Terrorismus (IBM Deutschland, 2018). Die digitale Forensik kann als eine gute Ergänzung zur normalen forensischen Prüfung betrachtet werden und bringt der IT-Sicherheit in den Unternehmen viel bei (Heinson et al. 2010, S. 75-76).

Die digitale Forensik umfasst den gesamten Untersuchungsprozess der Verdachtsfälle, sowie die Klarstellung der Delikte. Manche Delikte entstehen rein in der IT-Welt, aber es gibt Straftaten auch die in der Realität stattgefunden haben. Deswegen ist immer gut, die digitale Forensik mit der nicht-digitalen zu kombinieren. Wenn die Straftaten in der realen Welt entstehen, sind die Beweise der IT-Forensik gleich als Gerichtsnachweise anzusehen. Wenn sich bei den Straftaten die reale Welt einmischt, sind die IT-Forensik Beweise eine stabile

Grundlage für das weitere Beweissammeln (Heinson et al. 2010, S. 76). Computerforensik-Experten werden in der Regel aufgefordert, Computer und Computernetzwerke zu untersuchen, um Nachweise zu finden und zu bewahren, sowie um die Ziele aus den folgenden drei Bereichen zu erreichen:„

- Identifizierung des Täters (der Täter) der Straftat oder einer anderen rechtswidrigen Handlung,
- Auffindung und Rettung von Daten, Dokumenten, E-Mail-Nachrichten im Zusammenhang mit strafrechtlichen oder bürgerrechtlichen Fragen
- Wiederherstellung von beschädigten Datenbanken und Dokumenten (Casey, 2011, S. 378).“

Logischerweise sind diese Ziele an das betroffene Unternehmen angepasst und vom Typ der forensischen Prüfer abhängig. Das Identifizieren von Tätern ist meistens das primäre Ziel der Gesetzesvollstrecker, da Täterfindung im Herzen ihres Berufs liegt. Manchmal wollen auch die Opfer den Täter vor dem Gericht sehen bzw. dem Täter Gerechtigkeit widerfahren lassen. Die anderen Opfer haben wiederum nur ein Ziel – Schwächen zu entdecken und weitere digitale Angriffe durch gute Sicherheitsmaßnahmen zu vermeiden. In Abhängigkeit vom primären Ziel ist somit auch die Vorgehensweise der forensischen Prüfer zu definieren. Es besteht die Möglichkeit, die Daten, die Forensiker gesammelt haben, an interne Mitarbeiter des betroffenen Unternehmens oder an externe Dienstleister, die bei der Untersuchung mitwirken sollen, weiterzugeben. In diesem Fall bekommen alle Parteien Kopien, und die Originale bleiben bei den forensischen Prüfern (Heinson et al. 2010, S. 76).

Eine weitere Intention ist festzustellen, ob die Daten als Konsequenz eines Angriffs gestohlen, geändert oder beschädigt worden sind. Dabei ist wichtig genau zu bestimmen, um welche Datenarten es geht, weil der Verlust mancher Daten auch eine Verletzung des Datenschutzgesetzes darstellen könnte (Lochberg, 2014).

Forensischen Prüfer werden oft eingeladen, um Sicherheiten quer zu prüfen und festzustellen, wo die Schwächen der Firewalls liegen oder wieso es zum Angriff kam. Das Identifizieren von Sicherheitslücken ist ein sehr wichtiger Schritt, um neue Angriffe durch die gleiche Lücke auszuschließen, denn „wo es einen gibt, gibt es oft mehr (Casey, 2011, S. 378-380).“

Digitale forensische Prüfer müssen die wahre Expertise haben- die technischen Kenntnisse, Malware-Verständnis, Netzwerk- und Speicheranalysefähigkeiten. Über IP Adressen kann man nachverfolgen, mit welchen IPs das Gerät eine Interaktion hatte, die Exekution der Malware und die anderen mit dem Angriff verbundenen Informationen. Der Netzwerkverkehr gibt Auskunft über die spezifischen Einzelheiten, die mit dem Angriff eng verknüpft waren.

Digitale forensische Prüfer müssen zudem in der Lage sein, unter Druck effizient zu arbeiten. Die Gefahr, dass jederzeit relevante Daten seitens der Angreifer gelöscht werden, droht ständig. Zusätzlich ist das Opfer ungeduldig und erwartet die Antworten schnell zu bekommen, wodurch der forensische Prüfer unter zusätzlichen Zeitdruck gestellt wird.

Die Gefahr, dass es zu Fehlern kommt, oder wichtige Informationen und Beweise übersehen werden, ist unter den beschriebenen Umständen leicht möglich. Deswegen wird vom forensischen Prüfer ein hoher Spezialisierungsgrad und Erfahrung erwartet. Es ist wichtig, dass er sofort reagiert um keine relevanten Daten zu verlieren. Der ganze Prozess erfordert eine detaillierte Analyse, Vorbereitung und Effizienz (Casey, 2011, S. 380-383).

4.2.1. Prüfungsablauf

Sobald der forensische Prüfer das Gerät vor sich hat, wird der Focus nur auf die digitalen Daten gelegt. Wie schon erwähnt, muss der Prüfer gute technischen Kenntnisse haben, um sich mit der Entdeckung, dem Extrahieren und der Analyse der digitalen Daten aus dem Rechner auseinander setzen zu können (Milosavljevic & Grubor, 2009, S. 99-105; Buhse, 2013).

Die ersten Methoden zur Datenextrahierung und -wiederherstellung wurden schon im Jahr 1990 bekannt. Dieser Prozess ist unter dem Namen „mirror picture“ (Techtarget, 2016) in die Öffentlichkeit getragen worden. Die digitale Analyse wurde offiziell als Erweiterung der schon bekannten Methoden- Blutanalyse, DNA-Analyse, etc. anerkannt.

Der erste Schritt ist eine Image-Aufnahme bzw. eine eins-zu-eins Kopie aller Daten, die sich im Moment der Beschlagnahme auf dem Rechner befinden. Es muss garantiert werden, dass die Daten dem Stand zum Zeitpunkt der Beschlagnahme entsprechen. Das gilt auch vor dem Gericht als ein wichtiger Beweis. Eine der bekanntesten Anwendungen für die Image-Aufnahme ist Northon Ghost. Diese Methode ermöglicht eine vollständige

Informationsaufnahme und garantiert, dass keine Daten zufällig ausgelassen werden können. Bei einer Image-Aufnahme müssen die folgenden Regeln beachtet werden:

- „die Kopie muss Bit für Bit generiert werden
- die originale Disk darf in keinerlei Weise geändert werden
- die Integrität kann verifiziert werden
- die bekannten Fehler beim Einloggen und Ausloggen sind notiert
- alle Abläufe werden dokumentiert
- die digitalen Daten werden nicht geändert (Vgl. Serb. Quelle Milosavljevic & Grubor, 2009, S. 100).“

Es wird empfohlen, immer gleich zwei Images aufzunehmen. Eine Kopie wird dem forensischen Prüfer zur Bearbeitung zur Verfügung gestellt und eine weitere wird im Original für eine potenzielle Gerichtsverhandlung aufbewahrt. Wie schon erwähnt ist der beste Nachweis immer in Originalform. Aus dem Image kann sogar die originale Disk reproduziert werden und es kann nachvollzogen werden, was der Verdächtige damals auf seinem Rechner hatte, als auch die Viren die ihn befallen haben.

Die Probleme, die bei der Image-Aufnahme auftreten können sind unterschiedlich und abhängig vom Rechnersystem. Wenn der Rechner alt ist, kann es leicht passieren, dass die Image-Aufnahme nicht vollständig wird, weil der alte Rechner mit den modernen forensischen Technologien nicht kompatibel ist. Wenn das Gerät ein Windows Betriebssystem hat, müssen die Prüfer sogenannte Blockaden verwenden, um die Integrität der Daten zu gewährleisten. Das zweite essentielle Problem entsteht bei Laptops. Wenn man die Festplatte aus dem Gerät entfernen würde, wären eventuell nicht mehr alle Daten lesbar. Weitere Probleme entstehen, wenn sich der Server vom Gerät unterscheidet. Die Technologie, die ein forensischer Prüfer hat, reicht manchmal nicht aus, wenn der Mainframe Server physisch zu untersuchen ist. (Milosavljevic & Grubor, 2009, S. 99-105).

Es kann zwischen mehreren Analysemethoden und Massendatenanalysen in digitaler Forensik unterschieden werden, abhängig von dem Endziel und den zu untersuchenden Objekten. Die bekanntesten sind die statistische Analyse, der Datenabgleich und die Plausibilitätsprüfungen (Heinson et al. 2010, S. 76). Beispielsweise wie jede statistische Analyse, deutet auch diese statistische IT-Analyse auf jeweilige Abweichungen vom Normalverhalten hin. Diese Art der Analyse ermöglicht die Entdeckung von Anomalien in

Datenbeständen im Geschäftsleben eines Unternehmens und seinen Mitarbeitern. Diese Analyse gibt die Basis für weitere Untersuchungen. In der Praxis wird diese Methode sehr oft angewendet, z.B. bei Verdacht auf Kreditkartenbetrug oder Geldwäsche (Heinson et al. 2010, S. 76).

4.2.2. Datenintegrität

Für die Aufbewahrung des Images- und der Datenintegrität verwenden die Prüfer eine besondere „Einbahnstraße“ mathematische Funktion, die eine einzigartige Prüfsumme (Hashwert) bilden. Sobald jemand versucht, diese mathematische Funktion umzuschreiben oder zu ändern, ändert sich der Hashwert. Diese Änderung ist ein eindeutiges Alarmsignal für den Hasheigentümer, dass ein Dritter versucht hat in das System einzugreifen. Als gültiger Gerichtsnachweis kann nur der erste originale Hashwert dienen. Durch diesen Prozess wird die Datenintegrität und Richtigkeit gewährleistet. Die Änderung in nur einem Bit ändert die Information, wie in der nachfolgenden Abbildung gezeigt.

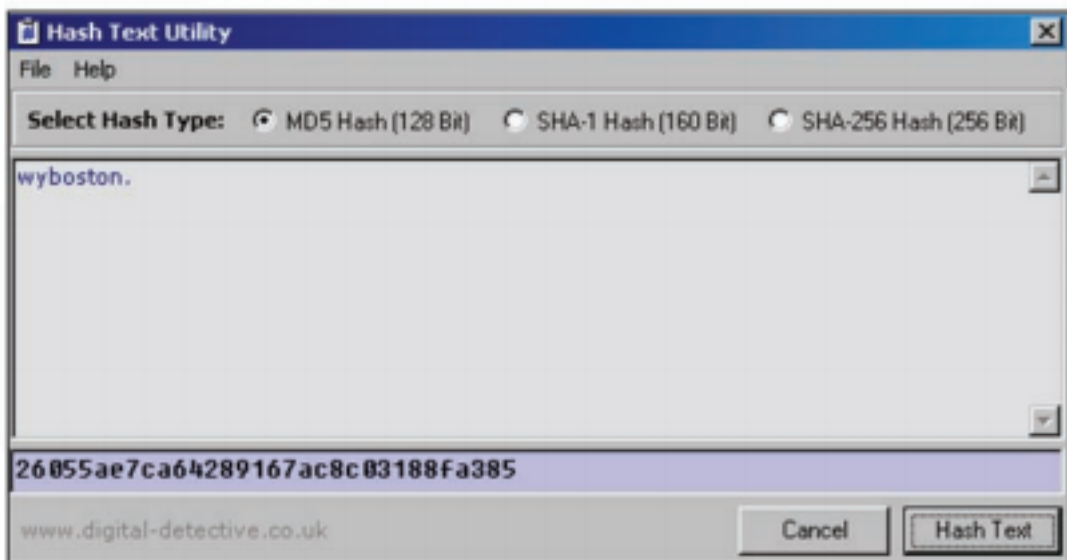
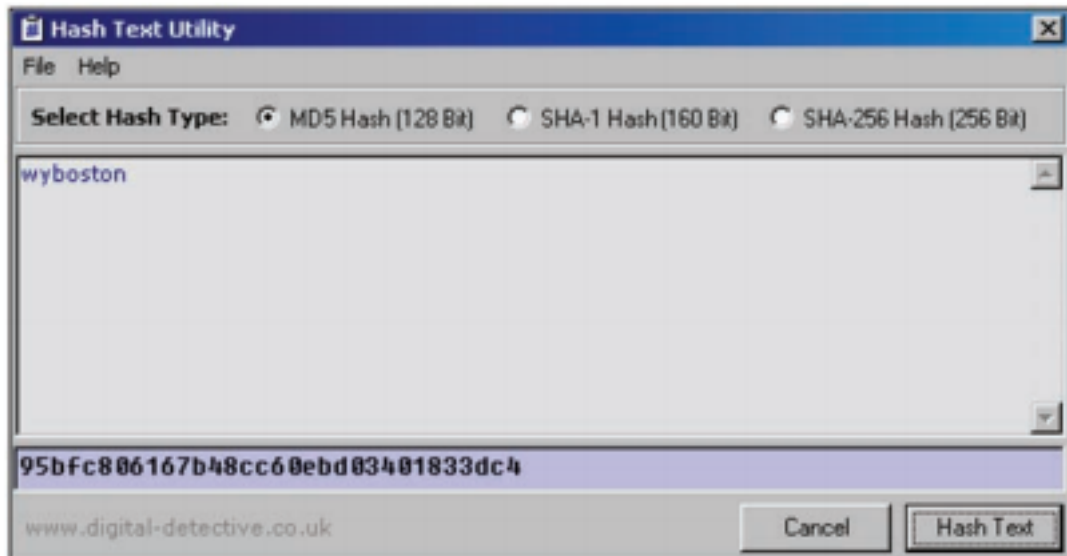


Abbildung 6- Hashsystem

(Milosavljevic & Grubor, 2009, S. 103)

Der Inhalt (der lange Code im unteren Teil) dieses Ordners ist komplett geändert worden, nachdem nur ein Punkt dazugeschrieben wurde (vergleiche: „wyboston" und „wyboston.").

4.2.3. Ausgewählte technische Berichte in Digitaler Forensik

Im folgenden Kapitel werden ausgewählte technische Berichte aus dem Berufsfeld „Digitale Forensik" vorgestellt. Hierbei geht es um Studien, die die Gefahren bei der Anwendung gewisser Technologien aufzeigen, die viele Menschen weltweit täglich nutzen. Die erste Technologie beinhaltet virtuelle Klienten, die den Studenten den Zugang zu den

Universitätsunterlagen auch von zu Hause ermöglichen, oder den Angestellten, in das Firmennetzwerk von Ferne einzusteigen. Die zweite Technologie sind die Solid-State-Disk (SSD) Karten, die in jedem neuen Rechner heutzutage als Standard eingebaut werden. Die dritte Technologie ist durch Handys gegeben.

4.2.3.1. Gefahr durch VPN-Clients

VPN oder „Virtual Private Network“ ermöglicht eine private Verbindung zu einem entfernten Server. Die Verbindung ist in der Regel kryptographisch abgesichert und wird durch das Internet abgewickelt. Die Kommunikation zwischen dem Rechner und dem Server basiert auf asymmetrischen Algorithmen, die es ermöglichen, dass sich die Rechner gegenseitig erkennen und authentisieren. Hierbei wird die Unversehrtheit der Verknüpfung durch die schon erwähnte Hashtag-Methode gewährleistet (die sogenannten „hashbasierten Message Authentication Codes“ (HMAC)). Manche VPN Lösungen sind kostenfrei und unterstützen unterschiedliche Plattformen (Windows OS, Linux, Mac OS). Das Verbinden via VPN ist meistens relativ einfach und zudem schnell (Jansen, 2016, S. 4-5).

VPN oder „Virtual Private Network“ wird heutzutage sehr oft benutzt. In der Arbeitswelt greifen die Mitarbeiter von zu Hause oder von Klienten auf das eigene Firmennetzwerk über VPN zu. Studenten können sich genauso von zu Hause in das Universitäts-Netzwerk einwählen, und z.B. online Universitätsbücher durchblättern. Statistiken zeigen, dass Menschen, wenn sie mit VPN bereits vertraut sind, dieses auch mindestens einmal pro Woche nutzen. Die folgende Abbildung zeigt die Anzahl der VPN-Nutzer im Vergleich zu der Anzahl der Internet-Nutzer (vpnMentor, 2017).

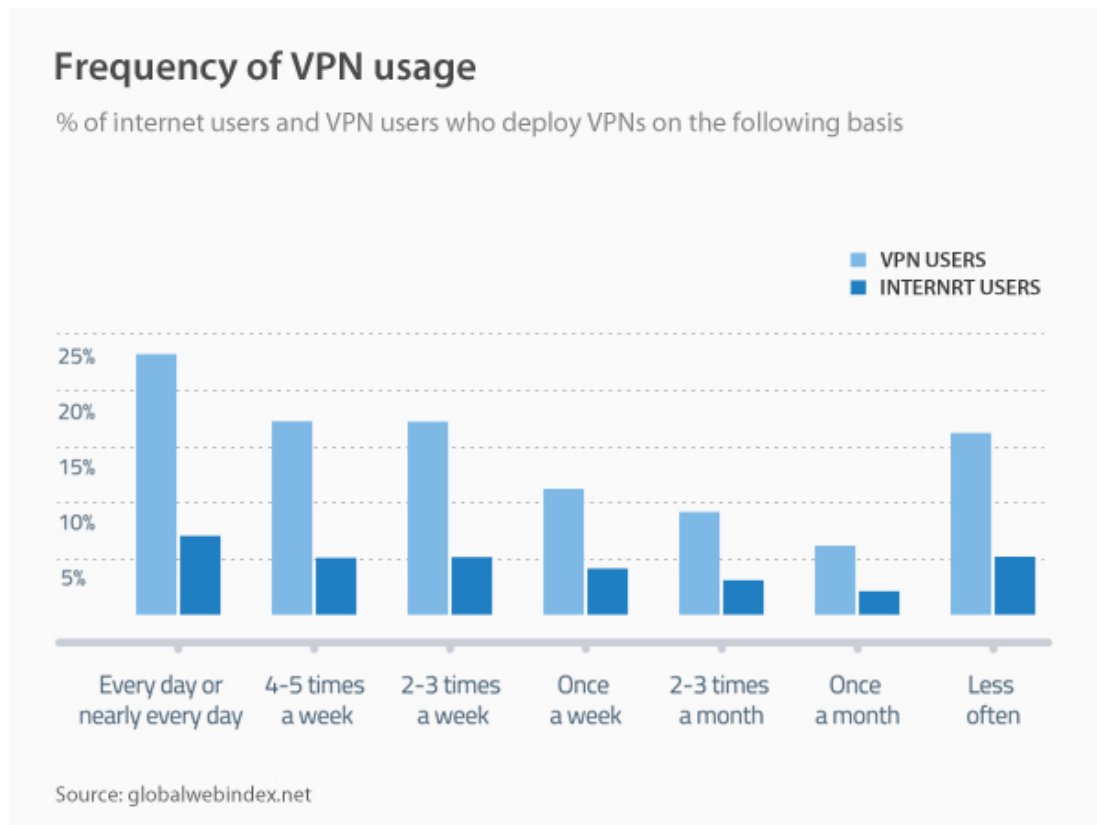


Abbildung 7- VPN

(vpnMentor, 2017)

Ein wichtiger Grund für die VPN-Nutzung ist, neben der schon bekannten Anwendung, auch die Möglichkeit, anonym im Internet zu surfen. Das reizt allerdings auch die Internet-Terroristen. Experten betonen, dass Täter oft VPNs nutzen, um unauffälliger Computerkriminalität betreiben zu können. Bevor der Täter eine konkrete Aktion beginnt, kann er eine oder mehrere aufeinander verbundene VPN-Server Verbindungen aufbauen und durch diese in das gewünschte Netzwerk einsteigen. Danach kann der Täter ohne Schwierigkeiten den Internet Proxy des betroffenen Unternehmensnetzwerks verwenden und die internen Daten wie gewünscht manipulieren. Die Verfolgung der Täter ist umso schwieriger, je mehr aufeinander bauende VPNs er für den Angriff verwendet hat. Ein weiteres Problem stellt die Auswertung der geklauten Daten dar. Da der Datenstrom bei VPN verschlüsselt ist, ist es unmöglich, genau zu bestimmen, welche Daten der Täter übertragen hat (Jansen, 2016, S. 5-6).

Eine der berühmtesten kostenfreien VPN-Clients, der OpenVPN, wurde dieses Jahr nochmals der Kontrolle unterworfen. WieTester berichten, hat sich herausgestellt, dass die Software viele große Fehler aufweist, obwohl sie in den letzten Jahren schon mehrmals

getestet wurde. Diese Fehler ermöglichen es den Tätern, eigene Codes in den VPN-Servern abzuspielen und diesen Server problemlos weiterhin zu verwenden. Die neuen Versionen vom OpenVPN sollen laut den Testern sicherer sein (der Standard, 2017).

4.2.3.2. SSD-Technologie und Digitale Forensik

Die neuen Festplatten, sogenannte SSD Festplatten, bieten einen Geschwindigkeitsvorteil im Vergleich zu den älteren Modellen von Festplatten (HDD – steht für Hard Disk Drive). Nutzer weltweit sind begeistert und mittlerweile sind fast nur SSDs in den neuen Rechnern eingebaut (Schadhauser & Graefen, 2017). Forensische Prüfer sind aber weniger begeistert von SSD als die Nutzer, da die SSDs ihre Arbeit wesentlich komplizierter machen, als die herkömmlichen Festplatten. Der Grund dafür liegt in der sogenannten „Garbage Collection“. Die Garbage Collection wird immer mit SSD in den Rechner eingesetzt, weil die Effizienz der Festplatte steigt, in dem sie die nicht benötigten Speicherteile löscht und für die neue Anwendung vorbereitet. Derzeit gibt es keine Möglichkeit diesen Prozess zu verhindern (Security Forum 2018, 2017). Das liegt in der Natur der SSD-Technologie: Jedes Mal, wenn etwas abgespeichert werden soll, muss der Speicherbereich komplett leer sein. Bei der alten Technologie konnte einfach der unbenutzte Speicher überschrieben werden. Ein weiterer Unterschied liegt in der Tatsache, dass mit dem Einsatz von Garbage Collection keine Information über die gelöschten Daten vorhanden ist. Früher waren die alten Daten immer noch vorhanden, auch wenn neue auf den gleichen Speicherbereich zusätzlich abgespeichert wurden. Für die Forensiker heißt das somit, dass die Implementierung von SSDs eine Unkenntnis über die gelöschten Daten mit sich bringt und daher ist die Wiederherstellung schwer, oder sogar nicht vollständig (PWC Global, 2015).

4.2.3.3. Digitale Analyse von Smartphones

Smartphones werden einfacher als Rechner zum Opfer eines Cyberangriffs und stellen somit für viele Unternehmen einen richtigen Albtraum dar. Das späte Entdecken von solchen Angriffen ist noch ein zusätzliches Problem für die betroffenen Unternehmen. Im Durchschnitt werden 210 Tage benötigt, um einen Cyberangriff auf ein Handy zu entdecken. Deswegen sind Handys beliebte Angriffsziele vieler Cyberterroristen. Viele Menschen nutzen Firmenhandys auch privat. Das führt zu einer Systemvielfalt, unterschiedlichen gespeicherten Daten und Verschlüsselungen. Um eine richtige Analyse durchzuführen, müssen forensische Experten in diesem Fall eine wesentlich umfassendere Analyse durchführen, als wenn die Handys nur als

Firmenhandys genutzt werden, weil Handys in diesem Fall eine Menge an Fotos, Apps, Notizen, Passwörter, verwendeten Netzwerken, drahtlosen Internetverbindungen, Textnachrichten, Browser-Cookies, etc. enthalten (Schonschek, 2013).

Es gibt mehrere Möglichkeiten, wie Handyangriffe entdeckt werden können. Beispielsweise kann über das Forensik-Tool „EnCase Forensic 7“ durch das Netzwerk in das betroffene Handy eingestiegen und die Untersuchung durchgeführt werden. Dieses Tool sammelt dann, alle verdächtigen Daten aus dem Arbeitsspeicher und der Festplatte zentral. Das Tool kann auch Datenkopien machen. Alle Änderungen und Manipulationen würden den schon erwähnten Hashcode ändern. Weitere Tools sind: Secure View 3, Fixmo Sentiel, Paraben Device Seizure, oder manche an das bestimmte Gerät angepasste Tools wie z.B. Elcomsoft Blackberry Backup Explorer. Im nächsten Paragraph wird eines der Tools beschrieben: Secure View 3 (Guidance Software (Webinar), 2017).

Secure View 3 ist mit mehreren Zusatzmodulen als ein umfangreicher Kit verfügbar. Mit Hilfe dieses Tools kann man ein mobiles Gerät (Handy oder Tablet) detailliert überprüfen, oder sogar die Berichte aus mehreren verknüpften Geräten ziehen und konsolidieren. Weiterst ist es möglich, alle gelöschten Daten wiederherzustellen. Das ist eine sehr wichtige Funktion, da dadurch bspw. auch die gelöschten Fotos wiederhergestellt werden können. Die Fotos haben versteckte Metadaten, die beispielsweise den Standort verraten. So können die Forensiker nachvollziehen, wo genau sich der Handynutzer bewegt hat. Die komplizierten Passwörter stellen kein Hindernis für dieses Tool dar- alle Passwörter können geknackt werden. Sogar die gelöschten Apps können entdeckt werden. Die spezifischen Zusatzmodule sind notwendig, um ein bestimmtes Gerät gut prüfen zu können (z.B. Elcomsoft Blackberry oder Elcomsoft iOS).

Hierbei ist aber wichtig darauf zu achten, dass sogar die forensischen Prüfer diese Tools nur nutzen können, wenn ein konkreter Verdachtsfall vorliegt. Ansonsten können solche Untersuchungen gegen die Datenschutzbestimmungen stoßen. Ein zusätzliches Problem liegt in der Tatsache, dass diese Tools nicht nur für Forensiker, sondern auch für Angreifer attraktiv sind, da sie mit Hilfe dieser problemlos Cyberangriffe durchführen können (Schonschek, 2013).

4.2.4. Qualitätsfaktoren der Forensik

Immer wenn eine Organisation mit einem potentiellen Systemangriff konfrontiert ist, steht sie vor dem moralischen Problem „wem zu vertrauen und wem die Untersuchung zu überlassen“. Oft mangelt es dem internen Team für Datensicherheit an Erfahrung, Kenntnissen und Anwendungen, sich mit solchen Problemen auseinanderzusetzen. Es kann sogar zu Datenbeschädigungen kommen. Deswegen werden externe digitale forensische Prüfer als Unterstützung hinzugezogen. Diese sind verpflichtet, das Unternehmensgeheimnis zu bewahren und, nach Absprache mit dem Management, an die zuständigen Behörden zu berichten. Die forensische Untersuchung besteht aus:„

- Erstellung solider digitaler Beweise, die für das Gericht akzeptabel sind
- Nachweis der Herkunft von E-Dokumenten und Untersuchung bei deren Authentifizierung
- Rekonstruktion von Ereignissen mit gespeicherten und computergenerierten Beweisen und Analyse der Zeitlinie des Angriffs
- Trojanische Verteidigung
- Minimierung der Auswirkungen der Folgen des Angriffs
- Analyse der Internetgeschichte und Registerdatenbank
- Verknüpfung digitaler Beweise, um den Fall vor Gericht beweisen zu können
- Erstellung digitaler Beweise (XII Medjunarodni naucni skup sinergija: "Kvalitet-put u Evropu", 2013, S. 61).“

Ein gutes forensisches Team kann unterschiedliche Leistungen anbieten. Neben der Entdeckung von versteckten Informationen aus diversen Quellen (Chats, Messages, E-Mails), kann das Team auch die beschädigten Daten wiederherstellen. Weiterst bieten forensische Teams eine Art von Unternehmensberatung. Das betroffene Unternehmen und seine Mitarbeiter werden auf die Situation besser vorbereitet und können hoffentlich die nächsten Drohungen rechtzeitig erkennen (IT Service, 2018).

Eine konstante Kooperation zwischen den forensischen Prüfern und dem betroffenen Unternehmen ist sehr wichtig, um eine effiziente Lösung zu finden. Das Management sollte um passende Arbeitsbedingungen für die Forensiker bemühen und ihnen möglichst viele Informationen zur Verfügung stellen. Gleichzeitig sollen die Prüfer dem Management regelmäßig Auskunft darüber geben, was sie machen und wie sie es machen. Dadurch wird

die Zusammenarbeit stabiler und effizienter, was eine Win-win-Situation für beide Parteien darstellt (XII Medjunarodni naucni skup sinergija: „Kvalitet-put u Evropu“, 2013, S. 61-62).

4.2.5. Mathematische Studie zur Forensik

Diese Studie wurde 2017 in Deutschland durchgeführt, mit dem Ziel, das Bewusstsein der Menschen und Unternehmen zu verstärken, inwiefern neue Technologien gefährlich sein können. Bekannte Fälle (Sony Playstation Netzwerk⁷, EMC Corporation⁸) zeigen das kein Unternehmen hundertprozentig vor einem Angriff geschützt ist. Auch wenn die Unternehmen glauben, sie seien nicht attraktiv für Angreifer, können sie leicht in die Angriffskralen fallen. Die IT-Angriffe sind oft unsichtbar und verbreiten sich schnell. Ein Beispiel wäre der "Stuxnet-Wurm", ein Computervirus, der die Rechner des Atomkraftwerks im Iran angesteckt hat, und sich aus dem Iran gleich nach Europa, Indonesien, Indien und USA verbreitet hat. Der Virus konnte alle Maschinen und Werke kontrollieren. Die Anti-Virus-Firmen Experten meinten, es sei eine „Zeit des Cyberterrorismus, der Cyberwaffen und der Cyberkriege (Welt.de, 2010).“ Bei solchen Angriffen können enorme Schäden entstehen. Nicht nur materielle Verluste machen die Unternehmen unsicher, sondern auch der potentielle Kundenverlust und ein schlechter Ruf, den sie bekommen würden. Die digitale Forensik bietet Lösungen, solche Angriffe aufzuklären und die Täter zu verfolgen. Diese Studie zeigt auf, wie viele deutsche Unternehmen sich bereits darüber bewusst sind, dass sie ein potenzielles Angriffsziel sind und was sie dagegen machen. Weitere Fragen, die durch diese Studie beantwortet werden, sind der Zweck der digitalen Forensik in Unternehmen, der Bezug zum IT-Management, und was die Unternehmen am Einsatz digitaler Forensik hindert (Meier & Pernul, 2017, S. 103-106).

Die Ergebnisse basieren auf einem Fragebogen mit 21 Fragen und wurden von 69 deutschen Unternehmen geliefert. Erstmals wurde die Anzahl der Mitarbeiter bzw. die Unternehmensgröße in Verbindung mit dem jährlichen Budget für die IT-Sicherheit in Verbindung gebracht. Prinzipiell waren die Budgethöhen im Einklang mit der Unternehmensgröße. Die zweite und dritte Frage versuchen zu erklären, wie viele

⁷ Angriff auf die Online-Community / den Online-Marktplatz für die Sony Playstation Spielekonsole, bei dem persönliche Daten von 77 Mio. Kunden erbeutet wurden (Hirai, 2011).

⁸ Angriff auf das interne System der Cybersicherheitssparte von EMC Corporation, bei dem sensible Daten über die Funktionsweise von Sicherheitsprogrammen (eingesetzt unter anderem bei Unternehmen und Regierungen) erbeutet wurden (Markoff, 2011).

Unternehmen schon Forensik-Maßnahmen implementiert haben, und wie viele die Implementierung vorhaben.

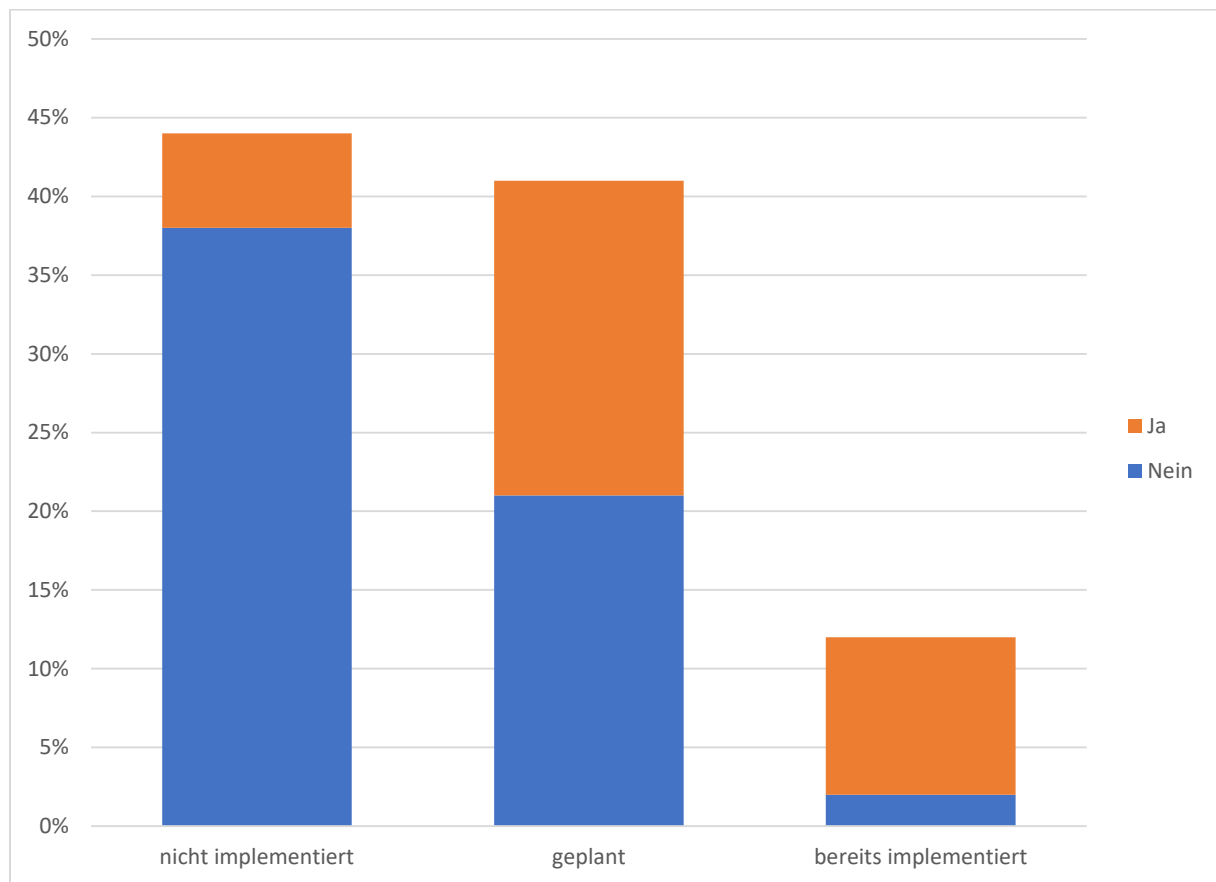


Abbildung 8- Forensikmaßnahmen Implementierung

(Meier & Pernul, 2017, S. 108)

Die drei Balken stellen drei Zustände dar- Digitale Forensik bzw. „Forensic Readiness“, wie sie in der Studie benannt wird, ist komplett irrelevant in Unternehmen (Balken 1), oder ist die „Forensic Readiness“ bekannt und wird implementiert (Balken 2), oder ist die „Forensic Readiness“ schon implementiert worden (Balken 3). Die Antworten sind in einer kombinierten Form dargestellt. Die Studie basiert auf einer einfachen Frage: „Wurde in Ihrem Unternehmen schon eine forensische Untersuchung durchgeführt?“. Die anderen Fragen folgen, in Abhängigkeit von der ersten Antwort und die Prozentsätze von dem ersten Balken werden im richtigen Verhältnis auf den zweiten Balken übertragen. Aus der Grafik kann geschlossen werden, dass mehr als 50% der befragten Unternehmen nicht vorhaben, eine forensische Untersuchung durchzuführen und, dass 15% die Untersuchungssysteme bereits implementiert haben.

Das weitere Untersuchungsgebiet basierte auf der Frage: „War Ihr Unternehmen schon ein Opfer des IT-Angriffes?“. Von befragten Unternehmen, haben 40% positiv auf diese Frage geantwortet. Leider war es der Studie unmöglich nachzuweisen, dass Unternehmen mit höheren Ausgaben für IT-Sicherheit auch tatsächlich sicherer sind.

Es wurde ebenso untersucht, mit welchem Ziel die Unternehmen überhaupt IT-Sicherheiten einbauen. Die meisten haben zugegeben, dass sie sich um die IT-Sicherheit erst nach einem Angriff kümmern, um die Täter möglicherweise zu identifizieren. Die andere große Gruppe waren die Unternehmen, die die Angriffe analysieren wollten. Manche haben gesagt, dass sie IT-Sicherheiten nutzen, um Verstöße gegen Firmenrichtlinien verfolgen zu können.

Interessant war herauszufinden, wieso die Unternehmen digitale forensische Maßnahmen nicht implementiert haben. Die meisten haben zugegeben, dass sie keine Finanzmittel für solche Investitionen haben. Die anderen behaupten, zu wenig Know-how und Erfahrung zu haben, und daher sei die Implementierung sinnlos. Für viele ist das Thema „digitale Forensik“ komplett unbekannt. Einige behaupten, digitale Forensik sei für ihr Unternehmen nicht geeignet. Die folgende Abbildung zeigt die Anzahl der befragten Unternehmen und ihre Antworten (Meier & Pernul, 2017, S. 103-111).

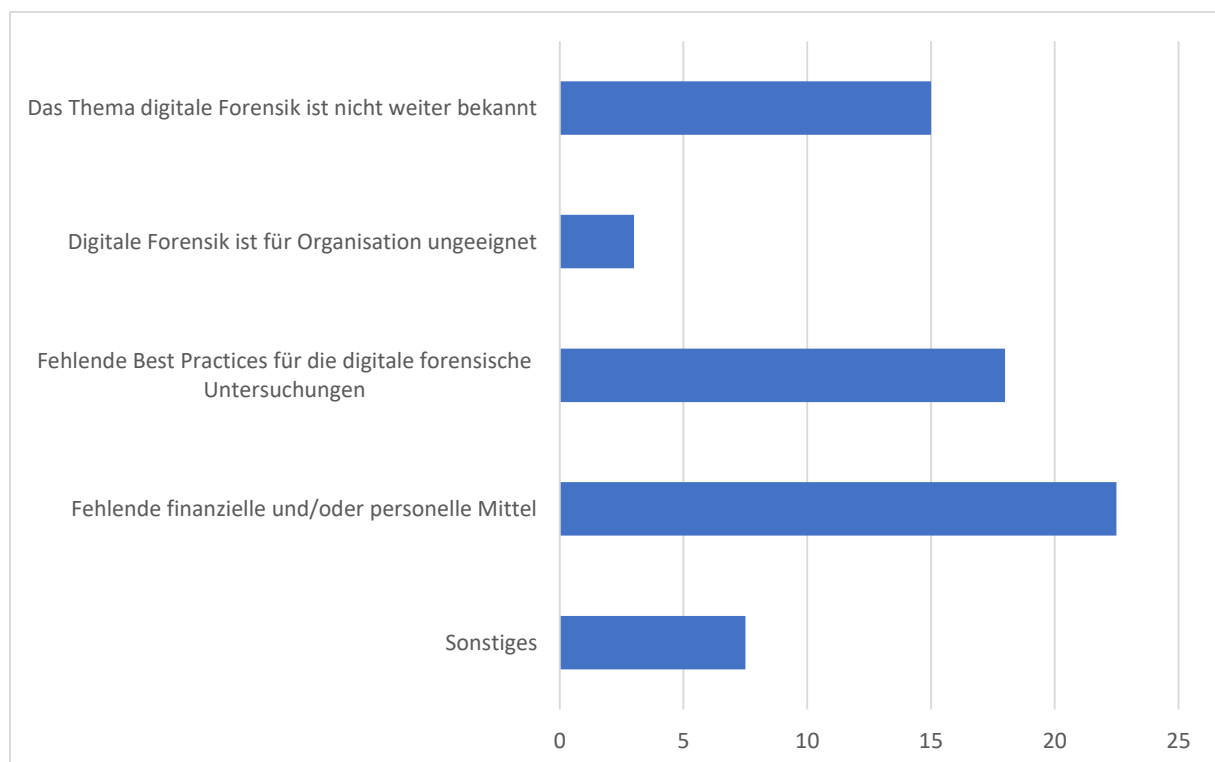


Abbildung 9- Interesse an Forensik

(Meier & Pernul, 2017, S. 111)

4.2.6. Zukunft digitaler Forensik

Die neuen Technologien bringen für Unternehmen große Entwicklungspotentiale, aber gleichzeitig für Betrüger die immer besseren Betrugsmöglichkeiten. Die betrügerischen Tätigkeiten werden immer mehr verfeinert und, wie schon erwähnt, die klassische interne Kontrolle kann sie nicht alleine bekämpfen. Die großen Unternehmensbetrüge werden durch das ganze Netzwerk von Mitarbeiter und unternehmensexternen Personen entwickelt. Die Betrugsmuster werden immer komplizierter zu erkennen (SAS Institute Inc., 2017). Die forensische Rechnungslegung und die digitale Forensik sind weitere Schritte bei der Betrugaufdeckung. Aber die Technologie entwickelt sich extrem schnell weiter, und es kommen immer wieder Begriffe wie „Robotics“ oder „maschinelles Lernen“ in den Umlauf. Es stellt sich die Frage, ob forensische Rechnungslegung den neuen Trends folgen kann und noch besser werden könnte als bis dato.

Beispielsweise wird im Bankenwesen sehr viel Wert auf schnelle und sichere Transaktionen gelegt. Es steigt die Tendenz, alle Prozesse die als hochriskant einzustufen sind, zu automatisieren. Hierbei geht es um die Identifizierung neuer Kunden und Geschäftspartner („Know Your Customer“ Tätigkeiten), Automatisierung der Geschäftsprozesse, E-Banking, etc. Durch die intelligente Automatisierung sollen die operationellen Risiken beseitigt werden. Sogar Geldwäscherisiken könnten reduziert werden. Neben dem Bankwesen, sind die anderen Industrien an der Automatisierung zutiefst interessiert (Capco, 2017, S. 142).

Die unterschiedlichsten Softwarehersteller bieten die automatisierten Lösungen für Unternehmen, wodurch die Risiken minimiert werden können. Beispielsweise bietet die Firma „SAS“ die Unterstützung für das gesamte Risikomanagement. Ihre Software deckt die ganze Prozesskette von Datensammlung, über Risikoauswertung bis auf das Meldewesen. SAS Software kann mit Hilfe von Data Mining⁹ die großen unterschiedlichen Datenmengen analysieren (z.B. Markt- oder Kundendaten, Kennzahlen, Messgrößen, ...). Alle Daten werden dann strukturiert gesammelt und ausgewertet, so dass sie für Risikosteuerung nutzbar sind und gleichzeitig revisionskonform, relevant und zuverlässig sind. Keine Prozessaktivität wird ausgelassen und menschliche Fehler oder absichtliches betrügerisches Benehmen wird somit ausgeschlossen: Alle Unregelmäßigkeiten werden mit Sicherheit bemerkt. Die Rechtsverstöße

⁹ Data Mining beschreibt die systematische Anwendung von Algorithmen auf große Datenmengen (Big Data) um daraus Muster und Verbindungen abzuleiten (Fayyad, Piatetsky-Shapiro, & Smyth, S. 39).

können nicht mehr unbemerkt passieren. Wenn die Software ein betrügerisches Benehmen entdeckt, können sich die forensischen Rechnungsprüfer mit dem gewählten Sachverhalt im Detail beschäftigen und die weitere Analyse durchführen. Außerdem sind die Informationen immer auf dem neusten Stand, weil die Software 24 Stunden am Tag aktiv sein kann und regelmäßige Prüfungen durchführen kann. Zusätzlich werden die Risikomanagementkosten in Unternehmen reduziert, da die Menschen nicht mehr die Prozessketten untersuchen müssen, sondern die Software diese Tätigkeiten schnell und präzise übernehmen können. Dadurch wird an Personalkosten gespart und die Unternehmen können dieses Geld in die Bekämpfung der weiteren Betrugsmechanismen investieren (SAS Risk Management, 2017).

Eine besondere, neue und interessante Tendenz in der Wirtschaftswelt ist die Entwicklung der Roboter (engl. „Robotics“ oder „RPA“ bzw. Robotic Process Automation). Hierbei geht es wiederum um die Softwarelösungen, die Menschen ersetzen sollen und dadurch die Prozesse beschleunigen können, da eine Software nicht schlafen muss, nicht müde wird und keine persönliche Interessen im Vordergrund stehen. Der Einsatz der RPA Technologie ist in vielen Unternehmensbereichen gut vorstellbar- Kapitalmärkte, Gesundheit, Verkauf, Telekommunikation, Versicherung, Bankwesen, Produktion. Die Roboter können die Menschen ersetzen und bei vielen Tätigkeiten unterstützen, die leicht dem Betrug unterliegen: z.B. Bestellungsprozesse, Identität der Kunden, Rechnungserstellung und Freigabe, präzise Geldflussrechnungen, operationale Effizienz, Meldewesen, Risikoüberwachung, etc. Alle diese Tätigkeiten können die Menschen leicht manipulieren und durch den Einsatz der Roboter wird das Risiko der Manipulation ausgeschlossen (Capco, 2017, S. 107).

Eines der Unternehmen, die sich mit dem Thema „Automatisierung“ in letzter Zeit stark auseinandergesetzt haben und gut in diesem Markt etabliert ist, ist „NICE“. Dieses Unternehmen legt seinen Fokus spezialisiert auf Finanzbetrug und Compliance. Es wird betont, dass die Unternehmen ihre Software mit schon bestehender Unternehmenssoftware kombinieren können und mit lediglich kleinem Aufwand einen großen Schritt in Richtung Sicherheit und Betrugsbekämpfung machen können. Die Software ermöglicht es dem Anwender, die kriminellen Tätigkeiten zu entdecken, Betrug zu vermeiden und gleichzeitig alle Compliance- und Meldeverpflichtungen rechtzeitig zu erfüllen. Man unterscheidet zwischen zwei Varianten der Softwarelösung- „begleitete“ und „nicht begleitete“. Bei dem ersten Typ, müssen sich die Mitarbeiter aktiv an der Recherche beteiligen und mit dem Robot

zusammenarbeiten, aber ihre gesamte Arbeitsauslastung wird reduziert und Fehleranzahl reduziert. Die nicht begleitete Variante entlastet die Mitarbeiter wesentlich mehr als die erste Variante, da sie die Roboter nur am Anfang programmieren müssen. Alle weiteren Tätigkeiten werden dann selbstständig vom Roboter durchgeführt. Die Prüfer müssen sich nicht mehr mit dem ganzen Unregelmäßigkeitsentdeckungsprozess beschäftigen, sondern können sich auf die detaillierte Untersuchung der, durch die Software entdeckten Problemgebieten, konzentrieren. Das Konzept ist als eine extreme Effizienzsteigerung und Kostenersparnis für Unternehmen aller Branchen gedacht. Es ist vorgesehen, dass die Einsetzung solcher Software einer Effizienzsteigerung der Prüfer um 50% bringen wird (NICE, 2018).

Ähnlich wie im Kapitel „Aufbewahrung der Datenintegrität“ beschrieben, hat sich die Technologie „der Kette“ stark geändert und verbessert. Die neuen „Ketten“, die Betrug verhindern sollen, sind unter dem Namen „Blockchain“ der Öffentlichkeit vorgestellt. Blockchain erfüllt eine der Hauptanforderungen jeder Industrie – Berichterstattung und Dokumentation. Man kann jederzeit und umgehend alle gewünschten Informationen aus der Kette abrufen und prüfen. Somit ist die zweite Fähigkeit des Blockchains die Überwachung der Prozesse (Capco, 2017, S. 12). Blockchain kann man sich als eine Kette bestehend aus Blöcken vorstellen. Jeder Block enthält eine oder mehrere Transaktionen, aber jeder Block ist inhaltlich verknüpft an den vorigen und nächsten Block. Wenn jemand Inhalt eines Blocks ändern würde, passt die Kette nicht mehr zusammen. Das ist ein klares Zeichen, dass es zu nachträglichen Änderungen gekommen ist und, dass ein Betrug potenziell vorliegt. Blockchain kann man als eine „selbständige Prüfungseinheit“ oder „Prüfung in sich“ bezeichnen (Capco, 2017, S. 77).

5. Conclusio

5.1. Diskussion und Schlussfolgerungen

Die eingangs gestellte forschungsleitende Fragestellung: *„Welche Rolle spielt die forensische Rechnungsprüfung bei der Untersuchung eines Finanzbetrugs in Großunternehmen?“* konnte erfolgreich beantwortet werden:

Vertrauen ist in jeder langfristigen Geschäftsbeziehung unerlässlich. Korruptionen und Betrugsfälle in Unternehmen aber auch im Wirtschaftssystem allgemein führen unweigerlich zum Vertrauensverlust. Die Rolle, die dabei von der forensischen Rechnungsprüfung

eingenommen wird, ist äußerst wichtig: Forensische Rechnungsprüfer sind diejenigen, die Schwachpunkte im Unternehmen aufdecken, analysieren und bekämpfen. Wird bereits ein Betrugsfall auch nur vermutet, treten sie in Aktion und sorgen für Transparenz und ausreichend Information. Ihre Haupttätigkeit besteht darin, Kriminalität und Betrugsfälle im Unternehmen aufzudecken und dann Beweise zu sammeln, die vor Gericht für die Überführung der Täter verwendet werden können. Analyse, Interpretation und das Zusammenfassen komplexer Geschäfts- und Finanzangelegenheiten sind die Tools, die dabei von ihnen angewendet werden.

Viele Missbräuche treten auf, weil die Geschädigten keinen Zugang zu den gleichen Informationen haben, die die auch Täter besitzen. Dies ist oft dann der Fall, wenn Betrugsfälle eintreten, die von der Unternehmensleitung zum Nachteil der Aktionäre, Investoren und Gläubiger durchgeführt werden. Zahlreiche Investitionsbetrüge und Missbräuche der Führungskräfte umfassen die Informationsvertuschung vor den potenziell Geschädigten. Ein angemessener Schutz gegen solche Missbräuche ist die Aufforderung an die Unternehmensleitung zur vollständigen Veröffentlichung der Informationen, einschließlich der überarbeiteten Jahresabschlüsse, Geschäftsgeschichte und anderen Daten, welche die Unregelmäßigkeiten offenlegen würden.

Die Unternehmen sind zur Implementierung von Programmen und Kontrollen verpflichtet, die das Auftreten von Betrugereien verhindern und durch die interne und externe Wirtschaftsprüfung bewertet werden. Obwohl in den meisten Unternehmen bereits bestimmte Verfahren zum Umgang mit diesem Problem bestehen, wie z.B. die Verabschiedung der Geschäftsordnung und des Ethik-Kodex, ist es notwendig, dass die Programme zur Aufdeckung und Verhinderung von Betrugsfällen verbessert werden, um den neuen gesetzlichen Anforderungen gerecht zu werden.

Die Aufgabe des forensischen Wirtschaftsprüfers ist es, in jeder Berichtsperiode, die Angemessenheit der Funktionsweise des internen Kontrollsystems zu überprüfen und die zuständigen Behörden über alle Mängel des Systems zu verständigen. Sein Augenmerk liegt besonders auf der Erkennung von Warnhinweisen, welche als Indikatoren für die Existenz von rechtswidrigen Handlungen sein können. Jeder Verdacht, dass in der Organisation ein Betrug begangen wurde, wird zu einer weiteren Untersuchung durch den internen Wirtschaftsprüfer

führen, und falls sich die Notwendigkeit dafür ergibt, zur Beauftragung von externen Experten wie den forensischen Rechnungsprüfern.

Der forensische Prüfer bewertet, ob Kontrollen zur Verhinderung, Identifizierung und Aufdeckung von Betrug im kontrollierten Umfeld bestehen, die häufig einen erheblichen Einfluss auf das Betrugsrisiko haben. Dementsprechend ist das mangelnde Engagement und eine mangelnde Überwachung dieser Prozesse durch die verantwortlichen Personen ein starker Indikator für das Bestehen eines größeren Betrugsrisikos im Prozess der Finanzberichterstattung.

Finanzielle Untersuchungen umfassen ein breites Spektrum an Aufgaben, wofür die forensischen Buchhalter beauftragt wurden, um herauszufinden, warum die finanziellen Ergebnisse oder Verhaltensweisen von den erwarteten Normen deutlich abgewichen sind, sowie um die Auswirkungen eines solchen Verhaltens zu quantifizieren. Die häufigsten Aufgaben in der Finanzkriminalität liegen im Bereich der betrügerischen Finanzberichterstattung, der Aneignung von Vermögen, der Erlangung von finanziellen Vorteilen aus den betrügerischen Vermögenswerten und dem Handeln mit Insidern.

Der Grundzustand im Rechnungswesen und in der Wirtschaftsprüfung ist von grundlegender Bedeutung, da diese Disziplinen die Grundlage für den spezialisierten Ansatz des forensischen Buchhalters bieten. Die forensische Buchhaltung wird allgemein als der am schnellsten wachsende Sektor im Rechnungswesen anerkannt, und dieses Wachstum zeigt keine Tendenzen kurzfristiger bzw. langfristiger Abnahme.

Im heutigen Geschäftsbetrieb sind die forensischen Buchhalter zum Bestandteil aller bedeutenden Wirtschaftsprüfungsgesellschaften geworden, die auf die Aufdeckung von Betrügereien sowie die Unterstützung von Gerichten spezialisiert sind, indem sie Nachweise über finanziell betrügerische Geschäfte vorlegen. Gerichte sind abhängig von der Fachkenntnis der forensischen Buchhalter in allen Finanzangelegenheiten und Streitigkeiten. Sie werden für alle Untersuchungen, Zusammenschlüsse und Übernahmen, als Ermittler im Bereich der Wirtschaftskriminalität benötigt. Somit ist die Rolle des forensischen Prüfers zu einer hochspezialisierten Funktion geworden.

Abschließend werden weitere Entwicklungen in diesem Berufsbereich dargelegt und auf die Limitationen dieser Arbeit kurz eingegangen.

5.2. Ausblick

Diskussionsbedarf für die Entwicklung und Beeinflussung der Wirtschaftsprüfung, liefern technologische Entwicklungen aber auch Innovationen wie etwa Blockchain (Capco, 2017, S. 77). Die Fragen reichen sogar bis zu einer vollständigen Ersetzung des etablierten Systems durch diese. Ein weiterer Standpunkt geht jedoch davon aus, dass die Wirtschaftsprüfung ein tiefes Verständnis voraussetzt und, dass keine Maschine oder Roboter fähig ist, in dieser Hinsicht die Menschen zu ersetzen. In diesem Fall stellen die Automatisierungsprozesse nur eine Verstärkung des Menschen dar und diese können sich auf die Betrugsursachen und eine tiefgehende Analyse dieser konzentrieren (Capco, 2017, S. 80). Die technologische Entwicklung lässt sich nur in den seltensten Fällen aufhalten. Rechnungsprüfer stehen nun vor der Entscheidung diese Technologie für sich zu Nutze zu machen oder von ihr gänzlich ersetzt zu werden. Die größte Herausforderung für Prüfer wird sein, sich möglichst schnell an die Änderungen anzupassen (ICAEW, 2018).

Diese großen Veränderungen betreffen auch eine große Gruppe von Menschen. Nicht nur die Prüfer müssen sich an die Trends anpassen, sondern alle, die Interesse am Unternehmen haben. Nur ein starker Zusammenhalt kann der Gefahr entgegenwirken, dass die Bedeutung der menschlichen Arbeit in der Wirtschaft verloren geht. Besondere Verantwortung liegt bei den großen Prüfungsgesellschaften, wenn es darum geht sowohl in die Entwicklung neuer Technologien zu investieren, aber auch darum ihre Mitarbeiter stetig auf dem neusten Entwicklungsland zu halten. Hierbei ist nicht nur wichtig, dass neue Technologien angewendet werden können, sondern auch, dass zudem potentielle neue Risiken entdeckt werden, die in Folge neuer Geschäftsmodelle und Software entstehen können. Diese komplexen Sachverhalte dürfen dabei nicht außer Acht gelassen werden (ICAEW, 2018; Rausenberger & Prenrecaj, 2017).

Im Gegensatz zu Großunternehmen, die es möglicherweise nicht schaffen, alle Änderungen zu koordinieren und dadurch das Tempo verlieren, besteht bei kleinen und mittleren Betrieben die Gefahr, dass sie aus finanziellen Gründen den Trends nicht folgen können. Es ist deswegen besonders wichtig, dass jedes Unternehmen ein Bewusstsein dafür entwickelt, mit welcher Vorgehensweisen und mit welchen Strategien es sich am besten im Markt positionieren kann (ICAEW, 2018).

Für den Beruf des Rechnungsprüfers bedeuten diese Veränderungen neue Herausforderungen. Sie müssen sich auf dem aktuellsten Informationsstand halten und ihre Kenntnisse und Fähigkeiten ständig weiterentwickeln. Somit ändern sich die Arbeitsprofile der Prüfer und anderer Wirtschaftler in den nächsten Jahren. Die zukünftigen Prüfer müssen noch mehr Fähigkeiten besitzen als bisher, weil es nicht nur um logische Denkweise und Rechnungslegungskenntnisse geht, sondern ein tiefes Verständnis von Informationstechnologien notwendig ist. Manche Prüfungsgesellschaften suchen schon jetzt nach solchen Berufsprofilen und investieren konsequent in deren Weiterbildung. Eine flexible, schnelle, höchstqualitative und agile Wirtschaftsprüfung ist in der absehbaren Zukunft zu erwarten (ICAEW, 2018; Finance-Magazin Deutschland, 2017).

5.3. Limitationen der Arbeit

Bei der Durchführung dieser Arbeit wurde festgestellt, dass nur ein geringer Zugang zu aktuellen empirischen Materialien möglich war, da es sich bei diesen um sensible Daten handelt, die aufgrund von Datenschutzgesetzen von den Unternehmen nicht zur Verfügung gestellt werden und dadurch diese Studie zum Teil limitieren. Zudem kommt hinzu, dass sich die forensische Rechnungsprüfung nur schwer von anderen wirtschaftsprüfenden Bereichen abgrenzen lässt und dadurch nicht klar definierbar ist. Aber globale Entwicklungen und Anforderungen der Wirtschaft lassen vermuten, dass sich diese in Zukunft verändern werden. Weitere Studien können zeigen, welche Auswirkungen dies nicht nur auf die Prävention von Betrugsfällen, sondern auch auf das Bewusstsein von Unternehmen im Betrugsbereich haben wird.

Literaturverzeichnis

- § 268 UGB. (14. 12 2017). *Jusline: § 268 UGB Pflicht zur Abschlußprüfung*. Abgerufen am 14.12.2017 von <https://www.jusline.at/gesetz/ugb/paragraf/268>
- §243 UGB Lagebericht. (kein Datum). Von <https://www.jusline.at/gesetz/ugb/paragraf/243> abgerufen am 10.02.2018
- ACFE (Report to the nations). (2016). *Report to the nations*. Von <http://www.acfe.com/rtn2016/docs/2016-report-to-the-nations.pdf> abgerufen am 04.01.2018
- Aghion, & Durlauf. (2005). *Handbook of Economic Growth*.
- AICPA. (2011). Von <https://www.aicpa.org/InterestAreas/ForensicAndValuation/Resources/PractAidsGuidance/DownloadableDocuments/2011%20FVS%20Trend%20Survey.pdf> abgerufen am 10.01.2018
- AICPA. (2018). *Statements on Auditing Standards*. Von <https://www.aicpa.org/research/standards/auditattest/sas.html#SAS84> abgerufen am 15.12.2017
- Albrecht, Albrecht, Albrecht, & Zimbelman. (2009). *Fraud Examination* . USA.
- Aleksic. (2012). *Revizija i Kontorla*. Banja Luka.
- Aleksic. (2015). Uloga i znacaj forenzickog racunovodjstva u otkrivanju finansijskih prevara. *Casopis za ekonomiju i trzisne komunikacije, Godina V, Broj II*.
- Amtsblatt der Europäischen Union . (17.05.2006). Abgerufen am 19.12.2017 von http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=uriserv:OJ.L_.2006.157.01.0087.01.DEU
- Amtsblatt der Europäischen Union. (26.10.2005). *RICHTLINIE 2005/60/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES*. Abgerufen am 08.12.2017 von <http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32005L0060>
- Anti Money Laundering & Counter Financing of Terrorism. (2018). Von <http://amlcft.bnm.gov.my/AMLCFT05a.html> abgerufen am 12.02.2018
- Arbeiterkammer Österreich. (2017). Abgerufen am 15.12.2017 von https://wien.arbeiterkammer.at/service/betriebsrat/ifamaufsichtsrat/ifamneu/Risikomanagement_und_internes_Kontrollsystem.html
- Aschermann. (2014). *CHIP.de*. Von https://praxistipps.chip.de/was-ist-malware_28542 abgerufen am 15.01.2018
- Audit Committee Institute. (2007). Von https://audit-committee-institute.de/docs/aci_quarterly_2007_2.pdf abgerufen 05.01.2018
- Babu, & Parishat. (11. 10 2004). *crime-research.org*. Abgerufen am 28.01.2018 von <http://www.crime-research.org/analytics/702>
- Bailey. (05 2015). *Fraud Magazine*. Abgerufen am 14.12.2017 von Why companies are afraid to fight fraud: <http://www.fraud-magazine.com/article.aspx?id=4294988395>

- Bartelsmann. (2018). *Der Bartelsmann Code of Conduct*. Von <https://www.bartelsmann.de/verantwortung/compliance/code-of-conduct/> abgerufen am 11.11.2017
- Bartulovic, & Filipovic. (2016). *Financijsko-racunovodstveni forenzicar- zanimanje buducnosti*. RRIF.
- Baur, & Blasius. (2014). *Handbuch Methoden der empirischen Sozialforschung*. Berlin: Springer.
- BDI & KPMG. (2009). Von Sichere Geschäfte?: https://bdi.eu/media/presse/publikationen/recht-und-oeffentliches-auftragswesen/Broschuere_Sichere_Geschaefte_85524_KPMG_BDI.PDF abgerufen am 10.12.2017
- BDO Deutschland. (Februar 2017). Beurteilung Ihres internen Revisionssystems- Grundsätze ordnungsmässiger Prüfung von internen Revisionssystemen (IDW EPS 983).
- Belak. (2012). *Poslovna forenzika i forenzicko racunovodstvo- Borba protiv prijevare*. Zagreb, Kroatien: Belak Excellens d.o.o.
- Belak, & Vudric. (2012). *Osnove suvremenog racunovodstva*. Zagreb, Kroatien: Belak Excellence d.o.o.
- Belopavlovic. (2014). *Book of Proceedings: Financial Reporting Function of The Corporate Governance*.
- Brodowski, & Freiling. (2011). *Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft*. Berlin.
- Budimir. (2017). *Forenzicko racunovodstvo i forenzicka revizija*.
- Buhse. (2013). *Auf der Jagd*. Von <http://www.zeit.de/2013/14/Beruf-Wirtschaftsforensiker> abgerufen am 15.01.2018
- Bundeskankleramt. (08.12.2017). *Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Finanzstrafgesetz, Fassung vom 08.12.2017*. Abgerufen am 08. 12 2017 von <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10003898>
- Bundeskankleramt. (08.12.2017). *RIS*. Abgerufen am 08.12.2017 von Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Strafgesetzbuch, Fassung vom 08.12.2017: <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296>
- Bundeskankleramt Österreich. (2018). *HELP.gv.at*. Von <https://www.help.gv.at/Portal.Node/hlpd/public/content/172/Seite.1720510.html> abgerufen am 11.02.2018
- Bundesministerium für Justiz. (2016). *Sicherheitsbericht 2016- Bericht über die Tätigkeit der Strafjustiz*. Von http://www.bmi.gv.at/508/files/SIB_2016/04_SIB2016-BMJ-Teil_web.pdf abgerufen 16.02.2018
- Bundesministerium für Wirtschaft und Energie. (2018). *Plattform Industrie 4.0*. Von <http://www.plattform-i40.de/I40/Navigation/DE/Industrie40/WasIndustrie40/was-ist-industrie-40.html;jsessionid=D7ED4118DED525F176F382A8F939369D> abgerufen am 14.12.2017
- Business Government Netherlands. (2018). Von <https://business.gov.nl/regulation/reporting-unusual-transactions/> abgerufen am 13.01.2018

- Capco. (2017). The Capco Institute: Journal of Financial Transformation. *The Capco Institute: Journal of Financial Transformation*.
- Casey. (2011). *Digital Evidence and Computer Crime, Forensic Science, Computers and Internet*.
- CCM-TV. (27. 03 2017). Abgerufen am 16.12.2017 von <http://ccm-tv.at/2017/03/27/die-cyberkriminalitaet-in-oesterreich-steigt-staendig/>
- Commission, E. (2013). *Eurostat-Statistical Working Papers*. Von <http://ec.europa.eu/eurostat/web/products-statistical-working-papers/-/KS-TC-13-007> abgerufen am 10.12.2017
- Computerwoche. (2018). *computerwoche.de*. Von <https://www.computerwoche.de/k/internet-of-things-iot,3528> abgerufen am 12.12.2017
- Controlling-Portal. (22. 08 2017). *CONTROLLING-Portal.de*. Abgerufen am 17.12.2017 von <https://www.controllingportal.de/Fachinfo/Sonstiges/Sarbanes-Oxley-Act.html>
- Cudan. (26. 10 2015). (K.-p. a. Beogradu, Produzent) Abgerufen am 01.11.2017 von <https://docslide.com.br/documents/ekonomsko-finansijsko-vestacenje-kao-oblik-forenzickog-racunovodstva.html>
- Der österreichische Zoll. (2013). *Bericht an den Nationalrat über die Anwendung der EG-Produktpiraterie-Verordnung 2004 und des Produktpirateriegesetzes 2004 im Jahr 2013*. Von https://www.bmf.gv.at/zoll/produktpiraterie/Produktpirateriebericht_2013.pdf?63xg74 abgerufen am 15.01.2018
- der Standard. (22.06.2017). *der Standard*. Abgerufen am 20.12.2017 von <https://derstandard.at/2000059666759/OpenVPN-Vier-kritische-Luecken-gefaehrden-VPN-Nutzer>
- Der Standard. (13.09.2017). *Der Standard*. Von Der Standard: <https://derstandard.at/2000063997323/Cyberattacken-gegen-Unternehmen-stark-im-Anstieg> abgerufen am 15.01.2018
- Detecon (Schweiz) AG in Zusammenarbeit mit der Handelshochschule Leipzig und der Wirtschaftsuniversität Wien. (01.2010). *IKS- Interne Kontrollsysteme nach der 8. EU-Richtlinie*. Abgerufen am 14.12.2017 von https://www.wu.ac.at/fileadmin/wu/d/i/ruw/revision/publ/IKS_2010__Detecon_Schweiz_.pdf
- Die österreichische Justiz. (2017). Abgerufen am 12.11.2017 von https://www.justiz.gv.at/web2013/home/buergerservice/die_justiz_von_a_bis_z/u/urheberr echt_~2c94848b4b92ce25014c314273ab1aca.de.html Die österreichische Justiz
- Die Welt. (04.10.2002). Abgerufen am 14.01.2018 von <https://www.welt.de/print-welt/article414412/Skandal-Manager-des-Enron-Konzerns-in-Handschellen.html>
- Dimitrijevic. (2015). Otkrivanje i sprecavanje manipulacija u bilansu stanja i izvestaju o novcanim tokovima.
- Easterly. (2005). *National policies and economic growth: A reappraisal*.
- Ernst & Young Österreich. (2017). Von [http://www.ey.com/Publication/vwLUAssets/EY_Fraud_Survey_Österreich_2017/\\$FILE/EY%20Fraud%20Survey%20Österreich%202017.pdf](http://www.ey.com/Publication/vwLUAssets/EY_Fraud_Survey_Österreich_2017/$FILE/EY%20Fraud%20Survey%20Österreich%202017.pdf) abgerufen am 20.02.2018

- Europäische Kommission Generaldirektion Regionalpolitik und Stadtentwicklung, Leitdaten zur Bewertung des Betrugsrisikos und zu wirksamen und angemessenen Betrugsbekämpfungsmassnahmen, Programmplanzeitraum 2014-2020. (2014).
- F.A.Z. (2008). Frankfurt.
- Faigle. (2016). *die Zeit*. Von <http://www.zeit.de/wirtschaft/2016-04/panama-papers-wirtschaftskriminalitaet-ohnmacht-justiz-briefkastenfirmen> abgerufen am 12.03.2018
- Fayyad, Piatetsky-Shapiro, & Smyth. (kein Datum). *From Data Mining to Knowledge Discovery in Databases*. Von <https://www.kdnuggets.com/gpspubs/aimag-kdd-overview-1996-Fayyad.pdf> abgerufen am 05.01.2018
- Finance laws*. (2017). Abgerufen am 14.01.2018 von <https://finance.laws.com/enron-scandal-summary>
- Finance-Magazin Deutschland. (2017). Von <https://www.finance-magazin.de/banking-berater/wirtschaftspruefer/dienstleistungsspektrum-der-wirtschaftspruefer-wird-breiter-2001111/> abgerufen am 12.12.2017
- Fischer. (Februar 2003). *Enron's Real Financials*. Von https://www.forbes.com/2003/02/03/cz_df_0203enron.html#1908df022b03 abgerufen am 09.11.2017
- Forensic Accounting Today. (2017). Von <http://jemoore.typepad.com/blog/2007/11/teamwork-its-ap.html> abgerufen am 10.10.2017
- Forensic CPA Society. (2018). Von <https://www.fcpas.org/about-us/what-is-a-forensic-accountant/> abgerufen am 12.09.2017
- Glaser. (2015). *Risikomanagement im Leasing: Grundlagen, rechtlicher Rahmen und praktische Umsetzung*.
- Goebel. (2016). *WirtschaftsWoche*. Von Unterschätzte Gefahr für Unternehmen : <https://www.wiwo.de/unternehmen/mittelstand/wirtschaftskriminalitaet-unterschaetzte-gefahr-fuer-unternehmen/13831748.html> abgerufen am 15.09.2017
- Gray. (2008). Forensic Accounting And Auditing: Compared And Contrasted To Traditional Accounting And Auditing. *American Journal of Business Education – Fourth Quarter 2008*.
- Gros. (2005). *Sarbanes Oxley Act*. ENI Group- AGIP Deutschland GmbH, 3. Finance-Gipfel, Berlin.
- Guidance Software (Webinar). (2017). Von <https://www.guidancesoftware.com/video/webinar/whats-new-in-encase-forensic-7-12> abgerufen am 12.01.2018
- Handelsblatt. (2003). Von <http://www.handelsblatt.com/politik/deutschland/interessenkonflikte-sollen-vermieden-werden-berlin-will-unabhaengige-wirtschaftspruefer/2279234.html> abgerufen am 15.01.2018
- Hayes, Dassen, Schilder, & Wallage. (2005). *Principles of Auditing: An Introduction to International Standards on Auditing*. Edinburgh: Pearson Education Limited.
- Heinson, Yannikos, Franke, Winter, & Schneider. (02 2010). Rechtliche Fragen zur Praxis IT-forensischer Analysen in Organisationen. *Datenschutz und Datensicherheit - DuD*.

- Hirai. (2011). *Flickr*. Von <https://www.flickr.com/photos/playstationblog/sets/72157626521862165/with/5686965323/> abgerufen am 10.12.2017
- Hlavica, Hülsberg, & Klapproth. (2011). *Tax Fraud & Forensic Accounting: Umgang mit Wirtschaftskriminalität*. Gabler.
- Holtzman, Venuti, & Fonfeder. (2003). *Enron and the Raptors*. Von <http://archives.cpajournal.com/2003/0403/features/f042403.htm> abgerufen am 11.10.2017
- IBM Deutschland. (2018). *Wie digitale Beweismittel bei der Strafverfolgung optimal genutzt werden können*. Von Video: https://www.ibm.com/industries/de-de/government/digitale-beweise-verwalten/?S_PKG=AW&cm_mmc=Search_Google-_Government_Government-_+daten++forensik_Broad_&cm_mmca1=000027FZ&cm_mmca2=10007783&cm_mmca7=9043851&cm_mmca8=kwd-341081039983&cm_mmca9=e1e14bc7-26 abgerufen am 12.12.2017
- ICAEW. (2018). *The future of Audit: Technology*. Abgerufen am 26.01.2018 von <https://www.icaew.com/en/technical/audit-and-assurance/faculty/the-future-of-audit/the-future-of-audit-technology>
- ICFA. (2016). Von <http://www.forensicglobal.org/forensicaccounting.html> abgerufen am 01.12.2017
- IFAC. (2009). *IFAC*. Abgerufen am 04.11.2017 von International Standard on Auditing 210, Agreeing the Terms of Audit Engagements: <http://www.ifac.org/system/files/downloads/a009-2010-iaasb-handbook-isa-210.pdf>
- IFAC ISA 260. (2009). *IFAC ISA 260*. Abgerufen am 28.01.2018 von <http://www.ifac.org/system/files/downloads/a014-2010-iaasb-handbook-isa-260.pdf>
- IFAC ISA 570. (30.01.2018). Von <http://www.ifac.org/system/files/downloads/a031-2010-iaasb-handbook-isa-570.pdf> abgerufen am 30.01.2018
- IFAC ISA 700. (30.01.2018). Von <https://www.ifac.org/system/files/publications/files/Proposed%20ISA%20700%20%28Revised%29-final.pdf> abgerufen am 30.01.2018
- International Standard on Auditing. (2009). *International Standard on Auditing- The auditor's responsibilities relating to fraud in an audit of financial statements*. Von International Standard on Auditing- The auditor's responsibilities relating to fraud in an audit of financial statements abgerufen am 11.12.2017
- International standard on auditing 400. (2018). *ISA 400*. Von <https://www.rechnungswesen-portal.de/Fachinfo/Interne-Revision/Interne-Revision.html> abgerufen am 10.10.2017
- Interne Revision. (2017). Von <https://www.rechnungswesen-portal.de/Fachinfo/Interne-Revision/Interne-Revision.html> abgerufen am 15.10.2017
- IPFS. (2018). *IPFS*. Abgerufen am 28.01.2018 von https://ipfs.io/ipfs/QmXoypizjW3WknFiJnKLwHCnL72vedxjQkDDP1mXWo6uco/wiki/Money_laundering.html
- ISAAB. (2018). Abgerufen am 28.01.2018 von <https://www.iaasb.org/about-iaasb>
- IT Service. (2018). Von <https://www.it-service24.com/lexikon/f/forensische-datenrettung/> abgerufen am 14.01.2018

- Jahn. (2001). Von <https://www.jura.uni-frankfurt.de/55029767/Glaubhaftigkeitsbeurteilung.pdf> abgerufen 15.02.2018
- Jansen. (2016). *Analyse der Spurmenge der Anwendung OpenVPN Client Version 2.3.9 in Microsoft Windows*. Friedrich-Alexander-Universität Erlangen-Nürnberg.
- JEANNEE Rechtsanwalt GmbH. (2014). Abgerufen am 15.12.2017 von <http://www.toplaw.at/wp-content/uploads/Compliance-Weihnachtsgeschenke-und-Korruptionsstrafr.pdf>
- Jimenez. (09.06.2013). *Welt N24*. Abgerufen am 12.11.2017 von Ein FBI-Agent als menschlicher Lügendetektor: <https://www.welt.de/gesundheit/psychologie/article116924156/Ein-FBI-Agent-als-menschlicher-Luegendetektor.html>
- Jovkovic. (2014). Primena tehnika prikupljanja dokaza u ispitivanju osnovnih ciljeva revizije u osiguravajućim društvima. *Ekonomski horizonti, Vol 16*.
- Kacanski. (2012). *Specifity of Continuous Auditing Approach on Information Technology Internal Controls*. Novi Sad.
- Klokar. (2017). *Internes Kontrollsystem*. Abgerufen am 14.12.2017 von http://www.klienten-info.at/599_3/create_pdf.php?kicat=1&navcat=1&art_id=722
- Kompjuterski i cyber kriminal*. (kein Datum). Abgerufen am 12.11.2017 von http://predmet.singidunum.ac.rs/pluginfile.php/13501/mod_folder/content/0/Kompjuterski%20i%20cyber%20kriminal.pdf?forcedownload=1
- KPMG. (2011). *Risk & Compliance: Compliance-Management-Systeme*. Abgerufen am 15.12.2017 von https://www.kpmg.at/fileadmin/KPMG/Publikationen/Broschueren_und_Studien/Compliance_Management_Systeme.pdf
- KPMG. (13.09.2017). Abgerufen am 16.12.2017 von <https://home.kpmg.com/at/de/home/media/press-releases/2017/09/kpmg-cyber-security-in-oesterreich-2017.html>
- KPMG Deutschland. (2017). *kpmg.com*. Abgerufen am 18.12.2017 von <https://home.kpmg.com/de/de/home/services/audit/forensic/forensic-due-diligence.html>
- Landeskriminalität Niedersachsen. (2017). Abgerufen am 08.12.2017 von <http://www.lka.polizei-nds.de/kriminalitaet/deliktsbereiche/wirtschaftskriminalitaet/definition-wirtschaftskriminalitaet-844.html>
- Larry. (2005). *Forensic and Investigative Accounting*.
- Lavion. (2018). *PWC*. Von PWC: <https://www.pwc.com/gx/en/forensics/global-economic-crime-and-fraud-survey-2018.pdf> abgerufen am 06.03.2018
- Leisinger. (2008). *Whistle blowing: Zum konstruktiven Umgang mit Kritik, die von innen kommt*. Abgerufen am 28.01.2018 von Book: Wirtschaftskriminalität und Ethik: <https://www.econstor.eu/bitstream/10419/68579/1/654462356.pdf>
- Leitlinie V 201: Zur Berichterstellung in der Internen Revision. (2012). Von <http://www.forum-interne-revision.org/leitlinien/leitlinien/leitlinie-v-2012-zur-berichterstellung-in-der-internen-revision.html> abgerufen am 11.12.2017
- Lochberg. (2014). Von <https://www.krollontrack.de/blog/worum-geht-es-bei-computer-forensik/1444> abgerufen am 13.12.2017

- Löffler, & Nayer. (27.07.2011). *Definition und Organisation des Internen Kontrollsystems*. Abgerufen am 14. 12 2017 von <https://www.lindeverlag.at/buch/handbuch-zum-internen-kontrollsystem-4360/b/leseprobe/B00856.pdf>
- Manager Magazin. (2005). Von <http://www.manager-magazin.de/unternehmen/karriere/a-369350.html> abgerufen am 12.01.2018
- Margret, & Peck. (2015). *Fraud in financial statements*. New York.
- Markoff. (2011). *New York Times*. Von <http://www.nytimes.com/2011/03/18/technology/18secure.html> abgerufen am 11.12.2017
- McNulty. (24.10.2006). *Financial Times*. Abgerufen am 14.01.2018 von <https://www.ft.com/content/6b300750-62d2-11db-8faa-0000779e2340>
- Meier, & Pernul. (2017). *Einsatz von digitaler Forensik in Unternehmen und Organisationen* . Abgerufen am 14.12.2017 von <https://subs.emis.de/LNI/Proceedings/Proceedings228/103.pdf>
- Mekic, Halilbegovic, & Huric. (01.02.2017). *Forensic accounting as a solution to manipulative accounting of SME's in Bosnia and Herzegovina*. Abgerufen am 21.09.2017 von Ecoforum: <http://www.ecoforumjournal.ro/index.php/eco/article/viewFile/634/396>
- Melcher. (2009). *Aufdeckung wirtschaftskrimineller Handlungen durch den Abschlussprüfer* (Band 18 Ausg.). EUL Verlag.
- Menzies. (2004). *Sarbanes-Oxley Act- Professionelles Management interner Kontrollen*. Stuttgart: Schäffer-Poeschel Verlag.
- Milosavljevic, & Grubor. (2009). *Digitalna forenzika racunarskog sistema*. Beograd.
- Möller, & Sigillo. (2010). *Der Enron-Andersen-Skandal und dessen Einfluss auf das Reputationskapital der Institution Wirtschaftsprüfung*.
- Möller, & Sigillo. (2010). *Der ENron-Andersen-Skandal und dessen Einfluss auf das Reputationskapital der Institution Wirtschaftsprüfung*.
- Moritz, & Gesse. (12.2005). Abgerufen am 18.12.2017 von <http://telc.jura.uni-halle.de/sites/default/files/altbestand/Heft49.pdf>
- Morris-Cotterill. (1999). *countermoneylaundering.com*. Abgerufen am 28.01.2018 von <http://www.countermoneylaundering.com/public/content/brief-history-money-laundering>
- Myatt. (2013). *ENRON. When the American Dream became the American Nightmare*. Von <https://jodimyatt.wordpress.com/2013/11/12/enron-when-the-american-dream-became-the-american-nightmare-by-jodi-myatt-bio-cybertronics/> abgerufen am 11.11.2017
- National Crime Agency. (2018). Von <http://www.nationalcrimeagency.gov.uk/publications/suspicious-activity-reports-sars/550-introduction-to-suspicious-activity-reports-sars-1/file> abgerufen 14.12.2017
- NICE. (2018). *NICE homepage*. Abgerufen am 26.01.2018 von <https://www.niceactimize.com/press-releases/NICE-Actimize-Introduces-Robotic-Process-Automation-to-Improve-Financial-Crime-and-Compliance-Efficiency-188>

- Nicevic, & Ivanovic. (August 2012). *Organizovani privredni kriminalitet kao faktor ugrozavanja ekonomske bezbednosti*.
- Nykodym. (2005). *Computer Law & Security Review*. 408-414.
- Owojori, & Asaolu. (2009). *The Role of Forensic Accounting in Solving the Vexed Problem of Corporate World*. Abgerufen am 15.12.2017 von European Journal of Scientific Research: https://www.researchgate.net/profile/Anthony_Owojori/publication/292566948_The_role_of_forensic_accounting_in_solving_the_vexed_problem_of_corporate_world/links/5840bc0908ae61f75dceecce.pdf
- Pearson, & Brickner. (May/June 2003). SAS 99- Another Implement for the Fraud Examiner's Toolbox. *Fraud Magazine*.
- Peavler. (14. 02 2017). *Business Finance*. Abgerufen am 08.12.2017 von IFRS and FASB - What are Financial Reporting Standards?: <https://www.thebalance.com/ifrs-and-fasb-what-are-financial-reporting-standards-392948>
- Petrovic. (2010). *Medjunarodni standardi revizije*. Beograd.
- Petrovic, Stanisic, & Vicentijevic. (2016). *Revizijska regulativa*. Beograd.
- Pickett. (2005). *The Essential Handbook of Internal Auditing*. West Sussex.
- Prashant. (26.08.2015). *LinkedIn*. Abgerufen am 14.01.2018 von <https://www.slideshare.net/PrashantMirgule/what-happened-with-enron>
- Pratap. (November 2016). *Corporate Culture of Enron and how it bred a Scandal*. Von <https://www.cheshnotes.com/2016/11/corporate-culture-enron-bred-scandal/> abgerufen am 02.01.2018
- Project Consultant. (2013). Von https://www.project-consult.de/in_der_diskussion/rechtsg%C3%BCtigkeit_gescannter_dokumente_ein_musterversuch abgerufen am 13.12.2017
- Public Law 107-204-JULY 30,2002; 116 STAT. 745. (30.07.2002). Abgerufen am 17.12.2017 von <https://www.sec.gov/about/laws/soa2002.pdf>
- Puhani. (2018). Von <https://www.internerevisiondigital.de/ce/pruefungskonzept/detail.html> abgerufen am 12.12.2017
- PWC Global. (2015). *securityforum.at*. Abgerufen am 20.12.2017 von https://www.securityforum.at/wp-content/uploads/2015/05/SSD_Forensik.pdf
- Rat der Europäischen Union (Brüssel). (26. Juni 2017). Von https://www.parlament.gv.at/PAKT/EU/XXV/EU/15/48/EU_154878/imfname_10746545.pdf abgerufen am 19.10.2017
- Rausenberger, & Prenrecaj. (2017). *AUDIT 4.0 – DIGITALE WIRTSCHAFTSPRÜFUNG*. Von https://www.pwc.ch/de/publications/2018/Expert_Focus_Digitale_Wirtschaftspruefung.pdf abgerufen am 01.02.2018
- Rautenstrauch. (2016). IKS: Mit einem klaren Konzept zu mehr Sicherheit in Organisation und Prozessabläufen.

- Rechtsanwalt Dr. Markus Kaltseis. (2016). Abgerufen am 14. 01 2018 von <http://www.rechtsanwalt-wels.at/fachartikel/insolvenzrecht-in-oesterreich-was-tun-bei-firmenpleite/>
- Rezaee. (2002). *Financial Statement Fraud: Prevention and Detection* . New York: Wiley.
- RIS §82 AktG. (kein Datum). Von <https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR12039576> abgerufen am 12.12.2017
- Rouse. (2006). Von <http://www.searchsecurity.de/definition/Social-Engineering> abgerufen am 10.11.2017
- SAS Institute Inc. (2017). Abgerufen am 26.01.2018 von https://www.sas.com/de_de/whitepapers/ff-wp-betrugserkennung-mit-analytischen-verfahren-2279899.html
- SAS Risk Management. (2017). Abgerufen am 26.01.2018 von https://www.sas.com/de_de/solutions/risk-management.html
- Savez racunovodja i revizora Srbije. (2005). *Medjunarodni standardi i saopštenja revizije*. Beograd, Srbija.
- Schadhauser, & Graefen. (2017). Von <https://www.storage-insider.de/was-macht-eine-ssd-besser-als-eine-hdd-a-517814/> abgerufen am 10.12.2017
- Schneider. (2009). Geldwäsche: Formen, Akteure, Größenordnung- und warum die Politik machtlos ist. *Praxis der Ökonomie*.
- Scholz. (2017). *Abschlussprüfung und Fraud: Hält der WP, was er verspricht?* Abgerufen am 28.01.2018 von <ftp://ftp.repec.org/opt/ReDIF/RePEc/osi/scispf/PDF/ScientificSymposiumPforzheim/pf2906.pdf>
- Schonschek. (19. 06 2013). *computerwoche.de*. Abgerufen am 21. 12 2017 von <https://www.computerwoche.de/a/tools-fuer-die-mobile-forensik,2533050>
- Schwanfelder. (2017). *Überzeugend führen mit Machiavelli- Machen macht mächtig*. Heidelberg.
- Security Forum 2018. (2017). *securityforum.at*. Abgerufen am 20. 12 2017 von <https://www.securityforum.at/ssd-forensik-das-problem-garbage-collection/>
- Sejfulovic. (2012). *Komparativni aspekti sprecavanja pranja novca u Bosni i Hercegovini i Republici Hrvatskoj*. Tuzla.
- Silverstone, & Sheetz. (2007). *Forensic Accounting and Fraud Investigation for Non-Experts*. New Jersey.
- Singelton, S. B. (2006). *Fraud Auditing and Forensic Accounting* . New Jersey: John Wiley & Sons, Inc.
- SPIEGEL Online. (27. 02 2002). Abgerufen am 14.01.2018 von <http://www.spiegel.de/wirtschaft/interview-zum-enron-skandal-die-kellner-werden-kontrolliert-die-speisekarte-bleibt-die-alte-a-184286.html>
- Stanisic. (2014). *Interna kontrola i revizija*. Beograd: Univerzitet Singidunum .
- Stanisic, & Nikolic. (2009). *Kontrola i revizija hotelskog poslovanja*. Beograd.

- Steuerberater.net. (2016). Von http://www.steuerberater.net/steuertipps/scan-von-original-oder-kopie-belegeinreichung-zur-vorsteuererstattung_000696.html abgerufen am 11.12.2017
- Strafgesetzbuch. (21.09.2017). § 146 StGB Betrug. *§ 146 StGB Betrug*.
- Suput. (2009). Odgovornost pravnog lica za krivicna dela. In *Strani pravni zivot*. Beograd.
- Sure. (2016). *Internationales Management: Grundlagen, Strategien und Konzepte*. Köln: Springer Gabler.
- Techtarget. (2016). Von <http://searchstorage.techtarget.com/definition/disk-mirroring> abgerufen
- The Guardian. (2002). Von <https://www.theguardian.com/business/2002/mar/24/enron.theobserver> abgerufen
- Theurer. (2016). Korruption so schlimm wie Terrorismus. *Frankfurter Allgemeine Zeitung*.
- Thielemann. (2005). *Der Fall Enrons- Ein Anlass, über den wirtschaftsetischen Status von Managementintegrität nachzudenken*. FORUM Wirtschaftsethik.
- Thomas. (2002). *Journal of Accountancy*. Abgerufen am 14.01.2018 von <https://www.journalofaccountancy.com/issues/2002/apr/theriseandfallofenron.html>
- Udruzenje racunovodja, forenzicara i revizora. (21.08.2017). Abgerufen am 01.11.2017 von <http://econforbd.com/index.php/sr/2015-10-04-18-31-38/170-uloga-i-znacaj-forenzickog-racunovodstva-u-otkrivanju-finansijskih-prevara>
- UGB. (08.12.2017). *§ 245a UGB Konzernabschlüsse nach international anerkannten Rechnungslegungsgrundsätzen*. Abgerufen am 08.12.2017 von <https://www.jusline.at/gesetz/ugb/paragraf/245a>
- United States Courts. (2018). Abgerufen am 14.01.2018 von <http://www.uscourts.gov/services-forms/bankruptcy/bankruptcy-basics/chapter-11-bankruptcy-basics>
- Universität Erlangen. (2018). Von https://univis.uni-erlangen.de/formbot/dsc_3Danew_2Fmodule_view_26mod_3Dtech_2FIMMD_2Flehrst_2F0_9_26dir_3Dtech_2FIMMD_2Flehrst_26lvs_3Dtech_2FIMMD_2Flehrst_2Fforens_26ref_3Dlecture abgerufen am 15.02.2018
- Unterhauser. (29.06.2007). *Lex and Tax: Riskmanagement "Rechtliche Rahmenbedingungen" Teil 1*. Abgerufen am 15.12.2017 von http://www.lexandtax.at/index.php?option=com_content&view=article&id=14023:10467&catid=52:40,30&Itemid=64
- Verordnung (EG) Nr. 1606/2002 des Europäischen Parlaments und des Rates vom 19. Juli 2002 betreffend die Anwendung internationaler Rechnungslegungsstandards. (19.07.2002). *EUR-Lex Access to European Union law*. Abgerufen am 12.08.2017 von <http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32002R1606>
- Vilendecic, & Vilendecic. (2014). Pronevjere u bjelim knjigama (kradje i prevare kroz papire). *SVAROG*.
- vpnMentor. (2017). Abgerufen am 20.12.2017 von <https://de.vpnmentor.com/blog/vpn-nutzung-und-datenschutz-statistiken-fuer/>

- Welt.de. (26. 09 2010). *Welt.de*. Abgerufen am 14.12.2017 von <https://www.welt.de/wirtschaft/webwelt/article9884891/Stuxnet-Wurm-befaelit-iranisches-Atomkraftwerk.html>
- Wirtschaftskammer Österreich- Die Finanzdienstleister. (12.04.2012). Abgerufen am 15.12.2017 von <https://www.wko.at/branchen/information-consulting/finanzdienstleister/artikel-interne-revision.pdf>
- XII Medjunarodni naucni skup sinergija: "Kvalitet-put u Evropu". (2013). Abgerufen am 11.11.2017 von <http://naucniskup.sinergija.edu.ba/wp-content/uploads/2017/02/Zbornik-2013-1.pdf>
- Zahra, & AL, E. (2005). Top Management Fraud. *Journal of Management*.