Initiative Wirtschaftsschutz – Wirtschaftsgrundschutz und Baustein „Umgang mit Wirtschaftskriminalität“

Timo Kob/Björn Schmelter/Peter Zawilla

1 Einleitung

Mit dem Wirtschaftsgrundschutz, herausgegeben vom ASW Bundesverband[1] (ASW), dem Bundesamt für Verfassungsschutz (BfV) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI), werden auf Basis der bekannten IT-Grundschutzstruktur die verschiedenen Sicherheitsthemen außerhalb der klassischen IT-Angriffsfelder aufgegriffen. Dabei ist ein Leitfaden entstanden, der allen Verantwortlichen in den Unternehmenssicherheitseinheiten, sowohl in der freien Wirtschaft als auch im behördlichen Umfeld, als Blaupause für den Aufbau und Ablauf der Sicherheitsorganisation dienen kann.

2 Wirtschaftsgrundschutz

Mit dem Wirtschaftsgrundschutz ist eine frei zugängliche Sammlung der wesentlichen Sicherheitsaspekte außerhalb der klassischen IT-Sicherheit entstanden. Die Grundidee, Zielsetzung und Herangehensweise zur Erstellung dieses Werkes in Form eines Handbuches wird in den folgenden Abschnitten näher erläutert.

2.1 Grundidee und Ziele

Cybersicherheit ist heute präsenter denn je und bildet sich auch in der Novellierung des IT-Grundschutzes ab. Das BSI beweist ebenfalls mit seinem neu gestalteten Leitbild die Bedeutung aller erdenklichen Cybersicherheitsszenarien.

Der Cyberhype bedeutet jedoch nicht, dass andere Themenkomplexe, wie physische oder personelle Sicherheit, an Bedeutung verlieren. Ganz im Gegenteil bilden Angriffe in den klassischen Sicherheitsdisziplinen meist einen Startpunkt für komplexe Angriffe im Cyberraum. Und gerade mit der zunehmenden Verbreitung von IT außerhalb klassischer IT-Systeme – wie wir sie heute v.a. unter den Schlagwörtern „Internet of Things“ oder „Industrie 4.0“ wahrnehmen – steigt auch die Bedeutung weiterer Sicherheitsaspekte, da die Interdependenzen immer größer werden.

Ein besonders kritischer Aspekt außerhalb der klassischen IT-Sicherheit ist die Sammlung von sicherheitsrelevanten Informationen, um z.B. das Erraten von Passwörtern oder die gezielte Ansprache im Spearphishing, d.h. einen Phishing-Angriff auf einen Einzelnen unter Zuhilfenahme von spezifischen und persönlichen Informationen, zu erlauben.

[1] ASW Bundesverband, Allianz für Sicherheit in der Wirtschaft e.V., 10178 Berlin.

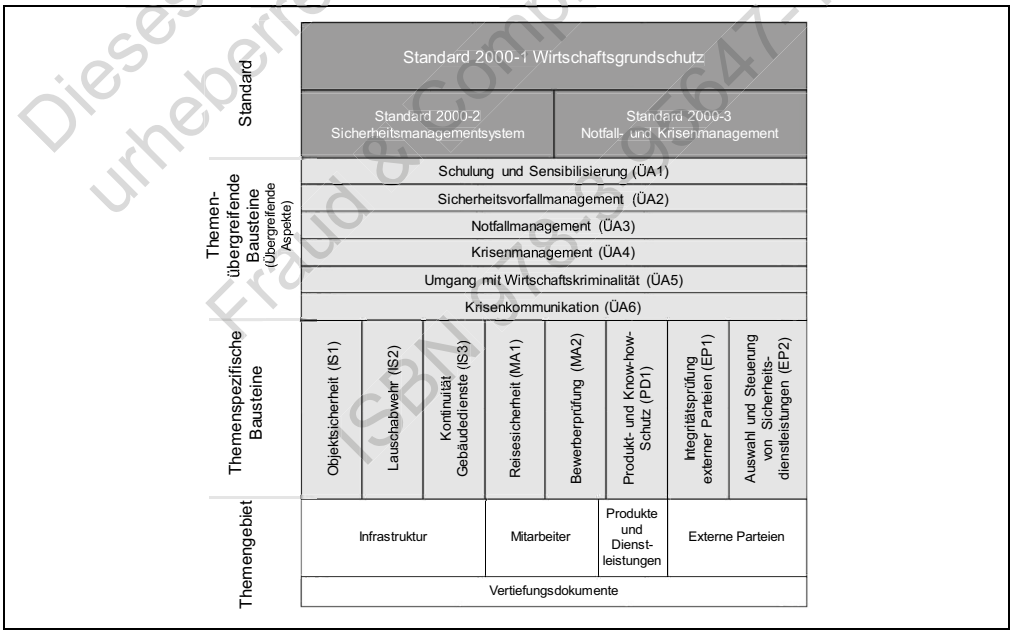
Hierauf zielen Maßnahmen der personellen Sicherheit (z.B. in Form von Sensibilisierungskampagnen oder der Einstellung geeigneter Mitarbeiter) und der physischen Sicherheit (z.B. durch Zutrittsbeschränkungen und das Wegschließen sensibler Informationen).

Nun ist dieser Ansatz nicht neu: Bereits seit Jahrzehnten existieren sowohl die klassischen Sicherheitsthemen – auch außerhalb der IT – sowie die Cyber- bzw. IT-Sicherheitsthemen. Eine Herausforderung, der sich aber alle stellen müssen, ist die Integration all dieser Sicherheitsaspekte und die Vermeidung redundanter Aufgaben. Das Schlüsselwort dabei lautet „einheitliches Sicherheitsniveau", damit jedes Themenfeld der Unternehmenssicherheit die gleiche Strategie verfolgt. Andernfalls entsteht schnell an einem spezifischen Punkt das schwächste Glied in der Kette und damit ein mögliches Einfallstor für Angriffe.

2.2 Projektstruktur und -rahmenbedingungen

Um Abhilfe bezüglich der fehlenden Integration aller Sicherheitsthemen in einem Werk zu schaffen, wurde von 2014 bis 2016 von der HiSolutions AG und dem ASW Bundesverband unter Einbindung der Fachhochschule Campus Wien als akademischem Partner ein Forschungsprojekt unter Schirmherrschaft des BfV und des BSI durchgeführt. Die Ergebnisse dieses Projekts – dargestellt in Abbildung 1 – werden seit November 2016 sukzessive als Wirtschaftsgrundschutz veröffentlicht – alle zugehörigen Inhalte sind kostenfrei auf www.wirtschaftsschutz.info abrufbar.

Abbildung 1: Struktur des Wirtschaftsgrundschutzes auf Basis des Projektantrages



3 Struktur des Wirtschaftsgrundschutzes

Kernidee des Wirtschaftsgrundschutzes ist es, die Philosophie und Methodik des IT-Grundschutzes als profundes und anerkanntes Werkzeug für Gefährdungen in der (oder besser durch die) IT um ein Werk für die klassischen Sicherheitsaspekte zu ergänzen.

3.1 Grundüberlegungen und Zielgruppen

Eine sprachliche Nähe zwischen dem IT-Grundschutz und dem Wirtschaftsgrundschutz ist dabei Absicht, um auch hier den anschließenden Charakter hervorzuheben. Dabei meint Wirtschaftsschutz weder, dass der IT-Grundschutz nicht ebenso für die Wirtschaft relevant ist, noch, dass er nur für die Wirtschaft geeignet wäre: Der Name soll vielmehr die ergänzende Bedeutung des Wirtschaftsgrundschutzes für einen ganzheitlichen Wirtschaftsschutz verdeutlichen.

Der Wirtschaftsgrundschutz ist ebenso wie der IT-Grundschutz als offener, lebender und konsensorientierter Standard zu verstehen. Alle Bausteine und Inhalte werden durch Expertenkreise begleitet und abschließend bewertet: So werden unterschiedlichste Branchenerkenntnisse in dem im Wirtschaftsgrundschutz beschriebenen Sicherheitsmanagement festgehalten und manifestiert. Neue Themen können – gesteuert durch den ASW Bundesverband – von allen Experten frei initiiert werden. Um sich für eine Mitarbeit zu melden, genügt eine Nachricht an info@asw-bundesverband.de.

Die grundlegende Idee des Wirtschaftsgrundschutzes beruht auf einem ganzheitlichen Schutzmodell, das nicht nur sämtliche Werte einer Institution abdeckt, sondern für deren Schutz auch alle erforderlichen Funktionen und Bereiche unter einer zentralen Funktion zusammenfasst und steuert. Dies stellt die unabdingbare Voraussetzung für ein einheitliches Sicherheitsniveau und eine effiziente Gestaltung des Sicherheitsmanagementsystems unter Berücksichtigung potenzieller Synergien dar.

3.2 Struktur des Standards

Der Wirtschaftsgrundschutz verfolgt die Idee einer integrierten Unternehmenssicherheit und unterscheidet die zu betrachtenden sicherheitsrelevanten Themenfelder der Sicherheitsorganisation in „Kernthemen" und „übergreifenden Themen": Die Kernthemen werden im Wirtschaftsgrundschutz durch einzelne Schichten dargestellt. Diese werden i.d.R. innerhalb einer Institution durch die Aufbauorganisation strukturiert und dedizierten Bereichen oder Gruppen zugeordnet.

Sanktionen gegen Unternehmen bei Compliance-Verstößen: Aktuelle Entwicklungen und Trends

Jörg Bielefeld/Lenard Wengenroth

1 Aktuelle Entwicklungen bei der Sanktionierung

Insbesondere Rechtsordnungen aus dem anglo-amerikanischen Rechtskreis kennen ein „echtes" Unternehmensstrafrecht, wie es etwa hinsichtlich spezifischer Konstellationen im britischen UK Bribery Act oder im Foreign Corrupt Practices Act (FCPA) in den USA kodifiziert ist.[1] Als Reaktion auf strafrechtliches Fehlverhalten – insbesondere im Zusammenhang mit Korruption – von Mitarbeitern oder Leitungspersonen können demnach gegen Unternehmen hohe Geldstrafen verhängt oder in besonders gravierenden Fällen sogar die Liquidierung des Unternehmens angeordnet werden. Die Rechtsordnungen benachbarter europäischer Länder kennen Unternehmensstrafen ebenfalls.[2]

Dem deutschen Strafrecht ist die Strafbarkeit juristischer Personen hingegen fremd. Die politische Diskussion um die Einführung eines Unternehmensstrafrechts dauert seit Jahren ohne konkrete Ergebnisse an. Der Koalitionsvertrag zwischen CDU, CSU und SPD zur 18. Legislaturperiode vom 16.12.2013 verhält sich dazu wie folgt:

> *„Mit Blick auf strafbares Verhalten im Unternehmensbereich bauen wir das Ordnungswidrigkeitenrecht aus. Wir brauchen konkrete und nachvollziehbare Zumessungsregeln für Unternehmensbußen. Wir prüfen ein Unternehmensstrafrecht für multinationale Konzerne."*[3]

Da derzeit noch kein Koalitionsvertrag zur 19. Legislaturperiode vorliegt, hilft ein Blick in die Regierungsprogramme der CDU/CSU[4] und der SPD.[5] Das Regierungsprogramm der CDU/CSU verhält sich, soweit ersichtlich, überhaupt nicht zur Sanktionierung von Unternehmen. Das Regierungsprogramm der SPD spricht nicht ausdrücklich von Plänen, ein Unternehmensstrafrecht einzuführen, wohl aber über Anpassungen einschlägiger bereits bestehender Vorschriften:

> *„Zudem stellen wir die Sanktionen für kriminelle Verfehlungen von Unternehmen auf eine neue gesetzliche Grundlage. Dafür schaffen wir Kriterien, um*

[1] Vgl. hierzu ausführlich den Beitrag von Fleischmann/Wittenburg zu Korruptionsstrafgesetz, Foreign Corrupt Practices Act und UK Bribery Act im Vergleich in diesem Buch.

[2] Vgl. nur das seit 2005 in Österreich geltende Verbandsverantwortlichkeitsgesetz (VbVG).

[3] Koalitionsvertrag der 18. Legislaturperiode, Ziff. 5.1 Abs. 6.

[4] Vgl. Regierungsprogramm der CDU und CSU, 2017, Für ein Deutschland, in dem wir gut und gerne leben, https://www.cdu.de/system/tdf/media/dokumente/170703regierungsprogramm2017.pdf, Zugriff 14.08.2017, S. 1-76.

[5] Vgl. Regierungsprogramm der SPD, 2017, Zeit für mehr Gerechtigkeit, https://www.spd.de/fileadmin/Dokumente/Regierungsprogramm/SPD_Regierungsprogramm_BTW_2017_A5_RZ_WEB.pdf, 14.08.2017, S. 1-116.

den Strafverfolgungsbehörden und Gerichten ausreichend scharfe und zugleich flexible Sanktionsmöglichkeiten an die Hand zu geben. Die geltende Bußgeldobergrenze von 10 Millionen Euro ist für kleinere Unternehmen zu hoch und für große Konzerne zu niedrig. Wir werden daher eine flexible Bußgeldobergrenze einführen."[6]

Damit korrespondieren Äußerungen des ehemaligen Bundesjustizministers Heiko Maas. Er äußerte, dass unternehmensbezogene Straftaten „grundsätzlich, fair und mit angemessenen Sanktionen" geahndet werden sollen.[7]

Einer Erhebung der Nichtregierungsorganisation Transparency International zufolge wollen „über drei Viertel der Wahlberechtigten in Deutschland" ein Unternehmensstrafrecht.[8]

Auf wissenschaftlicher Ebene befasst sich u.a. die Forschungsgruppe Verbandsstrafrecht an der Universität zu Köln mit Möglichkeiten, unternehmensbezogene Sanktionen unter besonderer Berücksichtigung strafprozessualer Fragen sinnvoll und ohne Friktionen in das bestehende straf- und ordnungswidrigkeitenrechtliche Regime zu integrieren.[9]

Es gilt demnach bis auf weiteres der Grundsatz, dass eine Bestrafung ein schuldhaftes Verhalten voraussetzt (*nulla poena sine culpa*). Zu schuldhaftem Handeln im Sinne eines „Dafür-Könnens" sind allein natürliche Personen in der Lage.

Dies bedeutet indes nicht, dass straf- und ordnungswidrigkeitenrechtlich relevantes Fehlverhalten von Mitarbeitern und Leitungspersonen für einen Verband nach geltendem Recht sanktionslos wäre. Vielmehr bestehen verschiedene, mitunter parallelgeschaltete, Zurechnungs- und Sanktionsregimes, die eine empfindliche Ahndung und faktisch harte Sanktionierung von Unternehmen bei Compliance-Verstößen ermöglichen. Im Fokus

[6] Regierungsprogramm der SPD, 2017, S. 73 Abs. 5.

[7] Gastbeitrag von Heiko Maas, vgl. Maas, H., 16.09.2017, Wirtschaftskriminalität muss härter bestraft werden, in: Die Welt Online, https://www.welt.de/debatte/kommentare/article168692359/Wirtschaftskriminalitaet-muss-haerter-bestraft-werden.html, Zugriff 18.10.2017. Dessen Kritik an angeblich mangelnden Sanktionsmöglichkeiten bei „Gewinnen aus krummen Geschäften" geht jedoch mit Blick auf § 17 Abs. 4 OWiG fehl, vgl. auch nachstehend Abschnitte 2.5.2 sowie 3.1.

[8] Transparency International Deutschland e. V., 14.09.2017, Umfrage: Wählerinnen und Wähler wollen Unternehmensstrafrecht und transparenten Lobbyismus, mit Verweis auf eine im Auftrag von Transparency International durch infratest dimap durchgeführte repräsentative Studie vom September 2017, https://www.transparency.de/aktuelles/detail/article/umfrage-waehlerinnen-und-waehler-wollen-unternehmensstrafrecht-und-transparenten-lobbyismus/, Zugriff 18.10.2017.

[9] Näheres zum „Kölner Modell" unter http://www.verbandsstrafrecht.jura.uni-koeln.de/.

steht dabei die Verbandsgeldbuße nach § 30 Ordnungswidrigkeitengesetz (OWiG). Diese ist spätestens seit der Siemens-Korruptionsaffäre[10] ein von den Ermittlungsbehörden und Gerichten regelmäßig angewendetes und von Praktikern geschätztes Sanktionsmittel. Es ist sowohl Aufsichtsräten und geschäftsführenden Organmitgliedern als auch Compliance-Professionals weit überwiegend bekannt. Daneben bestehen aber auch noch weitere, weniger bekannte Rechtsfolgen, die ein Unternehmen im Fall eines individuellen Fehlverhaltens von Mitarbeitern treffen können und daher zumindest als Sanktion im weiteren Sinne zu verstehen sind.

Der folgende Beitrag gibt einen Überblick über die Verbandsgeldbuße und weitere praxisrelevante Sanktionsmechanismen bei Compliance-Verstößen im Unternehmen sowie zu aktuellen rechtlichen Entwicklungen.

2 Verbandsgeldbuße (§ 30 OWiG)

Zentraler Anknüpfungspunkt bei der Frage der Sanktionierung von Unternehmen ist, wie vorstehend bereits angedeutet, die in § 30 OWiG geregelte Unternehmens- bzw. Verbandsgeldbuße. Hierbei handelt es sich um eine Regelung, die ein eigenständiges Sanktionsmittel gegen das Unternehmen als solches enthält. § 30 OWiG schafft also die Möglichkeit einer unmittelbaren Sanktionierung eines Unternehmens in Form einer Geldbuße.

Der Hauptzweck des § 30 OWiG liegt darin, juristische Personen und Verbände in Bezug auf die aus einer Straftat oder Ordnungswidrigkeit resultierenden Sanktionen mit natürlichen Personen gleichzustellen. Es soll verhindert werden, dass der nur durch ihre Organe handlungsfähigen juristischen Person zwar die Vorteile der in ihrem Interesse vorgenommenen Betätigung zufließen, sie jedoch nicht den Nachteilen ausgesetzt ist, die als Folge von Rechtsverstößen beim Einzelunternehmer eintreten können.[11] Weiterer Zweck der Vorschrift ist es, die Verantwortlichen eines Unternehmens dazu anzuhalten, bei der Auswahl der Organe die im Geschäftsleben notwendige Sorgfalt zu beachten, v.a. auf deren Rechtschaffenheit zu achten.[12]

Letztendlich soll über § 30 OWiG das Vermögen des betroffenen Unternehmens so für das Verschulden einer Leitungsperson haften, als wäre es dessen Vermögen.[13]

[10] Vgl. zum gesamten Komplex: Graeff, P./Schröder, K./Wolf, S. (Hg.), 2009, Der Korruptionsfall Siemens, Baden-Baden, Nomos.

[11] Vgl. BT-Drs. 5/1269, S. 59.

[12] Vgl. GJW/Niesler, 1987, OWiG, § 30 Rn. 1; vgl. BGH NJW-RR 1987, 637.

[13] Vgl. BGH wistra, 1986, 221.

Risikobasiertes Pre-Employment-Screening[1]

Bernhard Maier

[1] Der folgende Beitrag basiert auf einer erfolgreich abgeschlossenen Masterarbeit im Rahmen des Masterstudienganges Risk Management and Corporate Security an der FH Campus Wien.

1 Einleitung

Unter Pre-Employment-Screening (PES) ist die Überprüfung von Bewerbern zu verstehen, ehe diese in ein Unternehmen eintreten. Dabei werden Informationen aus öffentlichen Registern und anderen Quellen eingeholt, Ausbildungszeugnisse und die Angaben im Lebenslauf überprüft und ggf. persönliche Gespräche mit Referenzpersonen geführt. Die Überprüfung bezieht sich grundsätzlich nur auf Sicherheitsaspekte. Es gilt also zu klären, ob die betreffende Person ein absehbares Sicherheitsrisiko darstellt, wenn es zu einer Beschäftigung kommt. Abzugrenzen ist PES von der Überprüfung, in welchem Ausmaß Bewerber für die angestrebte Position qualifiziert sind (Ausbildung, Berufserfahrung, Soft Skills usw.). Dies ist eine Aufgabe, die im Personalbereich anzusiedeln ist, und nichts mit PES zu tun hat.

V.a. im angloamerikanischen Raum nutzen zahlreiche Unternehmen PES als Präventionswerkzeug, um Fraud- und Security-Risiken zu minimieren. Es gibt daher reichlich Literatur zu diesem Thema und einen Prozessstandard, der von der US-Security-Vereinigung ASIS entworfen wurde und eine Anleitung für die Durchführung von PES ist.[2] Es wird in diesem Standard und in den meisten Fachbeiträgen im Stil einer Checkliste vorgegeben, welche Informationsquellen bei der Überprüfung von Bewerbern zu nutzen sind. Dabei werden häufig behördliche Register (z.B. Register zivilgerichtlicher Verfahren) genannt, die in den USA öffentlich zugänglich sind, in Deutschland aber aus Datenschutzgründen nicht eingesehen werden dürfen. Aus diesem Grund erweist sich die operative Ausrichtung des ASIS-Standards und anderer in der Literatur genannter Checklisten als Nachteil, wenn es um Screenings außerhalb der USA geht. Deutlich wird aber an dieser Stelle, dass ein PES-Prozess-Modell auf operative Elemente (Nennung von bestimmten Informationsquellen im Checklisten-Stil) verzichten muss, soll es denn universell einsetzbar sein. Ein solches Modell, das sich strategisch dem Thema PES annähert, ist in der Literatur bis jetzt nicht zu finden.

Im deutschsprachigen Raum ist die Überprüfung von Bewerbern bei weitem weniger gängig. Bei Sichtung der Literatur ist eine geringere Anzahl an Fachbeiträgen zu finden. Diese widmen sich vorwiegend rechtlichen Fragen von PES.[3] Rechtlich betrachtet, insbesondere hinsichtlich Daten- und Privatsphärenschutz, gibt es in Deutschland und anderen europäischen Staaten zwei wesentliche Anforderungen, nämlich Relevanz und

[2] Vgl. ASIS, 2009, Pre-Employment Background Screening ASIS GDL PBS-2009, ASIS.

[3] Vgl. Deloitte & Touche, 2012, Risikominimierung bei der Personalauswahl, http://www2.deloitte.com/content/dam/Deloitte/de/Documents/finance/Studie-Risikominimierung-bei-der-Personalauswahl.pdf, Zugriff 05.04.2017, S. 1-31, S. 15.

Angemessenheit. PES darf nur durchgeführt werden, wenn sich die Überprüfung auf relevante Informationen bezieht. Zudem muss das Ausmaß der Informationsbeschaffung der Position angemessen sein, die der Bewerber anstrebt.[4]

> ***Beispiel**: Die Überprüfung des Gesundheitszustands des Partners eines Bewerbers wird vermutlich meist als irrelevant anzusehen sein. Dieser Punkt mag zwar für prospektive Arbeitgeber von Interesse sein, da bei schlechtem Gesundheitszustand der Partnerin oder des Partners mit häufigerer Abwesenheit des Mitarbeiters zu rechnen ist. Abgesehen davon, dass solche Faktoren bei Erteilung einer Beschäftigungszusage oder -absage im europäischen Rechtsraum rechtlich unzulässig sind, haben sie keine Sicherheitsrelevanz und sind aus diesem Grund beim PES nicht zu berücksichtigen.*

> ***Beispiel**: Die Angemessenheit des Screenings leitet sich aus der Position ab, die angestrebt wird. Als unangemessen ist umfassende Informationsbeschaffung anzusehen, wenn die Position mit geringer Eigenverantwortung und wenig Ausbildungsanforderung behaftet ist.*

Mit der Einschränkung der Durchleuchtung von Bewerbern auf Relevantes in angemessenem Ausmaß soll der Interessenkonflikt, der PES immanent ist, beigelegt werden. Prospektive Arbeitgeber wollen einerseits möglichst umfassend über Bewerber informiert sein. Dem steht andererseits das Interesse von Bewerbern gegenüber, die ihre Privatsphäre geschützt wissen wollen. Wenn nur in relevantem und angemessenem Ausmaß gescreent wird, ist beiden Positionen genüge getan. Soweit die Theorie. Die praktische Frage aber, wie das Security oder Fraud Management feststellen kann, was im Einzelfall als relevant und angemessen bei der Durchführung von PES gilt, bleibt unbeantwortet. Es fehlt an einem Messinstrument, das nachvollziehbar Vorgaben macht, in welchem Ausmaß in die Privatsphäre von Bewerbern eingedrungen werden darf.

Mit dem in der Folge dargestellten Instrument der Risikoprofil-Matrix werden die zuvor genannten Anforderungen unter einen Hut gebracht. Die Risikoprofil-Matrix ist ein Managementinstrument, das strategische Vorgaben macht, indem Screening-Ziele definiert werden. Ein solches Ziel könnte bspw. lauten, mit mittlerer Intensität die finanziellen Verhältnisse eines Bewerbers zu untersuchen. Der konkrete Weg der Informationsbeschaffung, also die operative Umsetzung bleibt offen. Damit ist auf der einen Seite die Risikoprofil-Matrix als Managementinstrument universell einsetzbar und unabhängig davon, welche Informationsquellen und Möglichkeiten des Zugriffs auf diese Information in einer bestimmten Jurisdiktion bestehen. Auf der anderen Seite genügt die Risikoprofil-Matrix auch den rechtlichen Anforderungen der Relevanz und Angemes-

[4] Vgl. Williams, A., 2014, Opportunity makes a thief, in: Loss Prevention Magazine, S. 19 ff.

senheit von PES. Die Risikoprofil-Matrix bildet das Ergebnis einer Risikobeurteilung der vakanten Position ab. Die Beurteilung zeigt auf, in welchen Bereichen Risiko besteht, und gibt Auskunft über das Ausmaß des Risikos. Aus dieser Erkenntnis leitet das Security oder Fraud Management die Breite (welche Informationen sind relevant?) und die Tiefe (wie intensiv muss nachgeforscht werden?) des Screenings ab. Damit wird die Integrität der Privatsphäre von Bewerbern und deren Recht auf informationelle Selbstbestimmung weitestgehend gesichert. Somit ist die Risikoprofil-Matrix nicht bloß ein Werkzeug des Security oder Fraud Managements, sondern darüber hinaus auch ein Compliance-Instrument.

2 Strategisches PES

2.1 Die sechs Risikodimensionen im PES

Bei Durchsicht der Literatur können häufig Checklisten gefunden werden, also Listen mit abzufragenden Informationen.[5] Wie bereits erwähnt, will der vorliegende Beitrag den Sprung von der operativen auf die strategische Ebene des Security oder Fraud Managements aufzeigen. Um dorthin zu gelangen, ist die Frage zu stellen, welche Lebensbereiche die verschiedenen Informationsquellen abdecken und was sie aussagen. Was soll überprüft werden, wenn Informationen aus dieser oder jener Quelle eingeholt werden, und worauf weisen die ermittelten Informationen hin?

Beispiel: *Die im zuvor erwähnten ASIS-Standard bestehende Vorgabe, Nachforschungen in der Gerichtsdatenbank im Wohnortbezirk des Bewerbers durchzuführen,[6] bezweckt die Überprüfung der Integrität. Eine andere Vorgabe, die häufig in amerikanischer PES-Literatur zu finden ist, ist die Überprüfung der Sozialversicherungsnummer. Diese Maßnahme verfolgt den Zweck, Sicherheit über die Identität von Bewerbern zu erlangen.*

[5] Solche Checklisten sind bspw. zu finden bei: Rosen, L.S., 2012, The Safe Hiring Manual, BRB Publications, Tempe, AZ, S. 245 ff.; Kirby, S.L., 2013, The art of the background, in: Blake, W.F. (Hg.), A manual of private investigations techniques, Charles C. Thomas, Springfield, IL, S. 257-266, S. 259 ff.; Ferraro, E.F., 2006, Investigations in the workplace, Taylor & Francis Group, Boca Raton, FL, S. 442 ff.; DeMey, D.L., 2001, 25 essential lessons for employee management, Facts on Demand Press, Tempe, AZ, S. 57 ff.; Preining, W., 2000, Betriebsspezifische Bedrohungen, in: Edelbacher, M./Reither, P./Preining, W. (Hg.), Sicherheits-Management, Linde, Wien, S. 97-316, S. 202 ff.; Colaprete, F.F., 2012, Pre-employment background investigations for public safety professionals, CRC Press, Boca Raton, FL, 165 ff.

[6] Solche Nachforschungen sind in den USA möglich, in Deutschland hingegen rechtlich unzulässig.

Die Bekämpfung von Arzneimittelfälschungen[1]

Daniel Moser

[1] Bei diesem Beitrag handelt es sich um eine Projektarbeit, die im Sommer 2015 vom Autor im Rahmen seines Zertifikatstudienganges zum Certified Fraud Manager erstellt wurde. Der Inhalt wurde vom Autor für die Veröffentlichung in diesem Buch an aktuelle Entwicklungen angepasst und hinsichtlich der Zeitpunkte von Entwicklungsständen/Erscheinungsdaten und Titeln der zitierten Normen aktualisiert. Die in diesem Beitrag enthaltenden Interviews wurden auf Wunsch der Institutionen für die Veröffentlichung dieses Buches anonymisiert.

1 Einleitung

Der Begriff der Arzneimittelfälschung wird von der Weltgesundheitsorganisation (WHO) durchaus weit gefasst interpretiert (siehe Abschnitt 2). Bereits 1985 wurde das Thema Arzneimittelfälschung als wachsendes Problem und Gefahr für die Menschen und die Gesellschaft erkannt. Seit diesem Zeitpunkt hat die WHO begonnen, mittels Konferenzen, an denen sowohl Regierungsbehörden als auch Vertreter der Industrie teilnehmen, Lösungen zu suchen und die Probleme in Bezug auf Arzneimittelfälschung zu bekämpfen. Als eines der Resultate daraus wurde die International Medical Products Anti-Counterfeit Taskforce (IMPACT) gegründet. Dass die Thematik der Arzneimittelfälschungen ein wachsendes Problem darstellt, lässt sich durch Schätzungen aus Berichten der WHO darstellen, wonach der jährliche Umsatz von gefälschten Arzneimitteln mit 75 Mrd. USD angegeben wird.[2]

Arzneimittelfälschungen haben derart große Konsequenzen auf die Gesellschaft, dass Regierungen, die Industrie und der Konsument entsprechende Gegenmaßnahmen treffen müssen. Gefälschte Arzneimittel sind eine Bedrohung für die Gesellschaft, die Wirtschaft und die Gesetzgebung und können nur durch eine effiziente Zusammenarbeit zwischen der pharmazeutischen Industrie, den Regulatoren und Behörden wie dem Zoll oder der Polizei gelöst werden.

In einem ersten Schritt gibt dieser Beitrag ein Verständnis über die aktuellen Themen und Definitionen, welche die Problematiken der Arzneimittelfälschungen beschreiben. Weiter schafft dieser Artikel einen Überblick sowohl über die nationalen wie auch die internationalen gesetzlichen Grundlagen. In Bezug auf nationale Gesetze und Grundlagen wurde das Schweizer Regelwerk als Hauptreferenz ausgewählt. Nichtsdestotrotz richtet diese Arbeit den Hauptfokus darauf, wie die Gesetze zur Bekämpfung von Arzneimittelfälschungen in der Praxis angewendet werden. Als zentrales Element hinterfragen und diskutieren wir, ob die internationale Gesetzgebung und die Umsetzungspraxis für den Kampf gegen das Verbrechen der Arzneimittelfälschungen geeignet ist. Zusätzlich untersucht dieser Beitrag, ob die Kooperation zwischen Behörden und anderen Interessensparteien ausreichend ist, um die Bevölkerung aber auch das geistige Eigentum der Firmen zu schützen.

[2] Vgl. Obi-Eyisi, O./Wertheimer, A. I., 2012, The Background and History of Counterfeit Medicines, in: Wang, P. G./Wertheimer, A. I. (Hg.), Counterfeit Medicines – Policy, Economics and Countermeasures, Verlag ILM Publications, St. Albans, S. 5.

Um diese Fragen beantworten zu können, werden wir sowohl mit Behörden wie auch mit privaten Personen und Mitarbeitern der Industrie über die Problematik der Arzneimittelfälschung sprechen. Ziel ist es, die aktuelle Lage und den abschließenden Umgang mit dieser Situation zu verstehen.

2 Definition der Arzneimittelfälschung

Obwohl die Definition der Arzneimittelfälschung in Gesetzesgrundlagen gefunden werden kann, gibt es aktuell keine universelle Definition. Um die Welt auf das globale Problem aufmerksam zu machen, hat die WHO folgende Definition für Arzneimittelfälschung erlassen:

> *„Ein gefälschtes Arzneimittel ist eines, welches absichtlich und betrügerisch hinsichtlich der Identität und Herkunft falsch deklariert ist. Sowohl Marken- wie auch Generikaprodukte können Gegenstand von Fälschungen sein und sie können die richtigen oder falschen Zutaten, eine ungenügende Menge oder gar keine Wirkstoffe beinhalten, oder schlicht über eine gefälschte Verpackung verfügen."*[3]

3 Gesundheitsrisiken für die Bevölkerung

Um die Risiken für die Gesundheit der Bevölkerung, welche von gefälschten Arzneimitteln ausgehen, bestimmen zu können, muss man zwischen medizinischen Produkten, welche über

1. die korrekte Menge an Wirkstoffen,
2. die inkorrekte Menge oder über überhaupt keine Wirkstoffe verfügen und
3. lebensgefährliche und/oder kontaminierte Substanzen beinhalten

unterscheiden. Jede genannte Version wird untenstehend kurz behandelt:

- zu 1: Arzneimittelfälschungen mit der korrekten Menge an Wirkstoffen, wie z.B. gestohlene und wiederverpackte Originalprodukte, stellen bis auf den Fall, wo sie falsch gelagert werden und somit durch ungenügende Kühlung wirkungsarm werden, normalerweise kein substantielles Gesundheitsrisiko für die Bevölkerung dar.[4]

[3] WHO, 29.05.2017, Definitions of Substandard and Falsified (SF) Medical Products, http://www.who.int/medicines/regulation/ssffc/definitions/en/, Zugriff 18.08.2017.

[4] Vgl. Interview mit einem großen Pharmakonzern, 11.09.2015, Head of Anti-Counterfeit, Interviewer: Daniel Moser.

Unternehmensinterne Täterermittlung mit Unterstützung kriminalpsychologischer Methoden

Jens Hoffmann/Peter Zawilla

1 Einleitung

Die Aufgaben und der Zuständigkeitsbereich im Rahmen des Fraud Managements bzw. in der Internen Revision umfassen im Zusammenhang mit anlassbezogenen (unternehmensinternen) Ermittlungen bzw. Sonderuntersuchungen die Untersuchung von Auffälligkeiten und Unregelmäßigkeiten sowie die Feststellung und Bewertung der entsprechenden Verantwortlichkeiten. Diese Aufgaben werden insbesondere bei Ermittlungen im Zusammenhang mit internen Tätern durch die Interne Revision wahrgenommen.[1] Dabei ist gerade die Identifizierung und Zuordnung der Verantwortlichkeiten bspw. bei Fällen von Cybercrime[2] oder die Urheberschaft bei anonymen Hinweisen[3] mit denunzierenden oder beleidigenden Inhalten[4] nicht immer mit den „traditionellen" revisorischen bzw. unternehmensinternen Ermittlungs-/Prüfungsansätzen zu erreichen.

Im Zeitalter der Digitalisierung von Daten[5] bietet insbesondere auch das Internet Tätern zahlreiche Möglichkeiten, die eigene Identität zu anonymisieren und somit zu verschleiern. Früher boten handgeschriebene Unterlagen noch die Möglichkeit, über Schriftvergleiche die Urheberschaft zu identifizieren (z.B. durch Erstellung von graphologischen Gutachten).

Ausgehend hiervon ist es notwendig, für die Täterermittlung ergänzende methodische Ansätze und Praktiken hinzuzuziehen, die es ermöglichen, über die Grenzen der bisherigen unternehmensinternen bzw. revisorischen Prüfungsmöglichkeiten hinaus im Rahmen der Fallanalyse zusätzliche Erkenntnisse zu generieren, um diese in Kombination mit den Prüfungsergebnissen zur Ermittlung von Tätern mehrwertschöpfend zu nutzen.

Der vorliegende Beitrag beschreibt einen strukturierten methodischen sowie mehrfach praxiserprobten Ansatz, wie es durch das Zusammenwirken von unternehmensinternen Ermittlungen und ergänzenden kriminalpsychologischen Methoden (Profiling) möglich ist, einem ansonsten anonym bleibenden internen Täter auf die Spur zu kommen.

[1] Vgl. Deutsches Institut für Interne Revision e.V. (DIIR), Internationale Grundlagen für die berufliche Praxis der Internen Revision 2017, Zugriff 07.12.2016.

[2] Vgl. den Beitrag von Drießen/Jackmuth/Franosch zu Cyberkriminalität und Angriffsszenarien durch CEO-Fraud in diesem Buch.

[3] Vgl. Glaz-Ocik, J./von Groote, E., 2012, Analyse anonymer Hinweise, in: Jackmuth, H.-W./de Lamboy, C./Zawilla, P. (Hg.), Fraud Management – Der Mensch als Schlüsselfaktor gegen Wirtschaftskriminalität, Frankfurt School Verlag, Frankfurt am Main, S. 613-626, S. 613 ff.

[4] Derartige Hinweise bzw. Schreiben können strafrechtliche Relevanz haben und erfüllen somit für Kreditinstitute den Tatbestand einer „sonstigen strafbaren Handlung" gemäß § 25h KWG.

[5] Vgl. den Beitrag von S. Jackmuth zu Integrierte Datenanalytik im Fraud Management in diesem Buch.

Daneben wird zum einen auf das grundsätzliche fallanalytische Vorgehen bei einem Betrugsverdacht eingegangen, zum anderen werden aktuelle Erkenntnisse der Kriminalpsychologie zu manipulativem und betrügerischem Verhalten vorgestellt.[6]

2 Grundsätzliche Vorgehensweise im Zusammenwirken von unternehmensinternen Ermittlungen und kriminalpsychologischen Methoden

Für jede Sonderuntersuchung sind somit neben dem entsprechenden Fachwissen und der professionellen Erledigung von Routineprüfungstätigkeiten auch größtmögliche Flexibilität, vernetztes Denken, emotionale Intelligenz, Kreativität sowie Intuition, Instinkt und Erfahrung zwingend erforderlich und unerlässlich.

Erfahrungsgemäß stellt sich jeder Einzelfall anders und sehr spezifisch dar. Daher ist es grundsätzlich sinnvoll, die jeweilige Vorgehensweise auch unter strategisch-taktischen Gesichtspunkten zu gestalten und in aufeinander folgende Phasen bzw. Teilschritte aufzuteilen.[7]

Stößt man dann an irgendeiner Stelle der „konventionellen" unternehmensinternen Ermittlungen/Prüfungshandlungen an Grenzen, lohnt es sich immer zu erwägen, inwieweit durch die Hinzuziehung zusätzlicher Expertise – wie bspw. datenanalytischer[8], IT-Forensik-[9] oder kriminalpsychologischer Methoden – neue Impulse für die Ermittlungsarbeit und die Identifizierung von Tätern generiert werden können. Dabei kommt es insbesondere auch auf den richtigen Zeitpunkt sowie auf die enge Zusammenarbeit und den detaillierten Austausch zwischen den verschiedenen Ermittlungsdisziplinen an.

[6] Die Mitarbeit von Dr. Jens Hoffmann zu diesem Buchbeitrag ist u. a. im Rahmen des Projektes „Erkennung von Wirtschaftskriminalität und Versicherungsbetrug (EWV)" mit dem Förderkennzeichen 13N13502 des Bundesministeriums für Bildung und Forschung (BMBF) entstanden. Das Projekt wird gefördert im Zuge der Bekanntmachung „Zivile Sicherheit – Schutz vor Wirtschaftskriminalität" des BMBF im Rahmen des Programms „Forschung für die zivile Sicherheit" der Deutschen Bundesregierung.

[7] Vgl. Zawilla, P., 2012, Vorgehensweise bei Sonderuntersuchungen – Strukturiertes Delikt- und Schadensfallmanagement, in: Jackmuth, H.-W./de Lamboy, C./Zawilla, P. (Hg.), Fraud Management – Der Mensch als Schlüsselfaktor gegen Wirtschaftskriminalität, Frankfurt School Verlag, Frankfurt am Main, S. 719-756, S. 719 ff.

[8] Vgl. den Beitrag von S. Jackmuth zu Integrierte Datenanalytik im Fraud Management in diesem Buch.

[9] Vgl. Becker, S., 2012, Computer-Forensik, in: Jackmuth, H.-W./de Lamboy, C./Zawilla, P. (Hg.), Fraud Management – Der Mensch als Schlüsselfaktor gegen Wirtschaftskriminalität, Frankfurt School Verlag, Frankfurt am Main, S. 805-822, S. 805 ff.

In der Kombination zwischen „konventionellen“ unternehmensinternen Ermittlungen/Prüfungshandlungen sowie ergänzenden bzw. unterstützenden kriminalpsychologischen Methoden hat sich dabei in der Praxis die in Tabelle 1 dargestellte Vorgehensweise in mehreren Phasen bewährt.

Tabelle 1: Darstellung der einzelnen Phasen einer strukturierten Fallbearbeitung unter Einbeziehung der Erstellung eines Täterprofils

Phase	Kurzbezeichnung der Phase
1	Rekonstruktion der konkreten Vorgehensweise sowie des zeitlichen Ablaufes
2	Fallanalytische Bewertung und Erstellung eines Täterprofils
3	Zusammenführung der Ergebnisse aus Tatverlauf und Täterprofil – Eingrenzung des potenziellen (unternehmensinternen) Täterkreises
4	Durchführung von Befragungen: Von Informationsgesprächen zu Konfrontationsgesprächen
5	Auswertung der Erkenntnisse und Ableitung von Maßnahmen/Konsequenzen
6	Erstellung einer (gerichtsverwertbaren) Abschlussdokumentation

Dabei können die Phasen 1 und 2 auch ganz oder teilweise parallel bearbeitet werden, sofern die Erstellung eines Täterprofils durch einen entsprechend hierfür auch qualifizierten (externen) Experten bereits zu Beginn der Fallbearbeitung feststeht bzw. das entsprechende Erfordernis bereits frühzeitig absehbar ist. Dies erhöht selbstverständlich auch die Bearbeitungseffizienz, wobei auch die zeitlich nachgelagerte Hinzuziehung eines Kriminalpsychologen und die Erstellung eines Täterprofils möglich sind.

In den folgenden Ausführungen dieses Abschnitts 2 werden die in der vorstehenden Tabelle skizzierten einzelnen Phasen näher dargestellt und beleuchtet. Die konkrete Anwendung dieser strukturierten Vorgehensweise veranschaulichen die konkreten Praxisfälle im Abschnitt 5 dieses Beitrages.

2.1 Phase 1 – Rekonstruktion der konkreten Vorgehensweise sowie des zeitlichen Ablaufes

Bei Auftreten von Unregelmäßigkeiten bzw. nennenswerten Schadenfällen werden i.d.R. im Rahmen des Schadenfallmanagements unternehmensinterne Sonderprüfungen oder Ermittlungen eingeleitet. Diese werden zumeist von der Internen Revision, teilweise auch von den Bereichen Compliance, Security oder – sofern vorhanden – einer eigenständigen Organisationseinheit für Fraud Management des betroffenen Unternehmens

Die Zeugenaussage – Einflüsse auf die Zeugenaussage und deren Wahrheitsgehalt sowie die Überprüfung der Glaubhaftigkeit einer Aussage[1]

Heidi Arendt/Kirsten Faust

[1] Bei diesem Beitrag handelt es sich um eine Projektarbeit, die im Frühjahr 2012 von den Autorinnen im Rahmen ihres Zertifikatstudienganges zum Certified Fraud Manager (CFM) erstellt wurde. Der Inhalt wurde von den Autorinnen für die Veröffentlichung in diesem Buch an aktuelle Entwicklungen angepasst und hinsichtlich der Zeitpunkte von Entwicklungsständen/Erscheinungsdaten und Titeln der zitierten Normen aktualisiert.

1 Einleitung

„Der Irrtum ist der größte Feind der Wahrheitsfindung vor Gericht."[2]

Schon dieses Zitat des ehemaligen Richters Rolf Bender zeigt sehr deutlich die Schwierigkeiten bei der Reproduktion des tatsächlich Erlebten bzw. Wahrgenommenen.

Bereits der angesprochene Irrtum kann zu einer maßgeblichen Verfälschung der Aussage und somit zu einer Falschdarstellung oder Fehlinterpretation eines Vorfalls führen. Über den Irrtum hinaus gibt es weitere Einflussfaktoren auf den Wahrheitsgehalt von Zeugenaussagen. Im Folgenden sollen diese dargestellt und erläutert werden, um dem Befragenden die Möglichkeit zu geben, die genannten Einflussfaktoren zu erkennen und zu berücksichtigen.

Die Weiterverwendung einer falschen Aussage dient nicht der Sachverhaltsaufklärung. Nur wenn man weiß, wo die Fehlerquellen liegen, kann man diese eliminieren.

In der Strafprozessordnung (StPO) sind vier Beweismittel zugelassen. Man unterscheidet hierbei zwischen dem Personalbeweis, welcher den Zeugen und den Sachverständigen umfasst, und dem Sachbeweis, der sich auf die Urkunde und den Augenschein bezieht.

Der Bundesgerichtshof (BGH) sagt,[3] den tatsächlichen Beweiswert von Aussagen bestimme nicht die verfahrensrechtliche Stellung der Auskunftsperson, sondern deren persönlicher Gesamteindruck, die Art und Weise ihrer Bekundung, die innere Wahrscheinlichkeit ihrer Schilderung und zahlreiche andere Umstände. Nicht nur durch die aussagende Person, sondern auch durch das Umfeld und den Befragenden selbst, ergeben sich Quellen der Aussagebeeinflussung.

Im Rahmen dieses Beitrags soll, neben den Gedächtnisleistungen und -prozessen, welche für die Reproduktion einer Zeugenaussage notwendig sind, auch auf die Beeinflussungsfaktoren durch das Umfeld, den Aussagenden selbst und den Befragenden eingegangen werden. Ferner wird anhand der Vorgaben des BGH[4] gezeigt, mit welcher Methodik ein Gericht die Glaubhaftigkeitsbeurteilung einer Aussage überprüft.

[2] Bender R., Richter am Oberlandesgericht a.D., 1982.

[3] BGHSt 18, 1963, 238, 241.

[4] BGH, 1999, 1StR 618/98.

2 Theoretische Grundlagen

2.1 Einflüsse auf die Wahrnehmung

In Abgrenzung zu der bewussten Falschaussage, der Lüge, existieren verschiedene Einflüsse auf die Wahrnehmung eines Zeugen. Hier wird zwischen Wahrnehmungsfehlern, Erinnerungsfehlern und den Wiedergabefehlern unterschieden.

Zu Wahrnehmungsfehlern kann es bei der ersten Informationsverarbeitung kommen. Ein natürlicher Grund liegt schon darin, dass der betreffende Zeuge z.B. Seh- oder auch Hörstörungen aufweisen könnte. Neben äußeren Einflüssen, wie bspw. der Beleuchtung des Umfelds, der Wetterlage oder auch der Entfernung, kann auch der Gesundheitszustand zu Fehlern führen.[5]

Im menschlichen Gehirn werden zur Speicherung von Erinnerungen oder Wahrnehmungen Muster oder Skripte angelegt. Werden in der Folge neue Informationen aufgenommen, so neigt das Gehirn dazu, diese in der Art der bereits vorhandenen Muster zu strukturieren. Dies erleichtert zwar die Aufnahme von Informationen, hat jedoch zur Folge, dass ähnliche Wahrnehmungen weniger Chancen haben, eigenständig zu bleiben. Ähneln Wahrnehmungen bereits gespeicherten Vorgängen (bspw. Routinehandlung), werden sie angepasst. Je stärker eine Erinnerung platziert ist, umso häufiger kann es vorkommen, dass Abweichungen nicht wahrgenommen werden. Der Mensch folgt dem, was er in Jahrzehnten gelernt, erlebt, gelebt hat bzw. vorgelebt bekam oder aus vermeintlich sicheren Quellen vermittelt erhielt. Abweichungen hierzu werden oftmals durch den Zeugen selbst verworfen.[6]

Die Wahrnehmungsverzerrung ist bei jeder Befragung als latentes Risiko zu berücksichtigen. So stellen Erwartungshaltungen, Motivation oder Vorurteile des Zeugen zu einem bestimmten Ereignis oder einer bestimmten Person bzw. Personengruppe gegenüber Filter der Wahrnehmung dar: „Es kann nicht sein, was nicht sein darf“.[7]

[5] Vgl. Hohlweck, M., 2002a, Beweiswürdigung: Beurteilung von Zeugenaussagen, in: Zeitschrift JuS – Juristische Schulung, Heft 11, S. 1105-1108, S. 1106 f.

[6] Vgl. Bender, R./Nack, A., 1995a, Tatsachenfeststellung vor Gericht, Band 1: Glaubwürdigkeits- und Beweislehre, 2. Auflage, Beck, München, S. 3 ff.

[7] Vgl. Artkämper, H./Schilling, K., 2010, Vernehmungen, VDP Verlag, Unna, S. 26.

Zu Wiedergabefehlern oder Einschränkungen der Erinnerungswiedergabe kann es kommen, wenn eine Intoxikation (Vergiftung, auch durch Medikamente oder Drogen) des Zeugen vorliegt, bzw. bei schwerem körperlichem Entzug.[8]

Besteht die Möglichkeit, dass der Zeuge unmittelbar nach dem Vorfall eine Aussage tätigt, können über das freie Erinnern und Berichten Fehlerquellen, aufgrund von Fremdeinflüssen, minimiert oder sogar ausgeschlossen werden.[9]

Im Anschluss der Zeugenaussage ist ein Abgleich zwischen Aussagekompetenz und Aussagequalität empfehlenswert. Das Ereignis berücksichtigend muss die Frage gestellt werden, ob der Zeuge über die Informationen oder Beschreibungen hätte verfügen können, ohne dass sie auf eigenem Erlebnis basieren.[10]

2.2 Realität und Wirklichkeit

Als Realität bezeichnet man objektiv wahre Aussagen, ungeachtet der Tatsache, ob sie bekannt oder erkennbar sind. Bei der Wirklichkeit handelt es sich um Aussagen, die ein Mensch oder auch eine Gruppe von Menschen für zutreffend hält.

Was für den einen Zeugen Wirklichkeit ist, muss nicht immer der Realität entsprechen.

Die Bilder in Abbildung 1 sollen illustrieren, dass ein Zeuge bspw. die nur virtuellen Konturen dieser Grafiken subjektiv sieht (Wirklichkeit), welche jedoch real nicht vorhanden sind und nur auf Täuschung beruhen. Der Zeuge glaubt, das Quadrat bzw. das Dreieck zu sehen, welche tatsächlich nicht vorhanden sind.

Abbildung 1: Quadrat und Dreieck

[8] Vgl. Bender, R./Nack, A., 1995b, Tatsachenfeststellung vor Gericht, Band 2: Vernehmungslehre, 2. Auflage, Beck, München, S. 277.

[9] Deckers, R./Köhnken, G., 2014, Die Erhebung und Bewertung von Zeugenaussagen im Strafprozess, 2. Auflage, Berliner Wissenschafts-Verlag, Berlin, S. 139.

[10] Deckers, R./Köhnken, G., 2014, S. 142.

Die Realität unterscheidet sich vom Gedachten, Vorgestellten, Erinnerten, Vermuteten, Halluzinierten und Geträumten.[11]

Bei der Bewertung von Zeugenaussagen sollten wir Täuschungen immer als eine verborgene Möglichkeit ansehen. I.d.R. kann der Mensch unterscheiden, ob eine Person real vor ihm gestanden hat oder nicht. Weitaus schwieriger kann es schon sein, ob eine Wahrnehmung bei besonderen Lichtbedingungen ein Schatten oder eine Person war.

2.3 Wahrnehmungs- und Erinnerungsfähigkeit

Neben personenbezogenen Einflüssen auf Zeugenaussagen lassen sich bei der Wahrnehmung und bei der Erinnerung Unterschiede feststellen. Verschiedene Informationen werden durch Zeugen unterschiedlich gut und lange erfasst.

Aus Tabelle 1 ergeben sich Fallgruppen, die tendenziell eher schlecht wahrgenommen werden bzw. eher gut wahrgenommen und erinnert werden können.

Tabelle 1: Wahrnehmung und Erinnerung

Schlechte Wahrnehmung und Erinnerung	Mittelmäßige Wahrnehmung und Erinnerung	Gute Wahrnehmung und Erinnerung
Zeit, Dauer	Chronologie	Zuordnung von Verhalten zu Personen
Menge, Volumen	räumliche Verhältnisse	Tatgegenstände
Größe		kleine Personengruppen
Farbe		bekannte Stimmen
große Personengruppen		Neuheiten und Auffälligkeiten
unbekannte Stimmen		
Entfernungen, Abstände		
Unangenehmes		
Standardsituationen		
räumliche Einordnung von Geräuschen		

Quelle: Artkämper, H./Schilling, K., 2010, S. 27.

[11] Vgl. Fabian, A./Fabian, T./Greuel, L./Offe, H./Offe, S./Stadler, M./Wetzels, P., 1998, Glaubhaftigkeit der Zeugenaussage, Beltz, Weinheim, S. 20 f.

Cyberkriminalität und Angriffsszenarien durch CEO-Fraud

Maria Drießen/Rainer Franosch[1]/Hans-Willi Jackmuth

[1] Der Mitautor ist Leitender Ministerialrat und als stellvertretender Abteilungsleiter im Hessischen Ministerium der Justiz u.a. für Cybercrime zuständig. Er war zuvor Leiter der Hessischen Zentralstelle zur Bekämpfung der Internetkriminalität. Der Beitrag gibt ausschließlich seine persönliche Auffassung wieder.

1 Einleitung

Als Cybercrime (früher „Informations- und Kommunikationskriminalität“ oder auch verkürzend „Internetkriminalität“) bezeichnet man alle kriminellen Handlungen, die

- gegen elektronische Kommunikationsnetze und Informationssysteme (Cybercrime im engeren Sinn, englisch: cyber-dependent crimes, z.B. Datenveränderung (§ 303a Strafgesetzbuch (StGB)), Ausspähen von Daten (§ 202a StGB) etc.) oder
- mittels derartiger Netze und Systeme verübt werden (Cybercrime im weiteren Sinn, englisch: cyber-enabled crimes, also Taten, bei denen das Internet als virtuelles Tatwerkzeug für die Begehung von Straftaten genutzt wird, z.B. Verbreitung von Kinderpornografie, Volksverhetzung, Verbreitung extremistischer Propaganda, öffentliche Aufforderung zu Straftaten, betrügerisches Anbieten von Waren und Dienstleistungen oder Geldanlagen, verbotenes Glücksspiel, unlautere Werbung, Urheberrechtsverletzungen, Verkauf von Waffen, Betäubungsmitteln oder verbotenen Medikamenten).

Die meisten Internetstraftaten sind Betrugsdelikte (Anteil in der Polizeilichen Kriminalstatistik 2016: 72,5%)[2]. Die besonderen Herausforderungen des Kriminalitätsfeldes Cybercrime resultiert aus den technischen Charakteristiken des Internets und spiegeln sich in der oben getroffenen Unterscheidung zwischen cyber-dependent und cyber-enabled wider.

Beide Aspekte werden nachfolgend anhand zweier ausgewählter Phänomene kurz beleuchtet. Schließlich werden die Verwendung klassischer Tatbegehungsweisen im Zeitalter elektronischer Kommunikation am Beispiel des CEO-Fraud dargestellt.

2 Darknet-Marktplätze und die Underground Economy – „cyber-enabled crime“

Als Darknet-Marktplatz wird eine abseits des offenen Internets im Darknet angesiedelte virtuelle Handelsplattform bezeichnet. Der Handel mit illegalen Waren und Dienstleistungen an sich ist dabei kein neues Phänomen. Schon von Beginn an wurde das Internet als Kommunikationsmedium zur Begehung von Straftaten verwendet. Illegale Güter gehörten zu den ersten Gegenständen, die mithilfe des noch jungen Internet gehandelt

[2] Vgl. Bundesministerium des Innern, 2017, Bericht zur Polizeilichen Kriminalstatistik 2016, http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2017/pks-2016.pdf, Zugriff 26.09.2017, S. 1-149, S. 15.

wurden. In den frühen 1970er Jahren nutzten Studenten an der Stanford University und dem Massachusetts Institute of Technology das Internet, damals noch als „Arpanet" bezeichnet, um den Kauf von Cannabis zu koordinieren.[3] In den 1980er Jahren wurden Drogenverkäufe über das Usenet in Gruppen wie „alt.drugs" angebahnt und offline abgewickelt.[4] Seit Anfang der 2000er Jahre wurden Foren für Internethandel mit den Crimeware- und Hackerwerkzeugen immer populärer, wobei schon in frühen Cybercrime- und Cardingforen, wie ShadowCrew, auch Drogen erhältlich waren.

Den Durchbruch bedeutete das Aufkommen des TOR-Netzwerkes. Die Veröffentlichung einer ersten Version des vom United States Naval Research Laboratory entwickelten TOR (Abkürzung für The Onion Routing) – einer Peer-to-Peer-Software, welche zur Wahrung der Anonymität die IP-Adressen der Nutzer verschleiert – im September 2002 ermöglichte erst das Darknet (auch als Deep Web bezeichnet) in seiner heutigen Form. Die TOR-Software bedient sich eines Prinzips, das an eine Zwiebel und ihre Schichten erinnert, woher auch die Bezeichnung rührt. Jede Anfrage wird durch mindestens drei TOR-Server geleitet, ohne dass der jeweilige Server weiß, woher die Anfrage kommt und wohin sie weitergeleitet wird. Zwischen ihnen werden die Informationen verschlüsselt verschickt und können nicht eingesehen werden.

Das TOR-Netzwerk erlaubt aber nicht nur den anonymen Zugriff auf herkömmliche Webseiten, sondern auch die Bereitstellung anonymer und schwer lokalisierbarer Angebote, wobei gleichzeitig die Anonymität der Nutzer durch Verschleierung der Verkehrsdaten gewahrt wird.

Der Zugriff auf diese TOR Hidden Services bzw. TOR Onion Sites erfordert grundsätzlich den Einsatz der TOR-Software. Die TOR-Technologie ermöglicht erstmals einem breiteren Publikum ohne größere IT-Kenntnisse ein anonymes Hosting, also die Einrichtung von Webseiten mit kriminellen Inhalten, deren physikalischer Speicherort für die Strafverfolgungsbehörden nicht ohne Weiteres aufklärbar ist und die nicht, wie sonst allgemein bei WWW-Angeboten möglich, über den Host-Provider abschaltbar sind.

Immer mehr verlagert sich seitdem der Handel mit illegalen Waren und Dienstleistungen unter Nutzung digitaler Währungen wie Bitcoin und mithilfe von Treuhanddiensten in

[3] Vgl. Power, M., 19.04.2013, Online highs are old as the net: the first e-commerce was a drugs deal, The Guardian, https://www.theguardian.com/science/2013/apr/19/online-high-net-drugs-deal, Zugriff 26.09.2017.

[4] Vgl. Howell O'Neill, P., 15.02.2015, The uncensored history of the Internet's drug revolution, The Kernel, http://kernelmag.dailydot.com/issue-sections/features-issue-sections/11680/hive-silk-road-drugs-history/, Zugriff 26.09.2017.

das Internet. Im Februar 2011 ging die Darknet-Plattform Silk Road ans Netz; vom später verhafteten Betreiber, dem US-Amerikaner Ross Ulbricht, offen als „Amazon für Drogen“ beworben.

Die zunehmend arbeitsteilig funktionierende Cyberunterwelt wird zu Recht als Underground Economy bezeichnet. Täter kaufen und verkaufen illegale Waren und Dienstleistungen, finden sich zu international agierenden Banden zusammen, ohne sich ein einziges Mal im wahren Leben getroffen zu haben. Es existiert ein funktionierender globaler Markt, auf dem Angriffswerkzeuge, Erkenntnisse über Schwachstellen in Betriebssystemen oder Schadsoftware eingekauft oder als Dienstleistung in Auftrag gegeben werden können (Crime-as-a-Service).

Sogar Auftragsmörder bieten ihre Dienste im Darknet an. Dies war aus US-amerikanischen Ermittlungsverfahren schon bekannt. Auch in Hessen hat es inzwischen einen derartigen Fall gegeben:

Im Frühjahr 2014 kam der Angeschuldigte A via Internet über das Darknet in Kontakt mit dem Mitangeschuldigten B. B. war im Forum http://germanyXXX.onion schon seit längerem auf der Suche nach Arbeit und bot gegen lukrative Bezahlung die Erledigung von Diensten aller Art an:

„Fast egal was! Transporter, Mafia, Hitman“

Der Angeschuldigte A beauftragte B über das Internet, gegen Entgelt für ihn das Opfer C zu töten, da dieser seit Mitte März 2014 der neue Lebensgefährte seines Ex-Freundes D war. Die Trennung von D hatte der von massiver Eifersucht sowie Missgunst geplagte A nicht verwunden. Für den geplanten Mord erhielt B eine Anzahlung in Höhe von 3.000 EUR, zusätzliche 10.000 EUR waren als „Erfolgshonorar“ vereinbart worden. B suchte sodann C auf und versuchte, ihm mit einem Messer mit 20 cm langer Klinge die Kehle durchzuschneiden. C konnte mit Hilfe von Zeugen den Angriff abwehren und überlebte mit erheblichen Schnittverletzungen im Hals-, Gesichts- und Schulterbereich sowie an den Händen.

Ohne die Möglichkeit, anonym über das Darknet nach einem Auftragsmörder zu suchen, wäre es dem in kriminellen Dingen völlig unerfahrenen A nicht gelungen, die Verbindung zu einer tatgeneigten Person aufzunehmen.

Die nahezu unbegrenzten Möglichkeiten von Cybercrime führen dazu, dass sich auch die Organisierte Kriminalität zunehmend dieses Bereiches annimmt. Der Drogen- und Waffenhandel über das Internet weist klare Bezüge zur Organisierten Kriminalität auf.

Auf vielen Plattformen wird das Thema angesprochen und v.a. die Frage, wie man sich vor solchen Angriffen schützen kann, diskutiert. Auch der ASW Bundesverband[17] brachte im Jahr 2016 ein Leitblatt zum Thema CEO-Fraud heraus, um somit eine Hilfestellung für die Unternehmen zu leisten. Gleichzeitig veröffentlichen das BKA und die einzelnen LKAs kontinuierlich Sicherheitshinweise bei neu auftretenden Fällen; sie geben auch Ratschläge zum Thema Prävention und Reaktion in Bezug auf CEO-Fraud. Letztlich stehen die Unternehmen aber immer noch selbst in der Verantwortung, ihre Mitarbeiter zu sensibilisieren.

4.2 Definition CEO-Fraud

CEO-Fraud, *Fake President* oder ins Deutsche übersetzt auch „Chef-Betrug" beschreibt einen Vorgang, bei dem ein Mitarbeiter eine E-Mail und/oder einen Anruf vermeintlich von einer Person der höchsten Führungsebene des eigenen Unternehmens erhält.[18] In dieser E-Mail fordert der vermeintliche Absender den Mitarbeiter auf, einen hohen Geldbetrag auf ein ausländisches Konto, meist in Asien oder in Osteuropa, zu transferieren, um z.B. einen Unternehmensverkauf oder eine größere geschäftliche Transaktion zu unterstützen.[19] Ein weiteres Charakteristikum dieses Angriffes ist die Aufforderung zur absoluten Diskretion, der Definition eines definierten Rückkommunikationskanals („Bitte antworten Sie immer nur auf diese E-Mail, damit wir keine anderen Mitlesenden haben") und wird unterstützt durch häufig in schwer verständlichem Wirtschaftsenglisch abgefasste Vertraulichkeitserklärungen.

Diese vorsätzliche Beeinflussung von im Unternehmen handelnden Personen (Social Engineering[20]) als ein wesentlicher Faktor beim CEO-Fraud basiert i.d.R. auf der gründlichen Recherche vor dem eigentlichen Angriff. Investitionen in eine derartige Vorbereitung spielen monetär oftmals keine Rolle, denn die Schäden, die durch CEO-Fraud ausgelöst werden und damit die Vorbereitung „refinanzieren", liegen oftmals pro einzelnen Transaktion im Millionen-Eurobereich.[21] Dennoch sind auch Fälle bekannt,

[17] Allianz für Sicherheit in der Wirtschaft e.V. (ASW Bundesverband) vertritt als Interessenverbund europaweit die Wirtschaft in Sicherheitsfragen gegenüber der Politik und Verwaltung.

[18] Aus Vereinfachungs- und Einheitlichkeitsgründen wird im Folgenden dieses Beitrages ausschließlich der Begriff „CEO-Fraud" verwendet.

[19] Vgl. Bundeskriminalamt (BKA), 16.05.2017, CEO-Fraud. Warnhinweis, https://www.bka.de/SharedDocs/Downloads/DE/IhreSicherheit/CEOFraud.html, Zugriff 26.09.2017.

[20] Vgl. Bédé, A., 2012b, S. 69 ff.

[21] Vgl. Bundeskriminalamt, 16.05.2017.

bei denen nur kleinere Beträge gefordert werden.[22] Die oftmals subtil gewonnenen Informationen werden dazu genutzt, um das Unternehmen und v.a. deren Strukturen intensiv kennenzulernen und Schwachstellen von außen zu erkennen. Es werden extrem intensiv Informationen gesammelt, so dass man dies oftmals mit annäherndem Insiderwissen gleichsetzen kann.

Meist werden als Opfer die Mitarbeiter ausgewählt, die sorglos und nicht unbedingt auf der höchsten Hierarchiestufe (aber nahe an finanziellen Transaktionen) arbeiten und dadurch leichter zu manipulieren sind. Diese Mitarbeiter verfügen allerdings innerhalb des Unternehmens über die (technischen) Berechtigungen, Geldtransfers über die Bankkonten des Unternehmens tätigen/veranlassen zu können. Hinzu kommt oftmals eine Häufung von (Freigabe-)Berechtigungen, damit die vom Täter gewollte betrügerische Transaktion ohne Einschränkungen durchgeführt werden kann. Der Erfolg des Angriffes lässt sich leicht über die Psychologie des Opfers erklären. Eine klare Anweisung auf Diskretion und die vorgespielte Wichtigkeit dieses Auftrages ausgehend vom „Firmenchef" löst in dem Opfer ein Gefühl des Gebrauchtwerdens und des Wichtigseins aus. Dieses Gefühl durch den Täter zu erzeugen, steigert auf der Opferseite die Bereitschaft, an dieser Transaktion von ungeheurer Wichtigkeit teilzuhaben („Dieses Geschäft wird im nächsten Geschäftsbericht stehen und ich werde Teil der Abwicklung") und zugleich absolute Diskretion zu wahren. Außerdem denkt das Opfer an die Aufmerksamkeit der anderen Mitarbeiter, wenn diese erfahren, dass ihm alleine Vertrauen geschenkt wurde, die Transaktionen von suggerierter besonderer Wichtigkeit als „Chefsache" durchzuführen (vgl. Abschnitt 4.6 „Psychologische Sicht"). Ein weiteres Auswahlkriterium kann auch aus der Eitelkeit mancher Mitarbeiter bestehen.[23]

Vom Grundsatz her ist CEO-Fraud letztlich lediglich eine weitere – aufgrund der teilweise extrem hohen Beträge allerdings bedeutsame – Variante eines Zahlungsverkehrsbetruges als weiterer Modus Operandi neben bspw. den bekannten (papierhaften) Überweisungsbetrug, den Lastschriftbetrug oder die in den letzten Jahren zunehmend

[22] Vgl. ASW Bundesverband – Allianz für Sicherheit in der Wirtschaft e.V., 2016, Leitblatt. CEO-Fraud, https://asw-bundesverband.de/fileadmin/user_upload/leitfaden_-blatt/Leitblatt_CEO_fraud_ENG.pdf, S. 1-2, S. 1.

[23] Vgl. Bielefeld, J., 28.02.2017, CEO-Fraud macht Dampf in der Compliance-Diskussion, CB – Compliance-Berater, http://compliance.ruw.de/cb-standpunkte/standpunkte/CEO-Fraud-macht-Dampf-in-der-Compliance-Diskussion-32179, Zugriff 26.09.2017.

aufgekommenen Cybercrime-Variante, des Phishings.[24] Neuartig ist dabei im Wesentlichen die Kombination von Social Engineering mit Cybercrime-Aspekten, die nachstehend ausführlich dargestellt und beleuchtet wird.

4.3 Vorgehensweise der Täter

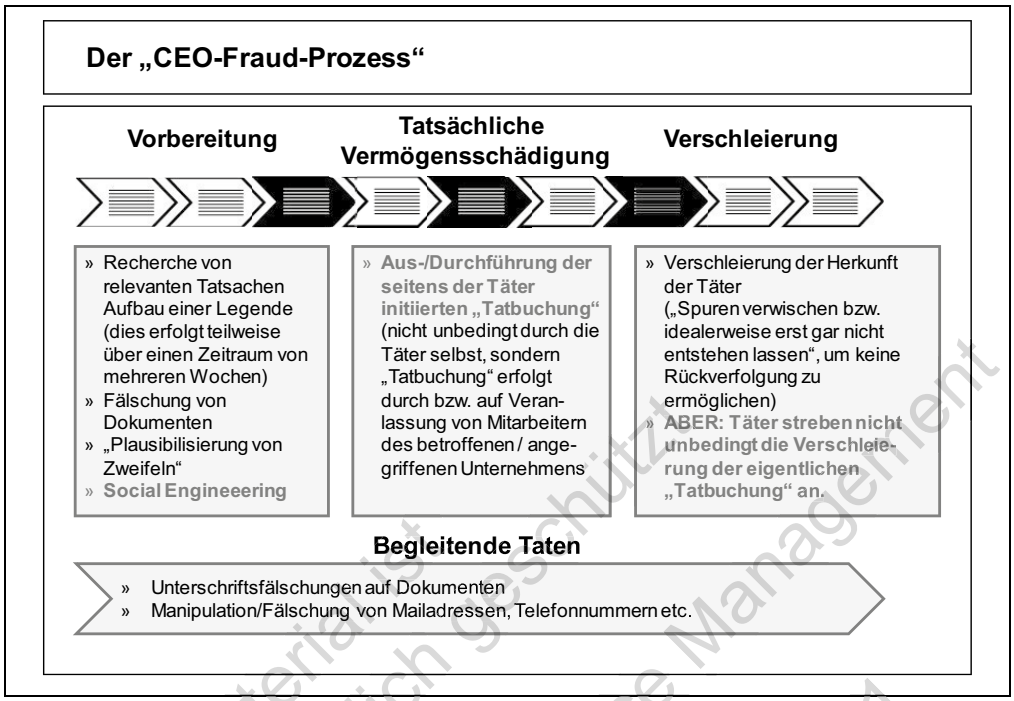
Ein sehr wesentlicher Faktor beim CEO-Fraud ist, dass insbesondere bei den Fällen mit hohen (Millionen-)Beträgen eine sehr sorgfältige Vorbereitung der Täter zu beobachten ist, so dass die „Story", die dann dem Mitarbeiter als für die Transaktion ausgewählter „unkritischer Erfüllungsgehilfe" von den Tätern vorgespielt wird, ein hohes Maß an Fakten enthält, die einzeln betrachtet, durchaus den Tatsachen entsprechen.

Abbildung 3 veranschaulicht die grundsätzliche Vorgehensweise der Täter, die einzelnen Phasen werden in den folgenden Abschnitten noch näher beschrieben.[25]

[24] Phishing bezeichnet den Vorgang, mittels z.B. gefälschter Internetseiten, die den echten Internetseiten von Banken täuschend ähnlich sehen, an vertrauliche Zugangsdaten (PIN und TAN) von Online-Banking-Nutzern zu gelangen. Anschließend werden mit Hilfe der erlangten Daten betrügerische Online-Überweisungen zu Lasten der betroffenen Bankkunden und zu eigenen Gunsten durchgeführt. Vgl. ergänzend Becker, S., 2013, Fraud-Praktiken mittels moderner Zahlungsverkehrspraktiken, in: Jackmuth, H.-W./de Lamboy, C./Zawilla, P. (Hg.), Fraud Management in Kreditinstituten – Praktiken, Verhinderung, Aufdeckung, Frankfurt School Verlag, Frankfurt am Main, S. 195-218, S. 195.

[25] Zum Betrugsprozess vgl. vertiefend Jackmuth, H.-W./de Lamboy, C./Zawilla, P., 2013, Ganzheitliches Fraud Management in Kreditinstituten, in: Jackmuth, H.-W./de Lamboy, C./Zawilla, P. (Hg.), Fraud Management in Kreditinstituten – Praktiken, Verhinderung, Aufdeckung, Frankfurt School Verlag, Frankfurt am Main, S. 1-34, S. 19 f.

Abbildung 3: Der „Betrugsprozess" beim CEO-Fraud[26]



4.4 Vorbereitende Maßnahmen

Die Recherche kann über viele Wege stattfinden. Eine Möglichkeit ist es, sich über verschiedenste Wege Zutritt ins Unternehmen – nicht unbedingt physisch – zu verschaffen. Andere Möglichkeiten können daraus bestehen, harmlose Gespräche auf Messen oder öffentlichen Veranstaltungen mit Mitarbeitern zu führen, um über diese an Informationen zu gelangen. Außerdem gibt es auch genügend Möglichkeiten, über soziale Netzwerke an bestimmte Informationen zu gelangen. Die einfachste Möglichkeit ist es jedoch, öffentlich verfügbare Informationen (wie bspw. in Jahresberichten oder sonstigen Veröffentlichungen des Unternehmens) zu sammeln. Diese können Informationen über mögliche Unternehmensübernahmen, öffentlich bereits bekannte Strategieziele und Investitionen oder Namen von Geschäftspartnern beinhalten.[27]

[26] Zawilla, P., 2016, Präsentation im Rahmen der Veranstaltung Praxisgespräch Compliance im November 2016 in München.

[27] Vgl. Bundeskriminalamt, 16.05.2017.

Integrierte Datenanalytik im Fraud Management

Stefan Jackmuth

1 Einleitung

Ohne Informationstechnologie ist moderne Datenanalyse nicht mehr denkbar. Da die Entwicklungszyklen innerhalb der Informationstechnologie bereits kurz sind und sich selbst weiter beschleunigen, wird dieser Beitrag bei seinem Erscheinen in Teilen bereits veraltet sein. Es ist dennoch sinnvoll, einen Blick auf den nun aktuellen technologischen Stand und die damit verbundenen Konzepte und strategischen Überlegungen zu werfen, was folgendes Zitat verdeutlichen soll:

> *„We should seek out unfamiliar summaries of observational material, and establish their useful properties."*[1]

Dieser Auszug aus der Arbeit „The Future of Data Analysis" von Tukey lässt sich frei mit den Worten übersetzen „wir sollten unbekannte Zusammenhänge in den untersuchten Informationen erkennen und die nützlichen Merkmale ableiten". Die Arbeit wurde bereits 1962 veröffentlicht. Auch wenn der Mensch seitdem den Mond betreten hat, politische Systeme gefallen sind und Dinge wie Smartphones das alltägliche Leben verändert haben, sind große Teile und grundsätzliche Denkansätze von Tukey bis heute aktuell.

Datenanalytik hat sich in Methoden und Technologien über die Jahre dennoch grundlegend verändert. Bereits im 17. Jahrhundert machte sich die niederländische Versicherungsbranche die manuelle Analyse von Alterstabellen mittels statistischer Modelle zunutze.[2] Trotz der grundlegend gewandelten Methodik und Werkzeuge ist das Ziel der Analyse in vielen Fällen gleichgeblieben: Daten sollen als Basis für unternehmerische Entscheidungen dienen. Seit den 1950er-Jahren wurden durch die rasanten Entwicklungen in der Informationstechnologie diverse Ansätze in der Datenanalyse verfolgt und weiterentwickelt. Folgende begriffliche Generationen können, nach Davenport, mehr oder minder exakt eingeteilt werden:[3]

[1] Tukey, J. W., 1962, The Future of Data Analysis, in: The Annals of Mathematical Statistics, Vol. 33, No. 1, S. 1-67.

[2] Vgl. Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV), 16.11.2015, Infografik – Die Geschichte der Datenanalyse, http://www.gdv.de/2015/11/infografik-die-geschichte-der-datenanalyse/, Zugriff 13.11.2017.

[3] Vgl. Davenport, T. H., 2014, Big Data at Work: Dispelling the Myths, Uncovering the Opportunities, Harvard Business Review Press, Watertown, S. 10.

Tabelle 1: Zeitliche Einteilung von begrifflichen Generationen der Datenanalytik

Name	Zeitraum	Methoden	Werkzeuge
Decision Support	1970-1985	Filterung, Aggregation und Sortierung	Relationale Datenbanken in Großcomputern
Executive Support	1980-1990	Filterung, Aggregation und Sortierung mit Bezug zu Geschäftsbereichen	Relationale Datenbanken in Großcomputern
Online Analytical Processing (OLAP)	1990-2000	u.a. multidimensionale Selektionen und Aggregationen	Multidimensionale Datenbankmodelle
Business Intelligence	1989-2005	Komplexe Visualisierungen	Data Warehouses und Spezialsoftware
Big Data	2010-heute	Maschinelles Lernen	Cluster, Datenbanken für unstrukturierte Daten

Einteilungen dieser Art haben natürlich nicht den Anspruch der absoluten Darstellung, sondern dienen dazu, Tendenzen der Entwicklung aufzuzeigen. Darüber hinaus fließen die Methoden und Werkzeuge einer Generation in die nächste ein, es handelt sich nicht um klar voneinander abzugrenzende Abschnitte, sondern um aufeinander aufbauende Entwicklungen. Vom Decision Support bis zu Big Data ist v.a. eine Tendenz zu sehen: Die Analysemodelle sollen eine immer größere Menge an Daten berücksichtigen und in Geschäftsentscheidungen einbeziehen. Seit einigen Jahren zeigt sich der Trend, die Statistik in der Datenanalyse vermehrt in den Fokus zu stellen. Ein Datenanalyst ist heute auch oft unter der Berufsbezeichnung „Data Scientist" zu finden, um den Fokus auf statistische, wissenschaftliche Modelle herauszustellen.

Eine Tendenz ist parallel zu den großen Konzepten erfolgt: Der Endanwender wird mehr und mehr dazu in die Lage versetzt, extrem große und komplexe Daten zu analysieren. Mehrere Millionen Datensätze können mit der richtigen Software auf heutigen, gewöhnlichen Workstations oder Laptops ausgewertet werden. Programmiersprachen treten bei der Anwendung solcher Software in den Hintergrund und der Anwender erhält die Möglichkeit, sich auf das wesentliche zu fokussieren: mittels des vorhandenen Prozesswissens Analysen durchzuführen.

In diesem Beitrag soll zunächst ein Überblick über die aktuellen Buzzwords in der Datenanalytik gegeben werden. Im Folgenden wird die, vom Autor in diversen Sonderuntersuchungen entwickelte, integrierte Datenanalytik im Fraud Management vorgestellt, die Elemente aus dem Knowledge Discovery in Databases (KDD)-Prozess und dem PDCA-Zyklus in einem modernen, prozessorientierten Modell zusammenführt. Zuletzt sollen anhand von Anwendungsbeispielen die Vorgehensweise der integrierten Datenanalytik und ihre Möglichkeiten für den Leser verdeutlicht werden. Die im Laufe dieses

Beitrages angesprochenen Programme, Produkte und Anwendungen werden regelmäßig vom Autor eingesetzt. Dabei handelt es sich überwiegend um frei verfügbare Software.

1.1 Big Data

Ein seit Jahren in vielen Kontexten genanntes, großes Thema ist Big Data. Oftmals fehlt allerdings das volle und umfassende Verständnis des Begriffes. Big Data ist nicht ausschließlich durch die schiere Menge an Daten eine Herausforderung:

- Unterschiedlichkeit der Struktur der Daten – Variety;
- Schnelligkeit der Datenerzeugung – Velocity;
- Menge der Daten – Volume.

Diese drei essentiellen Faktoren, wegen des englischen Anfangsbuchstaben auch „three V's" genannt, gelten gemeinhin als Definition für Big Data. Ein grundsätzlicher Ansatz ist, die Daten in Kombination zu nutzen. Eine der Herausforderungen, die sich daraus ergibt, liegt in der Varianz (Variety) der verschiedenen Datentypen: GPS-Daten, Sensordaten, Bilder, Zahlen, Texte, Videos usw. sollen oft gemeinsam abgelegt und analysiert werden. Ob Auto, Kaffeemaschine, Fernseher oder Kühlschrank, immer mehr Haushaltsgeräte sind online. So sind, laut einer von der gfu Consumer & Home Electronics GmbH[4] in Auftrag gegebenen Studie, bereits 53% aller Fernseher in Deutschland mit dem Internet verbunden.[5] Ortungsangaben, Kaffeebohnen-Füllstand und Sensordaten sind nur ein kleiner Teil der Informationen, die das Internet of Things (IoT) in unserem technisierten Alltag erzeugt. Unstrukturierte und nicht-relationale Datenbanken sorgen hier für verbesserte und beschleunigte Verfügbarkeit.

Neben dem schon genannten IoT fallen auch die Schlagworte „Industrie 4.0" oder „Digitalisierung" in diesem Zusammenhang immer wieder. Ein Ziel der von den Bundesministerien für Wirtschaft und Energie sowie Bildung und Forschung ins Leben gerufenen Initiative „Industrie 4.0" ist, neben der Schaffung einer intelligenten Wertschöpfungskette, die Erfassung aller Produktphasen, von der Idee bis zur Entsorgung nach der Nutzung. Die Datenmengen, die allein im Lebenszyklus eines einzelnen Produktes entstehen, sind groß. Die Datenmengen, die bei der Gesamterzeugung aller Produkte, allein in Deutschland entstehen, sind nur schwer fassbar. Die

[4] Ehem. Gesellschaft zur Förderung der Unterhaltungselektronik in Deutschland.

[5] Vgl. o.V., 06.08.2016, Studie: Smart-TVs erobern die Haushalte, Süddeutsche Zeitung, http://www.sueddeutsche.de/news/service/internet-studie-smart-tvs-erobern-die-haushalte-dpa.urn-newsml-dpa-com-20090101-160705-99-566859, Zugriff 13.11.2017.

Die Schwierigkeit für Datenanalyse im Bereich Fraud besteht darin, ein trennscharfes Modell zu entwickeln, dass die fraudulenten Handlungen innerhalb der Daten in jedem Fall sauber unterscheidet. Hierbei muss auf Analysen der Muster zurückgegriffen werden. Erst recht, da bereits heute die Datenmengen für regelbasierte Analysen oft zu groß sind.

2 Methodisches Vorgehen: Integrierte Datenanalytik

Im Fraud Management darf Datenanalyse kein reiner Selbstzweck sein, sondern muss ein klar formuliertes Ziel verfolgen. Das ist oft einfacher formuliert, als in der Realität befolgt oder umgesetzt. Durch das hypothesenfreie Arbeiten kann es schwierig sein, insbesondere Kennzahlen und messbare Ziele zu formulieren.

Auf das Fraud Management angewendet, lässt sich vielleicht noch das einfache Ziel: „es sollen so viele Fälle wie möglich identifiziert werden" ausgeben. Doch auch dieses ist nicht immer leicht messbar: Da die Grundgesamtheit der vorhandenen Fraud-Fälle in einem Unternehmen nicht bekannt ist, kann auch die Effizienz einer Datenanalyse nur abgeschätzt werden. Es müssen also Möglichkeiten gefunden werden, die Ziele zu operationalisieren und messbar zu machen.

In der Praxis hat sich daher eine Kombination aus verschiedenen Methoden unter Berücksichtigung von Einsatzformen – anlassbezogener, permanenter/präventiver und explorativer Analyse – in Verbindung mit dem PDCA-Zyklus und dem KDD-Prozess als Baukasten bewährt. Dadurch ist eine Planung, Durchführung, anschließende Bewertung und Optimierung von Datenanalysen nach einem definierten Vorgehen möglich. Im Folgenden wird dieser integrierte Ansatz, mit Möglichkeiten jeweils Messgrößen zu definieren, beschrieben.

2.1 PDCA-Zyklus

Der PDCA-Zyklus wurde von Deming entwickelt und basiert auf den Vorüberlegungen Shewharts und dessen Shewhart Cycle. Dabei handelt es sich um eine Methode der stetigen Qualitätsverbesserung von Produkten bzw. deren Entstehungsprozessen. Auf den Prozess der Datenanalyse angewendet umfasst der Zyklus die in Tabelle 2 dargestellten vier Phasen.[21]

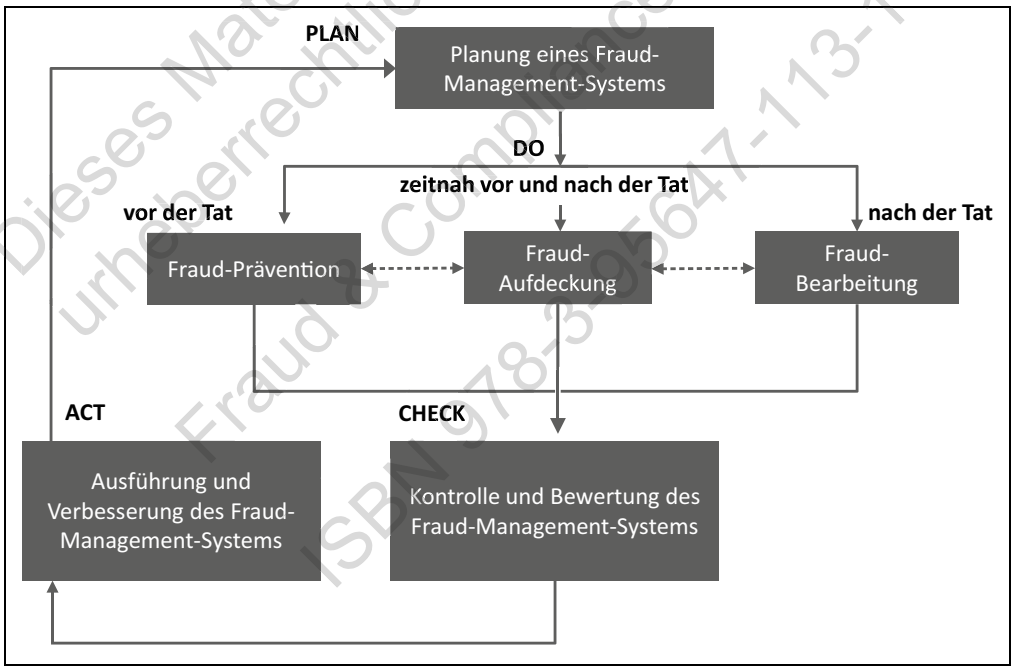
[21] Vgl. Jackmuth, H.-W., 2012, Datenanalytik im Fraud Management – Von der Ad-Hoc-Analyse zu prozessorientiertem Data-Mining, in: Jackmuth, H.-W./de Lamboy, C./Zawilla, P. (Hg.), Fraud Management – Der Mensch als Schlüsselfaktor gegen Wirtschaftskriminalität, Frankfurt School Verlag, Frankfurt am Main, S. 627-662, S. 635.

Tabelle 2: Anwendung des PDCA-Zyklus auf den Prozess der Datenanalyse

Plan – Planung	In der ersten Phase wird mittels Expertenwissen eine Analyse der Ist-Situation durchgeführt. Ziel ist es, Hypothesen zu definieren oder Themengebiete für hypothesenfreie Analysen festzulegen. Datentöpfe werden lokalisiert und Vortests zur Eignung der Datenqualität für die Analyse durchgeführt. Zusätzlich werden Ziele bzw. Erwartungen für die Analyse gesetzt.
Do – Umsetzung	Die Daten werden für die Analyse aufbereitet und mittels Data Minings, maschinellem Lernens oder anderer Verfahren analysiert.
Check – Überprüfung	Die durch die Umsetzung erhaltenen Ergebnisse werden überprüft und validiert. Mittels Prozesswissens werden Zusammenhänge erläutert und die angewendete Methodik auf Verbesserungspotentiale geprüft.
Act – Verbesserung	Die aus der Überprüfung gemachten Erfahrungen werden für die Planung und Umsetzung genutzt. Der Zyklus wird erneut durchlaufen und solange wiederholt, bis zufriedenstellende Ergebnisse erreicht sind.

Eine weitere Anwendungsmöglichkeit des PDCA-Zyklus auf ein Fraud-Management-System ist in Abbildung 3 zu sehen. Eine Integration der Datenanalyse ist, wie in den folgenden Abschnitten beschrieben, möglich und sinnvoll.

Abbildung 3: PDCA-Zyklus



Quelle: addResults Unternehmensberatung

2.2 Adaption des KDD-Prozesses

Knowledge Discovery in Databases (KDD), welches nach Fayyad, Piatetsky-Shapiro und Smyth, neben Data Mining als Teilprozess zur Datenanalyse bzw. zur Wissensgewinnung, auch die Vorbereitung der Daten und die Interpretation der Ergebnisse umfasst, ist dem Bereich der datengetriebenen oder hypothesenfreien Analysen zuzurechnen.[22]

Ein wichtiger Bestandteil von KDD ist der sogenannte KDD-Prozess, der das Vorgehen innerhalb einer Datenanalyse beschreibt. Dieser Prozess lässt sich in der Anwendung, wie im Folgenden erläutert, ideal durch den PDCA-Zyklus optimieren. Der Prozess besteht aus fünf Schritten und damit verbundenen Inputs und Outputs. Abbildung 4 zeigt den KDD-Prozess, in einer vom Autor angepassten Version. Der Schritt „Transformation" wurde um „Reduktion", der Schritt „Data Mining" um „Analyse" erweitert. Während die Ergänzung der Reduktion v.a. Auswirkungen auf die Tätigkeiten innerhalb des Prozessschrittes hat, ist die Ergänzung der Analyse innerhalb des „Data Mining"-Schrittes weitreichender: Das im Folgenden vorgestellte Vorgehen zur integrierten Datenanalytik beschränkt sich nicht auf die hypothesenfreie Analyse. Auch wenn der KDD-Prozess die Verwendung von Hypothesen nicht gänzlich ausschließt, hat sich in der Praxis die Nutzung von Prozesswissen und daraus abgeleiteten Hypothesen bewährt. Dies bedeutet ausdrücklich nicht, dass auf hypothesenfreie Algorithmen verzichtet werden soll, sondern sie sollen durch Hypothesen und weiteres Wissen unterstützt werden.

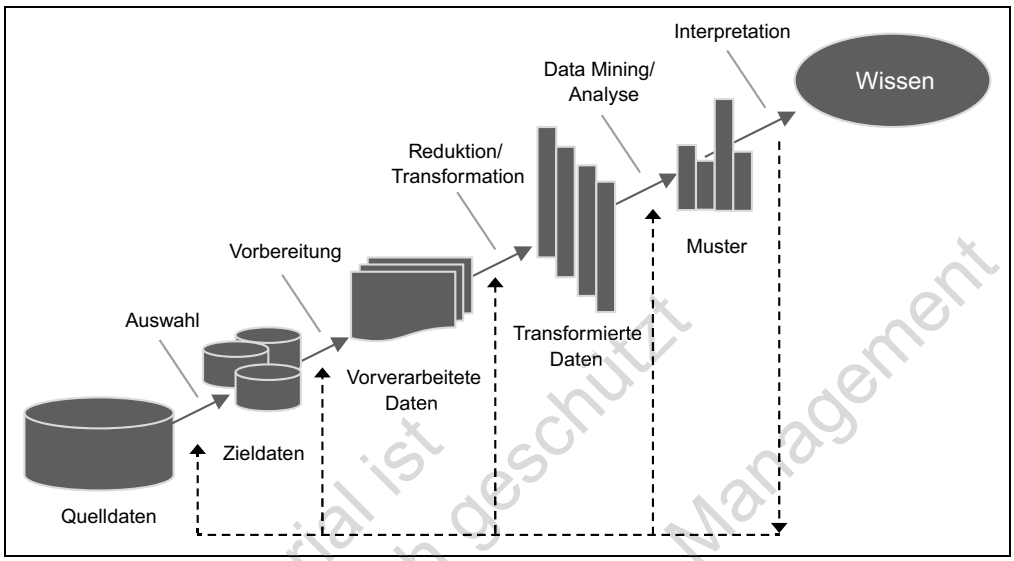
Eine wichtige Eigenschaft des KDD-Prozesses ist, dass er nicht bei jedem Durchlauf linear und vollständig durchlaufen werden muss. Ein Abbruch und folgende Anpassung der vorangegangenen Prozessschritte sind möglich und sinnvoll:

Durch eine Analyse wurde bspw. festgestellt, dass in den Daten auffällige Buchungen zu finden sind. Diese Buchungen wurden jeweils an verschiedene Bankkonten überwiesen. Viele dieser Bankkonten sind sogenannten Direktbanken zuzuordnen, die oft keinerlei Filialgeschäft haben und auf Drittanbieter zur Verifizierung von Neukunden angewiesen sind. Dokumentenfälschungen machen einige der Verifizierungsverfahren potenziell anfällig für Manipulationen. Für Täter bietet es sich also geradezu an, Direktbanken für die Zielkonten zu nutzen. Nachdem dieses Merkmal bei den auffälligen Belegen identifiziert wurde, sollte es für weitere Analysen nutzbar gemacht werden. In die Quelldaten wird eine Liste mit den Bankleitzahlen von Direktbanken hinzugefügt und in die Zieldaten aufgenommen, der Prozessschritt „Auswahl" wurde also wiederholt, die folgenden Schritte entsprechend neu durchlaufen. Bei der „Transformation/Reduktion"

[22] Vgl. Fayyad, U./Piatetsky-Shapiro, G./Smyth, R., 1996.

wurden nun die entsprechenden, an eine Direktbank gegangenen Belege gekennzeichnet und stehen für den Schritt „Data Mining/Analyse“ zur Verfügung.

Abbildung 4: Adaption des KDD-Prozesses



2.2.1 Plan – Planung: Auswahl

Da es nicht möglich und nicht sinnvoll ist, sämtliche Daten eines Unternehmens innerhalb einer Analyse zu untersuchen, muss eine Vorauswahl erstellt werden. Diese Vorauswahl geschieht auf Basis von Experten- bzw. Prozesswissen und der Formulierung von Zielen. Empfehlenswert ist eine Untersuchung von kritischen Prozessen bzw. Prozessen, bei denen bereits Schwächen identifiziert worden sind. Wichtig ist auch die Qualität der Daten zu beurteilen und ggf. auf Teilaspekte zu verzichten, denn schlechte Datenqualität erschwert die weitere Analyse enorm, bis hin zur völligen Unbrauchbarkeit.

Angewendet auf ein Szenario der Kreditorenprüfung werden exemplarisch folgende Daten aus einem ERP- (Enterprise Resource Planning) System ausgewählt:

- Kreditorenstammdaten;
- Bankverbindungen zu Kreditoren;
- Belegdaten;
- Bestellanforderungen;
- Bestellungen;
- Eingangsrechnungen.

Governance, Risk und Compliance (GRC) – Umsetzung in kleinen und mittleren Unternehmen (KMU)

Béla Maaß/Bernd Schindler

1 Einleitung

Die Erfüllung der Kundenwünsche mit einem attraktiven Produkt, welches in effizienten unternehmensinternen Prozessen durch qualifizierte und motivierte Mitarbeiter erstellt wird, ist nach wie vor die Basis eines profitablen und damit lange am Markt erfolgreichen Unternehmens.[1]

Jedoch zeichnet sich bereits seit geraumer Zeit ab, dass diese in der Unternehmensstrategie manifestierten Erfolgsfaktoren alleine den Fortbestand des Unternehmens nicht sicherstellen können. Zunehmend gleichrangig mit der erfolgreichen Umsetzung der Strategie ist die Einhaltung von Gesetzen, ein effizientes Risikomanagement zur Steuerung von Risiken sowie die Vorbeugung doloser Handlungen, deren wirtschaftlicher Schaden zunehmend existenzbedrohende Ausmaße annimmt.

Untermauert wird dieser Trend auch durch kontinuierlich steigende Strafzahlungen für Non-Compliance. So willigte die brasilianische Odebrecht-Gruppe am 22.12.2016 in die Zahlung einer Strafe für Korruptionsvergehen in Höhe von 3,5 Mrd. USD ein[2] und hält damit – zum Zeitpunkt der Verfassung dieses Buchbeitrags – den unrühmlichen weltweiten Allzeit-Rekord einer Strafzahlung für Non-Compliance.[3] Dabei beinhaltet die Strafe noch nicht einmal die möglichen weiteren Sanktionen in jenen zwölf Staaten, in denen Schmiergeldzahlungen für die Erlangung von Bauaufträgen getätigt wurden sowie wahrscheinliche künftige Umsatzausfälle aus der Aufnahme des Unternehmens in schwarze Listen.[4] Die eingangs bezifferte Strafzahlung resultiert vielmehr allein aus der Tatsache, dass die Zahlungen über US-amerikanische Bankkonten erfolgten – dabei hatten weder Geber noch Empfänger ihren Wohn- bzw. Firmensitz in den USA.

[1] Dies gilt grundsätzlich für jedwede Art von Organisation. Der Fokus wird nachfolgend jedoch auf privatrechtlich organisierte Unternehmen gelegt.

[2] Verlautbarung des The United States Department of Justice, 21.12.2016, https://www.justice.gov/opa/pr/odebrecht-and-braskem-plead-guilty-and-agree-pay-least-35-billion-global-penalties-resolve, Zugriff 22.05.2017.

[3] Im April 2017 wurde diese Strafe auf 2,6 Mrd. USD reduziert, da der Konzern glaubhaft darlegen konnte, dass eine noch höhere Strafe auch nachhaltig nicht leistbar sei.

[4] Hier verstanden als Sperrliste und damit Verzeichnis von Personen und Organisationen, die von wirtschaftlichen Transaktionen ausgenommen werden sollen. Schwarze Listen werden in der Praxis auch unternehmensintern geführt und verzeichnen Geschäftspartner, mit denen aufgrund schlechter Erfahrungen und/oder wegen Compliance-Verstößen keine Geschäfte gemacht werden sollen. Vgl. den Beitrag von Bielefeld/Wengenroth zu Sanktionen gegen Unternehmen bei Compliance-Verstößen in diesem Buch.

Ebenso zeichnet sich ein Trend zu kontinuierlich wachsenden Schäden aus dolosen Handlungen ab. Der CEO-Fraud[5] ist zwar als Deliktart nicht neu, jedoch mehren sich die Meldungen über Zahlungen für vorgeblich durch die Unternehmensleitung initiierte Sonderprojekte wie Unternehmensakquisitionen, die in Wahrheit auf Konten der Organisierten Kriminalität in länderübergreifenden dunklen Kanälen versickern. Diese Zahlungen erreichen je Schadenfall durchaus zweistellige Millionenbeträge, wie im Falle des deutschen Automobilzulieferers Leoni im Sommer des Jahres 2016.[6]

Auf internationaler Ebene ermittelte das US-amerikanische Federal Bureau of Investigation (FBI) im Zeitraum zwischen Oktober 2013 und Dezember 2016 einen Gesamtschaden von 5,3 Mrd. USD, basierend auf gemeldeten Straftaten.[7] Der tatsächliche Schaden dürfte noch wesentlich höher sein, da von einer beträchtlichen Dunkelziffer auszugehen ist.

Diese Beispiele illustrieren die finanziellen Auswirkungen von Non-Compliance und Fraud auf die betroffenen Unternehmen, die durchaus existenzbedrohende Ausmaße annehmen können. Zur Vermeidung derartiger Vorgänge können Großkonzerne im Rahmen der Corporate Governance[8] ein breites Arsenal an detektivischen und präventiven Maßnahmen durch eigenständige Risikomanagement-, Compliance- sowie Interne-Revisions-Bereiche einsetzen und diese kontinuierlich auf ihre Wirksamkeit prüfen lassen.

Diese Komfortzone bietet sich mittelgroßen Unternehmen nur eingeschränkt und kleineren Unternehmen i.d.R. gar nicht. Dennoch können auch kleine und mittlere Unternehmen (KMU[9]), bspw. im Logistikbereich, Teil einer weltweiten Lieferkette werden

[5] CEO = Chief Executive Officer (oberste Unternehmensleitung). Mit diesem Begriff wird ein Muster für Straftaten unternehmensexterner Täter beschrieben, bei dem Mitarbeiter von Unternehmen zur Überweisung von i.d.R. hohen Geldbeträgen genötigt werden. Dies wird durch den Aufbau von Druck mittels profunden Insiderwissen und der Verwendung falscher Identitäten erreicht. Vgl. auch den Beitrag von Drießen/Franosch/Jackmuth zu Cyberkriminalität und Angriffsszenarien durch CEO-Fraud in diesem Buch.

[6] Vgl. o.V., 14.08.2016, 40 Millionen Euro weg – dieser MDax-Konzern fällt auf Betrüger rein, Manager Magazin, http://www.manager-magazin.de/unternehmen/autoindustrie/autozulieferer-leoni-um-40-millionen-betrogen-a-1107998.html, Zugriff 22.05.2017.

[7] Vgl. Public Service Announcement, Business e-mail compromise, 04.05.2017, https://www.ic3.gov/media/2017/170504.aspx#fn3, Zugriff 22.05.2017.

[8] Corporate Governance bezeichnet den rechtlichen und faktisch durch die Unternehmensleitung geschaffenen Ordnungsrahmen für die ordnungsgemäße Leitung und Überwachung eines Unternehmens.

[9] Die Einordnung eines Unternehmens als KMU erfolgt i.d.R. anhand vordefinierter Wertgrenzen des Jahresumsatzes, der Bilanzsumme und der Anzahl von Mitarbeitern. Jedoch existieren uneinheitliche Schwellenwerte, z.B. des deutschen Handelsgesetzbuchs (HGB), der Europäischen Kommission in der EU-Empfehlung 2003/361 sowie des Instituts für Mittelstandforschung (IfM), Bonn.

und damit grundsätzlich den gleichen Risiken wie Großkonzerne ausgesetzt sein – und gesamtschuldnerisch für mögliche Schäden haften. Jedoch verfügen auch KMU über Organisationsbereiche, die entweder selbst Teil der Corporate Governance sind, oder aber vielfältige funktionsimmanente Schnittstellen zu dieser aufweisen und somit sprichwörtlich eine Brücke zu einem ansonsten brachliegenden Feld schlagen können.

Dieser Beitrag soll durch eine Analyse der Kernaufgaben der Risikomanagement-, Compliance- und Internen-Revisions-Einheiten konkrete Handlungsempfehlungen für KMU zum ressourcenneutralen Aufbau einer effizienten GRC-Einheit entwickeln. Ziel ist es dabei, eine bereits in der bestehenden Aufbau- und Ablauforganisation des Unternehmens verankerten Abteilung unter Fokussierung auf kongruente Aufgaben mit GRC-Aufgaben zu betrauen.

2 GRC-Rahmenwerk

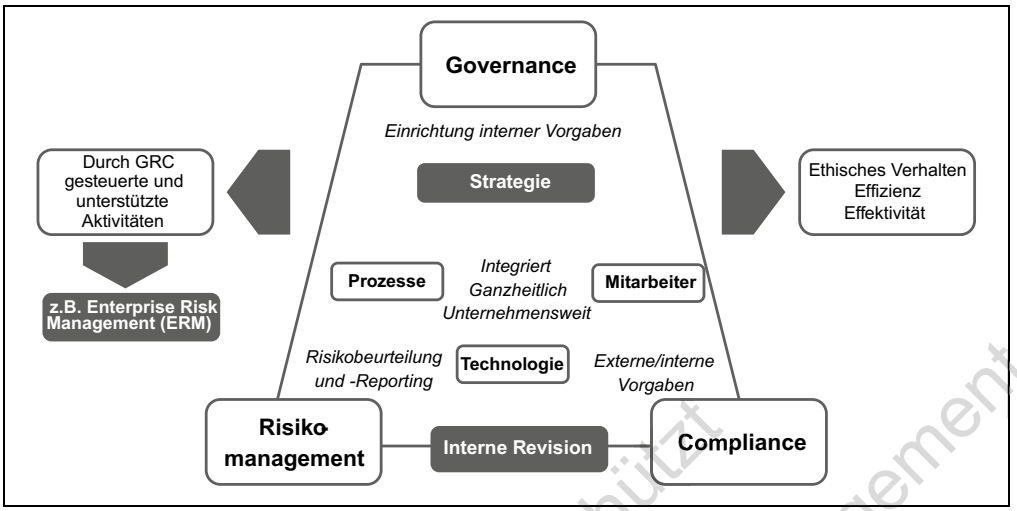
In Ermangelung einer einheitlichen Definition verstehen wir GRC als einen integrierten, ganzheitlichen Ansatz zu einer optimalen Unternehmensführung (Governance), ausgewogenem Risikomanagement (Risk) und der strikten Einhaltung von externen und internen Regeln (Compliance), der sicherstellt, dass eine Organisation entsprechend ihren selbstauferlegten Regeln, mit einem von ihr definierten Risikoappetit und in Übereinstimmung mit externen Bestimmungen handelt – durch die konsequente Ausrichtung von Strategie, Prozessen, Technik und Menschen, um dadurch Synergien für das Unternehmen zu heben und die Leistung zu steigern.[10]

Die wesentlichen Elemente und Einflussfaktoren des GRC-Rahmenwerks ergeben sich aus Abbildung 1.[11]

[10] Vgl. addResults Unternehmensberatung, o.D., Compliance, http://www.addresults.de/dienstleistungen/articles/compliance.html, Zugriff 22.05.2017.

[11] Vgl. Racz, N./Weippl, E./Seufert, A., 2010, A frame of reference for research of integrated GRC, in: De Decker, B./Schaumüller-Bichl, I. (Hg.), Communications and Multimedia Security, 11th IFIP TC 6/TC 11 International Conference, CMS 2010 Proceedings, Springer, Berlin, S. 106-117, S. 113.

Abbildung 1: Elemente und Einflussfaktoren des GRC-Rahmenwerks



Quelle: Racz, N./Weippl, E./Seufert, A., A frame of reference for research of integrated GRC, in: De Decker, B./Schaumüller-Bichl, I. (Hg.), Communications and Multimedia Security, 11th IFIP TC 6/TC 11 International Conference, CMS 2010 Proceedings, Springer, Berlin 2010, S. 106-117, S. 113.

Durch den integrierten Ansatz kann einerseits ein nachhaltig gesunder Einklang zwischen dem Risikoappetit und andererseits der Einhaltung interner sowie externer (Compliance-)Vorgaben zur bestmöglichen Umsetzung der Unternehmensstrategie i.S.v. Effektivität *(„die richtigen Dinge tun")* und Effizienz *(„die Dinge richtig tun")* erreicht werden.

Primäre GRC-Disziplinen sind Governance, Risikomanagement und Compliance, deren Wirksamkeit regelmäßig durch die Interne Revision geprüft werden sollte. Von GRC gesteuerte und unterstützte Aktivitäten sind insbesondere:[12]

- Enterprise Risk Management (ERM), hier verstanden als unternehmensweites Risikomanagementsystem (RMS),[13]
- Risikobewertung,

[12] Vgl. Tadelwald, J., 2014, GRC Integration: A Conceptual Foundation Model for Success, in: Management Accounting Quarterly, Vol. 15, No. 3, S. 10-18, S. 11.

[13] Vgl. The Committee of Sponsoring Organization of the Treadway Commission, 2004, Unternehmensweites Risikomanagement – Übergreifendes Rahmenwerk, https://www.coso.org/Documents/COSO-ERM-Executive-Summary-German.pdf, Zugriff am 22.05.2017, S. 1-16, S. 5.

3 Entwicklung eines ganzheitlichen GRC-Ansatzes für KMU

Im vorhergehenden Abschnitt wurden die Kernaufgaben der wesentlichen GRC-Einheiten dargestellt. Nachfolgend soll darauf aufbauend ein Ansatz für den Aufbau einer ganzheitlichen GRC-Einheit für KMU entwickelt werden.

3.1 Aufgabenkongruenz der GRC-Einheiten

Bei der Beschreibung der Haupttätigkeiten der GRC-Einheiten sind oftmals die gleichen Begriffe gefallen, insbesondere die Ableitung der konkreten Tätigkeit aus:

- der Unternehmensstrategie,
- der konsequenten Anwendung risikobasierten Denkens,
- dem Postulat der Einhaltung von Gesetzen und internen Vorgaben,
- prozessorientierten Ansätzen unter Anwendung des PDCA-Zyklus,

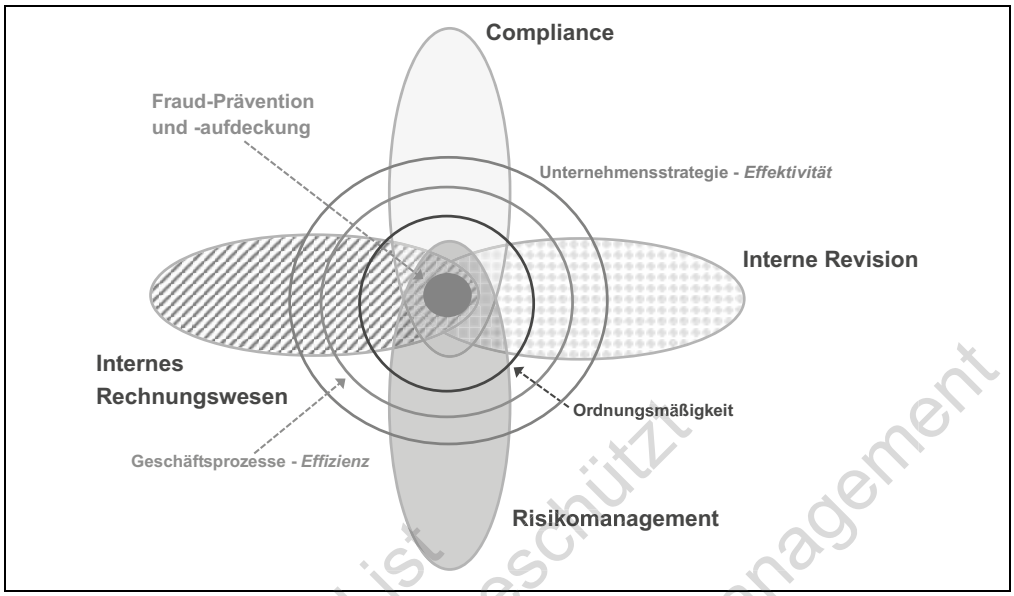
wodurch sich aus Sicht der Autoren eine große Schnittmenge der jeweiligen Aufgabenpakete ergibt.

Natürlich hat jede GRC-Einheit spezifische Aufgaben und Tätigkeiten, die andere GRC-Einheiten üblicherweise nicht abbilden. Dies gilt insbesondere für weltweit tätige Großkonzerne, deren Geschäftstätigkeit sehr komplex ist und deren GRC-Einheiten daher dieser Spezialisierung bedürfen. Jedoch gibt es auch hier bereits Überschneidungen in Form von Ausschüssen zu Risiken, Compliance etc., in denen das gleiche Fachgebiet von unterschiedlichen GRC-Einheiten als Team bearbeitet wird.

Die an der Maximierung des Unternehmensgewinns orientierte Unternehmensleitung vermutet hierdurch Redundanzen durch Aufgabendoppelung und damit verbundene unnötige Verwaltungskosten. Umso mehr stellt sich die Frage für KMU, ob diese intensive Spezialisierung erforderlich ist, u.a. da deren Geschäftsmodell i.d.R. weit weniger komplex ist. Die Zusammenhänge der Spezialisierung sind in Abbildung 11 grafisch dargestellt. Im Kern, sozusagen als Königsdisziplin, wollen alle GRC-Einheiten dazu beitragen, Fraud innerhalb des Unternehmens zu vermeiden bzw. aufzudecken. Als weitere, bezüglich der Teilmengen größer werdende Aufgabengebiete treten auf:

- die Sicherstellung von Ordnungsmäßigkeit, verstanden als die Einhaltung von Gesetzen und internen Vorgaben (Compliance),
- die Sicherstellung der Effizienz von Geschäftsprozessen und die Unternehmensstrategie als Ausgangspunkt der eigenen risikobasierten Tätigkeit und Objekt kontinuierlichen Hinterfragens zur Sicherstellung der Effektivität.

Abbildung 11: Aufgabenkongruenz der GRC-Einheiten



Quelle: addResults Unternehmensberatung

3.2 Aufbauorganisation der GRC in KMU

Selbst innerhalb von Großkonzernen zeichnet sich aus Gründen der Effizienzsteigerung und Kostenreduktion in den vergangenen Jahren ein Trend zu einem integrierten GRC-Modell ab. Dieses wird in mehreren Phasen aus der bestehenden GRC-Struktur entwickelt. Der Ausgangspunkt ist eine vollständig getrennte Struktur, in der das Risikomanagement, das Compliance-Management und das IKS – neben der Internen Revision – getrennt voneinander existieren. Dann folgt eine fließende Phase der Harmonisierung der in der GRC-Einheit zusammengefassten Funktionen, bis man schließlich in einem voll integrierten GRC-Modell mit nur einer GRC-Einheit ankommt.

Diesem Trend treten Berufsverbände wie z.B. das IIA entgegen, indem dieses nach wie vor eine organisatorisch eigenständige Interne Revision fordert. In einer idealen Welt mag dies der richtige Ansatz sein. Für KMU ist es jedoch mit prohibitiv hohen Kosten verbunden. Kritisch sei angemerkt, dass selbst ein (kosten-)intensiv und unter Beachtung aller nur erdenklichen Empfehlungen umgesetztes Three Lines of Defense-Modell nach wie vor nicht den Konkurs von Unternehmen, z.B. aufgrund doloser Handlungen, zu verhindern vermag. Als Praxisbeispiel sei erneut auf die Hintergründe des Zusammenbruchs der Investmentbank Lehman Brothers in 2008 hingewiesen.

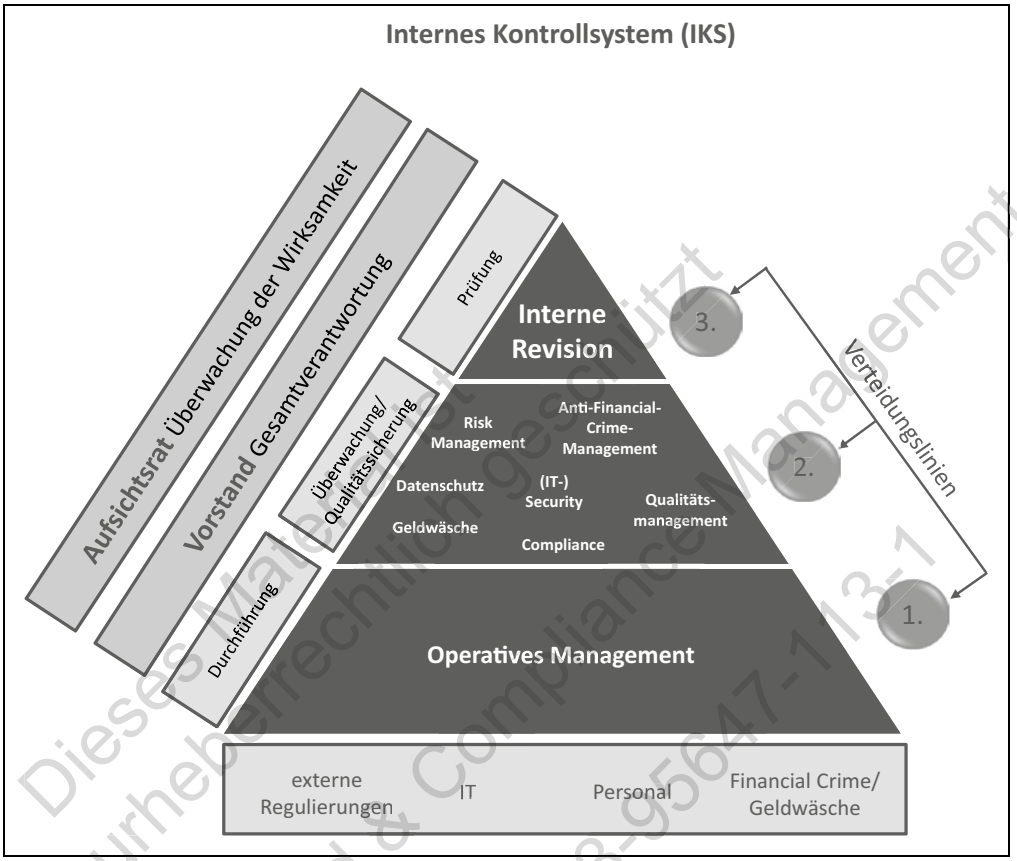
Wirksamkeit fraudspezifischer Kontrollpläne unter Nutzung des Internen Kontrollsystems

Hans-Willi Jackmuth

3.3 Three Lines of Defense-Ansatz

3.3.1 Verantwortlichkeiten im IKS

Abbildung 1: Three Lines of Defense-Ansatz



Quelle: addResults Unternehmensberatung

Gemäß dem Three Lines of Defense-Ansatz wird jede Organisationseinheit einer Verteidigungslinie zugeordnet und ist im Rahmen dieser Rollenzuweisung mit unterschiedlichen Aufgaben, Kontrollen und Schwerpunkten zur Verhinderung von „sonstigen strafbaren Handlungen" (Financial Crime) betraut:[20]

[20] Vgl. auch den Beitrag von Maaß/Schindler zu Governance, Risk und Compliance (GRC) – Umsetzung in kleineren und mittleren Unternehmen (KMU) in diesem Buch.

Die erste Verteidigungslinie (First Line) bildet das operative Management, welches für die Sicherstellung der Identifizierung, Beurteilung, Kontrolle sowie entsprechender Verminderung der Risiken im Rahmen des Tagesgeschäfts verantwortlich ist. Zusätzlich gewährleistet das operative Management die Übereinstimmung der Aktivitäten mit den Unternehmenszielen.

Die zweite Verteidigungslinie (Second Line) beinhaltet Risikomanagement-, Controlling- und Compliance-Funktionen, um die in der ersten Verteidigungslinie konzipierten Kontrollen auszubauen und zu überwachen. Hier ist das Fraud Management anzusiedeln, im nachfolgenden neutral auch als „Überwachungseinheit" benannt. Die Geschäftsleitung implementiert diese Funktionen, um sicherzustellen, dass die erste Verteidigungslinie ordnungsgemäß aufgebaut ist und effektiv funktioniert.

Die dritte Verteidigungslinie (Third Line) stellt als objektive und unabhängige Prüfungs- und Beratungsinstanz die Interne Revision dar. Die Interne Revision unterstützt in dieser Funktion Geschäftsleitung, Führungskräfte und Überwachungsinstanzen und gibt Sicherheit über die Angemessenheit und Wirksamkeit der Überwachungs-, Risikomanagement- und Kontrollstrukturen.

3.3.2 Auslagerung von Kontrollaktivitäten – Make or Buy?

Eine Auslagerung von Kontrollaktivitäten (bspw. auf Einheiten von Wirtschaftsprüfungsgesellschaften) kann unter gewissen Rahmenbedingungen sinnvoll erscheinen, erhöht ggf. aber das Risikoprofil des Instituts. Eine Entscheidung darüber sollte originäre Aufgaben, Zuständigkeiten wie auch Schnittstellen berücksichtigen und folgende Aspekte miteinbeziehen:

- Know-how-Transfer,
- Kapazitäten/Ressourcen,
- Zeit,
- Risiko,
- generelle Hinderungsgründe.

4 Arten, Ausgestaltung und Wirksamkeit von Kontrollen

4.1 Definition des Begriffes fraudspezifische Kontrollen

Unabhängig von den im Weiteren dargestellten Überlegungen zur Ausgestaltung eines IKS, das in erster Linie den Stakeholdern Sicherheit geben soll, dass die im Buchwerk dargestellten Zahlen der Realität (unter Berücksichtigung einer Wesentlichkeitsgrenze) entsprechen, sind die Angriffsszenarien der Täter kreativ, extrem veränderbar und halten sich vor allen Dingen nicht an die dargestellten und im Unternehmen definierten Prozessgrenzen.

Eines der möglichen Szenarien, an denen dies beispielhaft verdeutlicht werden kann, ist der Verkauf von Investmentanteilen eines Kunden. Das Beispiel wurde bewusst verallgemeinernd und simpel gewählt, wenngleich man das Ergebnis ggf. anders betrachten kann.

Aus dieser Logik heraus wird bspw. bei einem Verkauf von Investmentanteilen die Stückeseite (d.h. die Anteile des Kunden in Stück) mit einer Stückebuchung durchaus korrekt i.S.d. Bilanzierung abgebildet; das Investmentvermögen wird um die verkauften Stücke vermindert, der Kurs neu berechnet und somit stimmt sowohl die Stücke- als auch die Geldseite in der Bilanz aus Sicht des Investmentfonds.

Es bestehen jetzt ggf. mehrere Möglichkeiten des Täters, auf den anstehenden Zahlungsfluss des Verkaufserlöses zuzugreifen. Die Erarbeitung der vollständigen Möglichkeiten überlassen wir der Kreativität des Lesers - spontan könnte man sich einen Innentäter genauso vorstellen (die Kontonummer des Empfängerkontos wird im Banksystem verändert) wie einen externen Täter, der mittels eines Cyberangriffs Viren auf dem Rechner des Kunden platziert; oder einen Angriff auf das Zielkonto nicht bei der Investmentbank, aber bei der Bank des Kunden etc.

Natürlich kann auch davon ausgegangen werden, dass spätestens das Erkennen des Fraud-Falls zu Veränderungen im Buchwerk führt. Dies wäre dann die Sicht, dass das Szenario theoretisch im nicht-fraudspezifischen IKS auch abgebildet ist. Problem ist nur, dass hier dann keine Sicherungsmaßnahmen mehr greifen.

Dieses relativ simple Beispiel soll zeigen, dass die übliche Denkweise einer Gestaltung eines IKS im Rahmen der Rechnungswesenrelevanz für fraudspezifische Kontrollen nicht unbedingt ausreichend ist. Im Rahmen von Standards der berufsständischen Verbände wird dieser Umstand nur unzureichend beleuchtet.