1 Entwicklung und Gefährdungslage

Das Thema Wirtschaftskriminalität (englisch: Fraud)[1] spielt in der Wirtschaft eine immer bedeutsamere Rolle, nachdem diese Thematik in den Unternehmen lange Zeit sogar mehr oder weniger negiert wurde. So waren Kommentare wie „Bei uns passiert so etwas nicht", „Wir sind ja viel zu klein für so etwas" oder „Da sprechen wir nicht drüber" häufig anzutreffen. Dies erschien umso erstaunlicher bzw. unverständlicher, da die „Polizeiliche Kriminalstatistik" der letzten Jahre für Deutschland, das „Bundeslagebild Wirtschaftskriminalität" des Bundeskriminalamtes (BKA) sowie alle Analysen und Erhebungen bekannter Wirtschaftsprüfungsgesellschaften und Vertrauensschadenversicherer bereits seit längerem deutlich zeigen:

> *Wirtschaftskriminalität ist ein ernsthaftes und größer werdendes Problem mit einer sehr hohen Dunkelziffer, das alle Unternehmen und Branchen betrifft!*

Allein die bekannt gewordenen Schäden gehen für die Unternehmen in eine mehrstellige Milliardenhöhe, ganz abgesehen von der immensen Dunkelziffer, von der auch die Ermittlungsbehörden ausgehen und auf die in allen anderen Statistiken und Lagebilddarstellungen ausdrücklich hingewiesen wird.[2]

Dabei handelt es sich keineswegs um ein jeweils nationales Problem, sondern der Täter oder ganze Tätergruppen operieren – nicht zuletzt auch begünstigt durch die technische Entwicklung der letzten Jahren – länder- und kontinentübergreifend[3] sowie mit einer Geschwindigkeit, die es teilweise erheblich erschwert, sich hiervor als einzelnes Land oder Unternehmen angemessen zu schützen.

In jedem Unternehmen können daher durch Fraud-Fälle von eigenen Mitarbeitern und/oder Externen erhebliche, oftmals unmittelbar ertragsmindernde Schäden entstehen und sind nicht selten auch bereits entstanden. Dies zeigen aktuelle Fälle sowohl bei namhaften

[1] Im weiteren Verlauf des Buches wird der Begriff „Fraud" als ein Synonym für den Begriff „Wirtschaftskriminalität" verwendet, ohne allerdings eine inhaltliche Begriffsdefinition damit zu verbinden. Zur Definition des Begriffes „Wirtschaftskriminalität" vergleiche Abschnitt 2 dieses Beitrags.

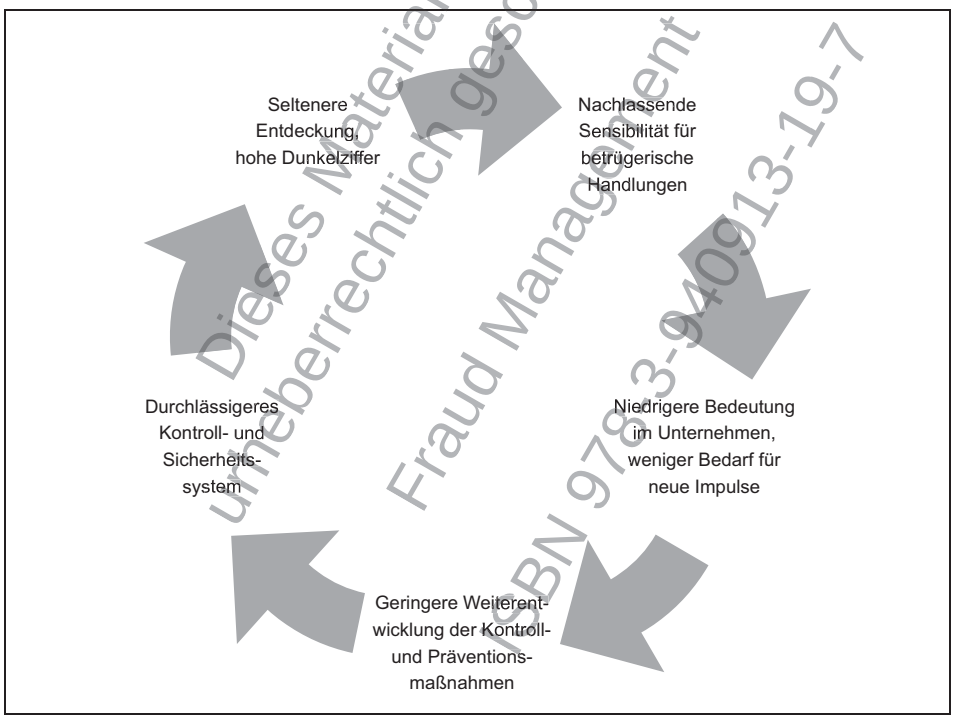
[2] Die Dunkelziffer in den polizeilichen Statistiken ist zweigeteilt, einerseits beinhaltet diese noch nicht aufdeckte Fälle, anderseits aber auch alle die Fraud-Fälle, die von Unternehmen oder Privatpersonen zwar aufdeckt, nicht aber gegenüber den Ermittlungsbehörden angezeigt wurden und demzufolge ebenfalls nicht statistisch erfasst werden können. Die aktuellen Entwicklungen werden jeweils im jährlichen „Bundeslagebild Wirtschaftskriminalität" des Bundeskriminalamtes abgebildet.

[3] Vgl. hierzu den Report to the Nations on Occupational Fraud and Abuse, der regelmäßig von der Association of Certified Fraud Examiners herausgegeben wird.

nationalen als auch internationalen Unternehmen deutlich. Neben materiellen Auswirkungen erleiden die geschädigten Unternehmen zudem aufgrund der meist unvermeidlichen Publizität dieser Vorkommnisse einen – teilweise massiven – Vertrauensverlust und eine deutliche Beeinträchtigung ihrer Reputation.

Insbesondere kleinere und mittelgroße Unternehmen verfügen i.d.R. über vergleichsweise wenig eigene Erfahrungen im Umgang mit Fraud-Fällen und Unregelmäßigkeiten von eigenen Mitarbeitern. Dies liegt zumeist in einer in der Vergangenheit bisher nur geringen Anzahl bekannt gewordener Fälle im jeweils eigenen Haus begründet. Dadurch werden die vorhandenen Gefahren und Risiken z.T. erheblich unterschätzt (gefühlte Sicherheit).[4] Dabei unterliegen viele Unternehmen oftmals noch immer dem Phänomen des so genannten „Teufelskreises trügerischer Sicherheit".

Abbildung 1: „Der Teufelskreis trügerischer Sicherheit"



[4] Vgl. hierzu auch die Ausführungen auf der S. 20 der Studie „Wirtschaftskriminalität 2011 – Sicherheitslage in deutschen Großunternehmen", die die Wirtschaftsprüfungsgesellschaft PricewaterhouseCoopers (PwC) in Zusammenarbeit mit der Martin-Luther-Universität Halle-Wittenberg erstellt und herausgegeben hat.

Waren Unternehmen bisher noch nicht oder nur selten Opfer betrügerischer Handlungen, so neigen sie dazu, ihr Augenmerk nicht unbedingt auf vorbeugende Maßnahmen zur Verbesserung des Entdeckungsrisikos – z.B. durch die Optimierung des eigenen Internen Kontrollsystems (IKS) – zu legen. Somit sinkt gleichzeitig auch die Aufdeckungswahrscheinlichkeit tendenziell weiter. Hierdurch wird allerdings Wirtschaftskriminalität nicht verringert, sondern im Gegenteil lediglich die Dunkelziffer erhöht.

Ausgehend hiervon tragen die Unternehmen – wenn auch bisher teilweise eher noch zurückhaltend – den Risiken aus wirtschaftskriminellem Handeln zu ihren Lasten Rechnung und treffen umfassendere Vorkehrungen zur Vermeidung von Fraud als bisher. Allerdings bestehen derzeit nur in einzelnen Branchen auch konkrete gesetzliche sowie aufsichtsrechtliche Verpflichtungen, sich im Rahmen des Risikomanagements auch und konkret gegen Fraud zu schützen.[5]

Die entsprechende Verantwortlichkeit hierfür liegt dabei bei der Geschäftsleitung. Allerdings zeigt die Praxis, dass bei vielen – insbesondere den für den Vertrieb zuständigen – Mitgliedern der Geschäftsleitung das nachhaltige Bewusstsein sowie die Akzeptanz noch erhöht bzw. teilweise erst noch geschaffen werden müssen. Auch dieser Bereich der operationellen Risiken eines Unternehmens stellt eine ernst zu nehmende Herausforderung dar und kann erhebliche Risiken bergen.

Die nachfolgenden Ausführungen in diesem Beitrag geben einen Eindruck sowie einen Überblick über die Vielfältigkeit der Fraud- und Manipulationsmöglichkeiten sowohl durch Mitarbeiter als auch durch Externe, über die maßgebliche Rolle des Schlüsselfaktors Mensch sowie über die Notwendigkeit eines ganzheitlichen, integrierten Fraud Prevention & Fraud Managements zur wirksamen und effizienten Bekämpfung von Wirtschaftskriminalität.

[5] Hier ist insbesondere die Finanzdienstleistungsbranche zu nennen, vgl. hierzu auch den Beitrag von Romeike zu Risikomanagement im Fraud-Kontext.

2 Vorgehensweisen beim Social Engineering

2.1 Vorbereitung – Basisinformationen einholen

Ein Social Engineer versucht zunächst, möglichst viele leicht zugängliche Informationen über ein Unternehmen zu sammeln, die ihm Insiderwissen vermitteln. Die Kenntnis von Unternehmensstrukturen, -hierarchien und -abläufen ermöglicht es ihm, im zweiten Schritt als vermeintlicher Unternehmensangehöriger aufzutreten.

Neben öffentlich zugänglichen Informationen (z.B. Internet-Homepage eines Unternehmens, Werbebroschüren etc.) gibt es weitere – i.d.R. leicht zu beschaffende – Informationsträger wie z.B.:

- Organigramme;
- Telefonlisten;
- Werk-, Gebäude- und Raumpläne;
- Mitarbeiterzeitungen;
- Dienst- und Schichtpläne;
- Arbeitsanweisungen.

Einmal mehr sei an dieser Stelle auf potenzielle Gefahren des Internets hingewiesen. Es ist immer wieder verblüffend, wie viele – z.T. sehr persönliche – Informationen durch einfachste Recherche mittels Suchmaschinen (z.B. Google) erlangt werden können. Ein Zitat aus der Security-Fachzeitschrift „Der Sicherheitsberater" bringt die aktuelle Situation auf den Punkt:[16] „Die meisten Anwender und auch viele Sicherheitsverantwortliche verstehen nicht, wie das Internet funktioniert und unterliegen dem Irrglauben, in der Masse an Informationen im Internet doch eher anonym zu sein. Dementsprechend gehen sie oft leichtfertig mit sensiblen Informationen um. Man sollte sich daher stets einige Grundprinzipien des Internets vor Augen halten, die entscheidend sind:

- Das Internet vergisst nichts!
- Anonymität ist ein frommer Wunsch!
- Fälschung ist einfach!"

[16] O.V., 2007, Gezielte Ausforschung und Manipulation, S. 197.

Einzeln betrachtet sind die o.a. Informationen eher unspektakulär und harmlos – erst miteinander verknüpft ergibt sich ein mosaikartig vervollständigtes erstes Gesamtbild. Als Faustregel gilt: Fünf unwichtige Informationen ergeben eine wichtige (sensible) Information.

***Hinweis**: Eine einfache Möglichkeit, sich einen Überblick über frei zugängliche Informationen in Hinblick auf das eigene Unternehmen zu verschaffen, bietet eine gezielte Online-Recherche.*

2.2 Aktive Beschaffung von Detailinformationen – Kontaktphase

2.2.1 Am Telefon – Psychologische Methode

Nach wie vor ist das Telefon das wichtigste Hilfsmittel eines Social Engineers, da es ein gezieltes Agieren bei gleichzeitiger Wahrung der eigenen Anonymität erlaubt.

„Gespräch mit falschem Müntefering" meldete Spiegel-Online am 14.09.2008 und bezog sich auf einen Stimmenimitator, der sich für einen Radiosender als SPD-Chef Franz Müntefering ausgab und sieben Minuten mit der hessischen SPD-Chefin Andrea Ypsilanti telefonierte. Obwohl die Ausstrahlung des Gesprächs sofort untersagt wurde, kursierte das unvorteilhafte Gespräch auf der Internet-Plattform YouTube und führte zu einem erheblichen Imageschaden.

Der Sachverhalt zeigt, wie schnell man Opfer einer Täuschung mittels Telefon werden kann. Bezogen auf Social-Engineering-Angriffe gegen Unternehmen, könnte sich folgendes Gespräch ergeben.

***Beispiel**:*

Angreifer: Social Engineer (SE)
Opfer: IT-Mitarbeiter Meier (M) der Firma Fiktiv-AG

M: *Meier, guten Tag, IT-Support der Fiktiv-AG. Was kann ich für Sie tun?*

SE: *Guten Tag, Listig mein Name von der Firma Data-Fantast. Spreche ich mit dem Leiter der IT-Abteilung der Fiktiv-AG?*

M: *Nein, bedauere, unser Unit-Manager Herr Krüger ist noch bis kommenden Mittwoch im Urlaub. Donnerstag ist er auf jeden Fall im Haus, denn um 10:00 Uhr ist immer Team-Meeting.*

SE: Ach, wie ärgerlich – ich bin nämlich seitens Data-Fantast mit Ihrer Kundenbetreuung beauftragt. Es gab in letzter Zeit wiederholt Probleme mit dem neuen Server X.

M: Das verstehe ich nicht, den Server X setzen wir gar nicht ein – wir verwenden hier Y in der Version 7.0.

SE: Mmh – bin ich jetzt vielleicht selber durcheinander gekommen? Ich vertrete bei uns nämlich Herrn Lehmann und muss mich selbst noch in dessen Unterlagen einarbeiten. Ich schaue jetzt alles noch mal durch und melde mich dann wieder. Entschuldigen Sie bitte meine schlechte Vorbereitung. Könnten Sie mir freundlicherweise noch die Durchwahl von Herrn Krüger geben?

M: Gerne – Herr Krüger hat die Apparat-Nr. 800. Wie gesagt, bitte erst ab Mittwoch versuchen.

SE: Vielen Dank – Ihnen noch einen schönen Tag und sorry für die Störung.

Welche Informationen hat unser Social Engineer in diesem kurzen Telefonat erlangt?

- Name des IT-Mitarbeiters, Name des Vorgesetzten;
- firmeninterne Bezeichnungen wie Unit-Manager und Team-Meeting;
- Urlaubssituation von Herrn Krüger;
- eingesetztes Produkt und Version;
- Durchwahl von Herrn Krüger.

Diese Informationen versetzen unseren Social Engineer nun in die Lage, sich in einem weiteren Telefonat mit einem anderen Mitarbeiter der IT-Abteilung der Fiktiv-AG als vertrauenswürdig zu authentifizieren und einen gezielten Angriff durchzuführen. Vorgenannte Informationen werden dabei genutzt, um Insiderkenntnisse vorzutäuschen und/oder ein Überordnungsverhältnis zu suggerieren („… Ihr Unit-Manager, Herr Krüger, hat mich beauftragt, während seines Urlaubs …“).

Das scheinbar beiläufige Nennen von Personen höherer Hierarchieebenen, das auch als *name dropping* bezeichnet wird, ist dabei eine häufig angewandte Methode.

2 Bestechlichkeit und Bestechung im geschäftlichen Verkehr (§ 299 StGB)

(1) Wer als Angestellter oder Beauftragter eines geschäftlichen Betriebes im geschäftlichen Verkehr einen Vorteil für sich oder einen Dritten als Gegenleistung dafür fordert, sich versprechen lässt oder annimmt, dass er einen anderen bei dem Bezug von Waren oder gewerblichen Leistungen im Wettbewerb in unlauterer Weise bevorzuge, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer im geschäftlichen Verkehr zu Zwecken des Wettbewerbs einem Angestellten oder Beauftragten eines geschäftlichen Betriebes einen Vorteil für diesen oder einen Dritten als Gegenleistung dafür anbietet, verspricht oder gewährt, dass er ihn oder einen anderen bei dem Bezug von Waren oder gewerblichen Leistungen in unlauterer Weise bevorzuge.

(3) Die Absätze 1 und 2 gelten auch für Handlungen im ausländischen Wettbewerb.

2.1 Normzweck

Durch diese Vorschrift soll der freie, lautere und faire Wettbewerb gewährleistet und insbesondere Auswüchsen im Wettbewerb begegnet werden.[9] Die Norm ist als abstraktes Gefährdungsdelikt ausgestaltet, so dass es auf den Eintritt des gewünschten Erfolges nicht ankommt. Betriebsinhaber sind keine tauglichen Täter des Delikts, sehr wohl aber Geschäftsführer und Vorstände juristischer Personen, auch der Alleingeschäftsführer einer GmbH.[10]

2.2 Objektiver Tatbestand

Täter

Täter kann jeder Angestellte oder Beauftragte einer Firma sein. So hat sich ausweislich des Hamburger Abendblatts vom 08.10.2011 die Firma Repower von einem externen Beauftragten getrennt, der sich bei so genannten Outsourcing-Prozessen intensiv um Zah-

[9] BGH vom 16.07.2004, wistra 2004, S. 22.

[10] Vgl. Fischer, T., 2011, Kommentar zum Strafgesetzbuch, § 299, Rn. 10c.

lung von Geldern derjenigen Firma bemüht hat, die am Ende noch im Bieterkreis verblieben ist. Nach Aufdeckung der Tat hat sich Repower unverzüglich von dem externen Interimsmanager getrennt.[11]

Handel im geschäftlichen Verkehr

Der Handel im geschäftlichen Verkehr umfasst alle Tätigkeiten, die auf die Förderung eines beliebigen Geschäftszwecks gerichtet sind. Damit einhergehend sind jedoch auch private Verbraucher nicht mit umfasst.

Vorteilsbegriff

Der Vorteil, der den des § 331 StGB entspricht, umfasst jede Leistung auf die der Empfänger keinen Rechtanspruch hat und die seine wirtschaftliche, rechtliche oder auch persönliche Lage objektiv verbessert.[12] Dabei kann der Vorteil sowohl materiell wie auch immateriell zugewandt werden, wobei ein nur mittelbarer Vorteil ausreicht.

Die materielle Zuwendung kann in Form von Provisionen, Honoraren, Rabatten, zinslosen Darlehen, Erlass von Schulden, Zuwendung von Waren oder Dienstleistungen, Reisen und üppigen Geschäftsessen erfolgen. Immaterielle Zuwendungen können in der Hilfe beim beruflichen Aufstieg, Verleihung besonderer Ämter und möglicherweise durch sexuelle Zuwendungen erfolgen.[13]

Ein Vorteil im Sinne der Vorschrift ist zu verneinen, wenn die Zuwendung als sozial adäquat anzusehen ist. Dies ist gegeben, wenn sie nach der Verkehrssitte oder den Regeln der Höflichkeit gewährt und allgemein gebilligt wird, sowie nicht den Charakter einer Gegenleistung hat.[14]

Unrechtsvereinbarung

Der Vorteil muss als Gegenleistung für eine künftige unlautere Bevorzugung gedacht sein, der Vorteilsgeber handelt mithin mit dem Ziel, auf die künftige Handlung Einfluss nehmen zu wollen. Dies jeweils zu beurteilen, unterliegt der Beurteilung des Tatgerichts.

[11] http://www.abendblatt.de/wirtschaft/article2052908/Korruptionsversuch-bei-Repower.html, Zugriff 09.10.2011.

[12] Vgl. Heybrock, H., 2010, Praxiskommentar zum GmbH-Recht, § 299 StGB, Rn. 14.

[13] Vgl. Tiedemann, K., 2006, Leipziger Kommentar Strafgesetzbuch, § 299, Rn. 25.

[14] Vgl. Fischer, T., 2011, Kommentar zum Strafgesetzbuch, § 299, Rn. 16.

- Eine stabile Gewinnentwicklung sowie eine hohe Risikotragfähigkeit (Eigenmittelausstattung) reduziert die Wahrscheinlichkeit einer Insolvenz.
- Eine stabile Gewinnentwicklung sowie eine niedrigere Insolvenzwahrscheinlichkeit sind im Interesse von Arbeitnehmern, Kunden und Lieferanten, was es erleichtert, qualifizierte Mitarbeiter zu gewinnen und langfristige Beziehungen zu Kunden und Lieferanten aufzubauen.
- Bei einem progressiven Steuertarif haben zudem Unternehmen mit schwankenden Gewinnen Nachteile gegenüber Unternehmen mit kontinuierlicher Gewinnentwicklung.
- Die Verhinderung von wirtschaftskriminellen Handlungen verringert finanzielle Schäden.
- Ein präventives Fraud- und Risikomanagement reduziert das Risiko von Reputationsschäden und schützt die Marke sowie den Unternehmenswert.

Risikomanagement bietet insgesamt v.a. eine Erhöhung der Planungssicherheit und eine nachhaltige Steigerung des Unternehmenswerts.

2.2 Risikolandkarte in Unternehmen

Die Wahrnehmung von Risiken ist eine höchst subjektive Angelegenheit, da Risiken in ihrer Dimension und Materialität und Immaterialität durch unsere Sinnesorgane konstruiert werden.[25] Ob wir etwas als Risiko auffassen oder nicht, hängt von unseren Urteilen ab, die von Meinungen, Moden und Moralvorstellungen geprägt sind: Was für den einen ein Risiko ist, braucht für die anderen noch lange keins zu sein. Auch die Einschätzung von Wahrscheinlichkeiten ist eine höchst subjektive Angelegenheit. Was für den einen Experten wahrscheinlich ist, hält der nächste für unwahrscheinlich. Risiken sind unsichere Ereignisse, die eintreten können, aber nicht müssen.

Daher sind Risikolandkarten nicht nur über die Branchengrenzen hinweg, sondern auch innerhalb eines Unternehmens eher heterogen. Empirische Studien zeigen jedoch auf, dass Unternehmenszusammenbrüche primär auf strategische oder operative Risiken zurückgeführt werden können, zu denen auch Wirtschaftskriminalität zu zählen ist.[26]

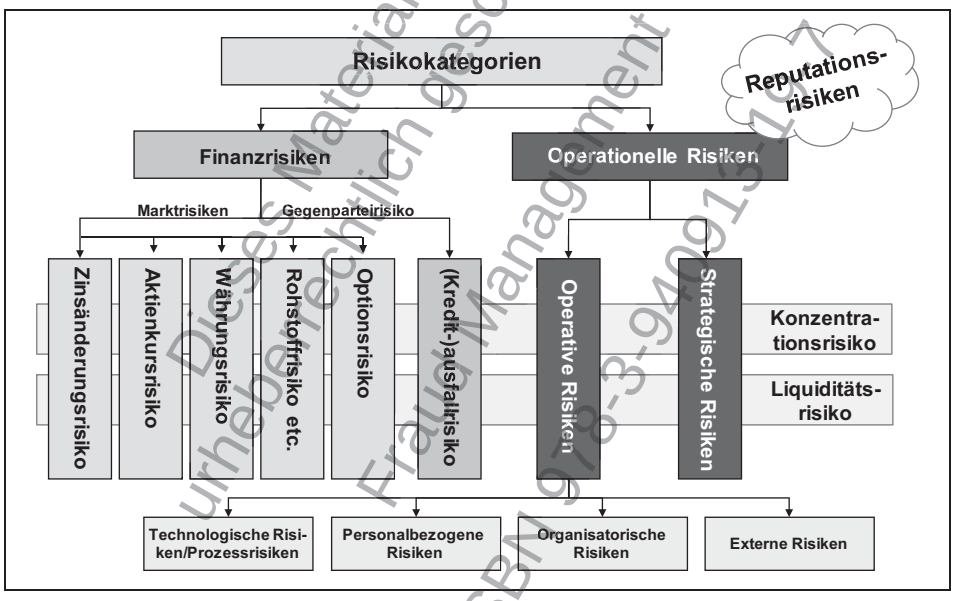
[25] Vgl. Romeike, F./Hager, P., 2009, Erfolgsfaktor Risiko-Management, S. 109.

[26] Vgl. Romeike, F., 2004, Integration des Managements der operationellen Risiken in die Gesamtbanksteuerung, S. 41-54 sowie Erben, R./Romeike, F., 2003, Allein auf stürmischer See, S. 13 ff.

Strategische und operative Risiken zusammen werden auch als operationelle Risiken bezeichnet. In Abbildung 2 ist eine generische Risikolandkarte für Unternehmen aller Branchen skizziert.

Risiken im Kontext Fraud können sich in unterschiedlichen Risikokategorien wiederfinden. So können sich beispielsweise Risiken in der Folge deliktischer bzw. doloser Handlungen sowohl im Bereich Finanzrisiken als auch im Bereich der operativen bzw. strategischen Risiken niederschlagen. Der Begriff dolose Handlungen (nach lat. *dolosus* = arglistig, trügerisch) fasst hierbei Bilanzmanipulationen, Untreue, Unterschlagung und alle anderen zum Schaden des Unternehmens vorsätzlich durchgeführten Handlungen zusammen. In der Konsequenz werden derartige Handlungen v.a. auch zu einem Reputationsverlust führen.

Abbildung 2: Risikokategorien im Überblick[27]



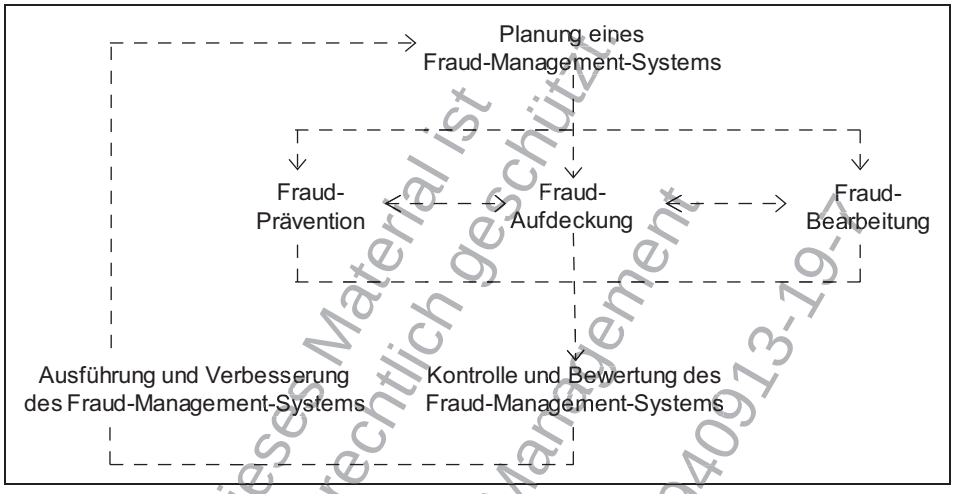
Des Weiteren können Risiken durch externe oder interne Ereignisse und Störungen verursacht werden. So kann etwa ein Beschaffungsrisiko auf Schwierigkeiten im Beschaffungsprozess oder ebenso auf die Ursache zurückgeführt werden, dass durch ein externes Schadensereignis (Erdbeben, Überschwemmung etc.) bestimmte Produkte auf dem Weltmarkt nicht mehr oder nur zu höheren Preisen verfügbar sind. Nachfolgend sind einige Beispiele für potenzielle Risikobereiche aufgezählt:

[27] Vgl. Romeike, F./Hager, P., 2009, Erfolgsfaktor Risiko-Management, S. 111.

3 Umsetzung eines ganzheitlichen, prozessualen Ansatzes (PDCA-Modell)

Zu Beginn dieses Buches wurde im Beitrag „Ganzheitliches Fraud Management und der Schlüsselfaktor Mensch“ bereits der nachstehend noch einmal abgebildete ganzheitliche, prozessuale Ansatz eines Fraud Prevention & Fraud Managements vorgestellt.

Abbildung 7: Ganzheitliches Fraud-Prevention-&-Fraud-Management-System gemäß PDCA-Modell



Die einzelnen Prozessschritte und deren konkrete Inhalte werden in den nachfolgenden Abschnitten näher dargestellt. Detaillierte Ausführungen zu den Inhalten sind wiederum den jeweiligen Beiträgen der verschiedenen Autoren zu entnehmen.

3.1 Planung eines Fraud-Management-Systems

Unter dem Begriff werden alle Aktivitäten verstanden, die sich mit der Planung von (Einzel-)Maßnahmen befassen, um ein wirkungsvolles (Präventions-)System gegen Fraud zu implementieren. Dieser Planungsprozess definiert im Sinne des PDCA-Zyklusses alle Aktivitäten, die sich mit der Verhinderung und Aufdeckung von wirtschaftskriminellen Handlungen sowie den daraus abgeleiteten Optimierungsaktivitäten für das System der Bank befassen.

Mögliche Einzelmaßnahmen des Planungsprozesses können u.a. sein:

- Fraud-Prevention-Policy erstellen;
- Leitlinien entwickeln;
- Fraud-Bedrohungspotenzial ermitteln;
- Gefährdungsanalyse durchführen;[17]
- Maßnahmen/Aktivitäten planen;
- Bedarf für IT-Programme/Tools zur Fraud-Prävention, Fraud-Aufdeckung und Fraud-Bearbeitung ermitteln;[18]
- Aufgaben- und Verantwortlichkeiten festlegen (vgl. Abschnitt 5);
- Stellenbeschreibung für den Fraud-(Prevention-)Manager/-Beauftragten erstellen (vgl. Abschnitt 5.4);
- Zeitplan festlegen und benötigte Mitarbeiterkapazitäten ermitteln;
- Schadensfallmanagementleitfaden entwickeln und aktualisieren;[19]
- Informations- und Kommunikationskonzept „Fraud" entwickeln;
- Fraud-(Incident)-Reporting festlegen.

3.2 Fraud-Prävention

Unter der Durchführung von Fraud-Prävention sind alle Maßnahmen zu verstehen, welche sich mit der Verhinderung von wirtschaftskriminellen Handlungen durch zeitlich „vor der Tat" erfolgende Aktivitäten befassen (z.B. mit der Bewusstseinsbildung durch Schulung und Sensibilisierung der Mitarbeiter, vgl. hierzu Abschnitt 2.6). Dies kann in der Praxis in verschiedenen Stufen erfolgen, zu denen beispielsweise die Erstellung eines „Ratgebers zur Fraud-Prävention" (z.B. in Form eines Merkblattes) oder die Schulung mittels eines Web-Based-Trainings gehören.

[17] Vgl. hierzu ausführlich den Beitrag von Jackmuth/Zawilla zur Gefährdungsanalyse.

[18] Vgl. hierzu ausführlich die Beiträge von Jackmuth zu unterstützenden Werkzeugen/Tools für das Fraud Management sowie zu Datenanalytik.

[19] Vgl. hierzu den Beitrag von Zawilla zur Vorgehensweise bei Sonderuntersuchungen.

Führung beachtet, empfiehlt sich, diese mit Wachsamkeit und Fleiß zu unterfüttern. Damit wird der wichtigste Grundstein für Fraud-Prävention in Ihrem Unternehmen gelegt.

2. Es gibt keinen 100 %-igen Schutz – wer dies verspricht handelt grob fahrlässig.

2 Verteidigungslinien im Personalmanagement

2.1 Schutzmaßnahmen nach außen – strukturierter Einstellungsprozess

Der Fraudster steht vor den Unternehmenstoren und maskiert sich als Freund, zumindest als freundlicher Bewerber. Um einen Fraudster zu demaskieren, gestaltet sich das Bewerbungsverfahren wie ein Hürdenlauf, den es für jeden Bewerber zu bewältigen gilt. Für die Unternehmensvertreter besteht die Aufgabe darin, diesen Eingangshindernisparcours so gewissenhaft wie möglich zu gestalten, denn neben der Leistungsfähigkeit gilt es auch, die Silhouette[6] zu prüfen. Was im Volksmund lautet: „Vertrauen ist gut, Kontrolle ist besser!", bedeutet für die Fraud-Prävention: „Vertrauen ist unverantwortlich und Kontrolle nicht nur kriegsgewinnend, sondern kriegsvermeidend!" Dabei gilt, dass je näher ein Fraudster an Sie und Ihr Unternehmen herankommen kann, desto gefährlicher wird er. Er ist dann in der Lage, sein Eindrucksmanagement[7] einzusetzen und wird Sie durch *lovebombing*[8] schwächen. Um dies zu unterbinden, sollten im Personalmanagement eines Unternehmens Verteidigungslinien eingezogen werden.

***Hinweis**: Die ersten und damit äußersten und für den Fraudster im Sinne seiner Reichweite zu Ihnen entferntesten Verteidigungslinien sind die entscheidenden.*

[6] Die so genannte Silhouette ist die Gesamtheit der Fassade, von der adretten Frisur, über die vorzeigbare Ehefrau, bis zum perfekten Lebenslauf.

[7] Eindrucksmanagement ist die Kunst einen guten Eindruck zu hinterlassen, durchaus auch bei und im Besonderen zur Kaschierung von Substanzmangel. Genauer: der Fraudster konzentriert sich darauf, dass Sie einen guten Eindruck von seinen angeblichen Kompetenzen bekommen, ohne diese tatsächlich anzuwenden. Sie erhalten einen gefühlten Eindruck von Kompetenz, aber keinen faktischen Beweis.

[8] Sie werden mit Nettigkeiten „erschlagen". Je subtiler dies geschieht, desto effektiver ist es! Dieses Zuschütten mit Aufmerksamkeiten und Zuwendung soll Sie menschlich verpflichten und Ihre Wachsamkeit lähmen. Wer eng umarmt wird, kann sich auch nicht mehr frei bewegen – und das Beste daran ist, dass man es von sich aus auch gar nicht mehr will. Vgl. auch Grieger-Langer, S., 2011, Die Tricks der Trickser.

2.1.1 Erfordernis der Klarheit bei der Erstellung einer Stellenbeschreibung

Soll eine Stelle (neu) besetzt werden, ist es die Aufgabe des zuständigen Managers, eine dezidierte Stellenbeschreibung aufgrund des Unternehmensbedarfs zu liefern. Grundelemente einer Stellenbeschreibung sind:

- Titel;
- Angabe der Rolle, die erfüllt werden soll;
- Liste der Aufgaben oder Verantwortlichkeiten;
- Liste mit den grundlegenden Kenntnissen, Fertigkeiten, Fähigkeiten und Einstellungen, die für eine gute Leistung erforderlich sind;
- Aufstellung der Ziele und der entsprechenden Messstandards.

Bei der Listenerstellung der Kenntnisse, Fertigkeiten und Fähigkeiten hat sich eine Kategorisierung in Muss-, Soll- und Kann-Kriterien bewährt. Die Ausarbeitung einer Stellenbeschreibung ist ein mühsamer Prozess. Gleichwohl ermöglicht erst diese verantwortungsvolle Vorarbeit, unqualifizierte Bewerber effektiv auszuschließen. Unternehmen, die keine Stellenbeschreibungen für ihre Mitarbeiter haben, sparen sich zwar vorweg Arbeit, im Nachhinein aber müssen sie ständig nachbessern, etwa durch Zeitaufwand für Konfliktlösungen, Motivationsversuche etc.

> ***Hinweis**: Die beste Prävention gegen Manipulationen sind klare Absprachen und Verträge.[9] Diese erste Verteidigungslinie ist das Fundament Ihrer Schutzmaßnahmen!*

2.1.2 Interne Prüfung der Stellenbeschreibung

Auf Grundlage der Stellenbeschreibung erfolgt die offizielle Beantragung zur Einstellung eines neuen Mitarbeiters. An diesem Punkt kommen weitere Personen mit ins Spiel, denn jeder zusätzliche wache Geist erhöht die Sicherheit. Neben administrativen Entscheidungen und der Budgetüberprüfung bedarf es der Zustimmung weiterer Entscheider. Deren Aufgabe besteht im Wesentlichen darin, zu prüfen, ob der zuständige Manager klar und kompetent in seiner Stellenbeschreibung ist.

Sollte dies nicht in allen Details der Fall sein, gilt es, konsequent auf Optimierung zu bestehen, bevor eine Zustimmung zum nächsten Schritt erfolgt. Auf Grundlage der Stellenbeschreibung wird eine Stellenausschreibung formuliert.

[9] Vgl. Grieger-Langer, S., 2011, Die Tricks der Trickser.

Führung beachtet, empfiehlt sich, diese mit Wachsamkeit und Fleiß zu unterfüttern. Damit wird der wichtigste Grundstein für Fraud-Prävention in Ihrem Unternehmen gelegt.

2. Es gibt keinen 100 %-igen Schutz – wer dies verspricht handelt grob fahrlässig.

2 Verteidigungslinien im Personalmanagement

2.1 Schutzmaßnahmen nach außen – strukturierter Einstellungsprozess

Der Fraudster steht vor den Unternehmenstoren und maskiert sich als Freund, zumindest als freundlicher Bewerber. Um einen Fraudster zu demaskieren, gestaltet sich das Bewerbungsverfahren wie ein Hürdenlauf, den es für jeden Bewerber zu bewältigen gilt. Für die Unternehmensvertreter besteht die Aufgabe darin, diesen Eingangshindernisparcours so gewissenhaft wie möglich zu gestalten, denn neben der Leistungsfähigkeit gilt es auch, die Silhouette[6] zu prüfen. Was im Volksmund lautet: „Vertrauen ist gut, Kontrolle ist besser!", bedeutet für die Fraud-Prävention: „Vertrauen ist unverantwortlich und Kontrolle nicht nur kriegsgewinnend, sondern kriegsvermeidend!" Dabei gilt, dass je näher ein Fraudster an Sie und Ihr Unternehmen herankommen kann, desto gefährlicher wird er. Er ist dann in der Lage, sein Eindrucksmanagement[7] einzusetzen und wird Sie durch *lovebombing*[8] schwächen. Um dies zu unterbinden, sollten im Personalmanagement eines Unternehmens Verteidigungslinien eingezogen werden.

***Hinweis**: Die ersten und damit äußersten und für den Fraudster im Sinne seiner Reichweite zu Ihnen entferntesten Verteidigungslinien sind die entscheidenden.*

[6] Die so genannte Silhouette ist die Gesamtheit der Fassade, von der adretten Frisur, über die vorzeigbare Ehefrau, bis zum perfekten Lebenslauf.

[7] Eindrucksmanagement ist die Kunst einen guten Eindruck zu hinterlassen, durchaus auch bei und im Besonderen zur Kaschierung von Substanzmangel. Genauer: der Fraudster konzentriert sich darauf, dass Sie einen guten Eindruck von seinen angeblichen Kompetenzen bekommen, ohne diese tatsächlich anzuwenden. Sie erhalten einen gefühlten Eindruck von Kompetenz, aber keinen faktischen Beweis.

[8] Sie werden mit Nettigkeiten „erschlagen". Je subtiler dies geschieht, desto effektiver ist es! Dieses Zuschütten mit Aufmerksamkeiten und Zuwendung soll Sie menschlich verpflichten und Ihre Wachsamkeit lähmen. Wer eng umarmt wird, kann sich auch nicht mehr frei bewegen – und das Beste daran ist, dass man es von sich aus auch gar nicht mehr will. Vgl. auch Grieger-Langer, S., 2011, Die Tricks der Trickser.

2.1.1 Erfordernis der Klarheit bei der Erstellung einer Stellenbeschreibung

Soll eine Stelle (neu) besetzt werden, ist es die Aufgabe des zuständigen Managers, eine dezidierte Stellenbeschreibung aufgrund des Unternehmensbedarfs zu liefern. Grundelemente einer Stellenbeschreibung sind:

- Titel;
- Angabe der Rolle, die erfüllt werden soll;
- Liste der Aufgaben oder Verantwortlichkeiten;
- Liste mit den grundlegenden Kenntnissen, Fertigkeiten, Fähigkeiten und Einstellungen, die für eine gute Leistung erforderlich sind;
- Aufstellung der Ziele und der entsprechenden Messstandards.

Bei der Listenerstellung der Kenntnisse, Fertigkeiten und Fähigkeiten hat sich eine Kategorisierung in Muss-, Soll- und Kann-Kriterien bewährt. Die Ausarbeitung einer Stellenbeschreibung ist ein mühsamer Prozess. Gleichwohl ermöglicht erst diese verantwortungsvolle Vorarbeit, unqualifizierte Bewerber effektiv auszuschließen. Unternehmen, die keine Stellenbeschreibungen für ihre Mitarbeiter haben, sparen sich zwar vorweg Arbeit, im Nachhinein aber müssen sie ständig nachbessern, etwa durch Zeitaufwand für Konfliktlösungen, Motivationsversuche etc.

> ***Hinweis**: Die beste Prävention gegen Manipulationen sind klare Absprachen und Verträge.[9] Diese erste Verteidigungslinie ist das Fundament Ihrer Schutzmaßnahmen!*

2.1.2 Interne Prüfung der Stellenbeschreibung

Auf Grundlage der Stellenbeschreibung erfolgt die offizielle Beantragung zur Einstellung eines neuen Mitarbeiters. An diesem Punkt kommen weitere Personen mit ins Spiel, denn jeder zusätzliche wache Geist erhöht die Sicherheit. Neben administrativen Entscheidungen und der Budgetüberprüfung bedarf es der Zustimmung weiterer Entscheider. Deren Aufgabe besteht im Wesentlichen darin, zu prüfen, ob der zuständige Manager klar und kompetent in seiner Stellenbeschreibung ist.

Sollte dies nicht in allen Details der Fall sein, gilt es, konsequent auf Optimierung zu bestehen, bevor eine Zustimmung zum nächsten Schritt erfolgt. Auf Grundlage der Stellenbeschreibung wird eine Stellenausschreibung formuliert.

[9] Vgl. Grieger-Langer, S., 2011, Die Tricks der Trickser.

Viel spezieller wird der Fall, wenn im Rahmen fraudulenten Verhaltens bewusst Datensätze abgelegt werden, die nur teilweise ähnliche Daten aufweisen: Gleiche Anschrift bei fiktiven Personen, unterschiedliche Firmenschreibweisen zur Verschleierung etc. Es muss somit im optimalen Fall eine Methode implementiert werden, die mittels Clusteranalyse mit einer hohen Anzahl von Clustern für die jeweiligen Variablen derartige Zusammenhänge aufzeigt. Gerade bei Großunternehmen werden hier die Grenzen der Modelle (SQL-Datenabfragen oder Queranalysen über Links) schnell erreicht.

4 Aufdeckung doloser Handlungen durch neuronale Netze

Die derzeit bekannten und in Tools eingebundenen neuronalen Netze gehen auf eine Entwicklung des finnischen Mathematikers Teuvo Kohonen zurück, der im Jahre 1995 mittels Algorithmen sensorische Karten nachbildete. Sensorische Karten übernehmen die Aufgabe, die Distanzen verschiedener Körperreize zu ermitteln und im menschlichen Gehirn zu verorten. Dies findet bereits in einer frühkindlichen Phase durch permanentes Training statt.

Neuronale Netze können vom Typ her nach der Art ihrer Lernfähigkeit klassifiziert werden. Dabei ist eine grobe Einteilung in überwachtes und unüberwachtes Lernen möglich. Beim überwachten Lernen ist die Ausgabe bekannt und wird mittels zahlreich zur Verfügung stehender Trainingsbeispiele und immer wieder neu korrigierter Durchläufe erreicht.

Beim unüberwachten Lernen ist die Ausgabe hingegen nicht zwangsläufig bekannt, so dass das Netz auf eigenständiges, d.h. selbstorganisierendes Lernen angewiesen ist. Ziel ist die „Kartierung eines Eingaberaums", wobei jedem Neuron ein spezieller Teil zugewiesen wird. Benachbarte Neuronen sind dabei durch ähnliche Eingabewerte charakterisiert. Selbstorganisierende Karten wie auch der Großteil der unterschiedlichen Kohonen-Netze sind im Bereich des unüberwachten Lernens einzuordnen.[39]

Der Vorteil der Nutzung neuronaler Netze in der Datenanalyse liegt in folgendem Sachverhalt: Eine Vielzahl verschiedener Kriterien, die einen Zustand mittels Daten beschreiben, kann angelernt werden. Damit lassen sich Effekte beobachten, die vielleicht nur in der Wechselwirkung von fünf oder sieben Dimensionen in den Daten zu Tage treten.

[39] Vgl. Einführung in neuronale Netze, http://www.math.uni-muenster.de/SoftComputing/lehre/material/wwwnnscript/strfx/Kohonen.html (Abruf 13.01.2011).

In der Anfangseuphorie der Nutzung dieses herausragenden Verfahrens wurde und wird leider immer noch eine Menge Humbug getrieben. Denn genauso wenig wie Menschen lebensfähig wären, wenn sie nur und ausschließlich über funktionierende sensorische Karten verfügen würden, nutzen neuronale Netze nichts, wenn sie nicht in einen Analyseaufbau integriert sind und für den Anwender handhabbar werden.

An dieser Stelle soll ein einfaches Beispiel die Funktionsweise dieses Verfahrens im Fraud Management illustrieren:

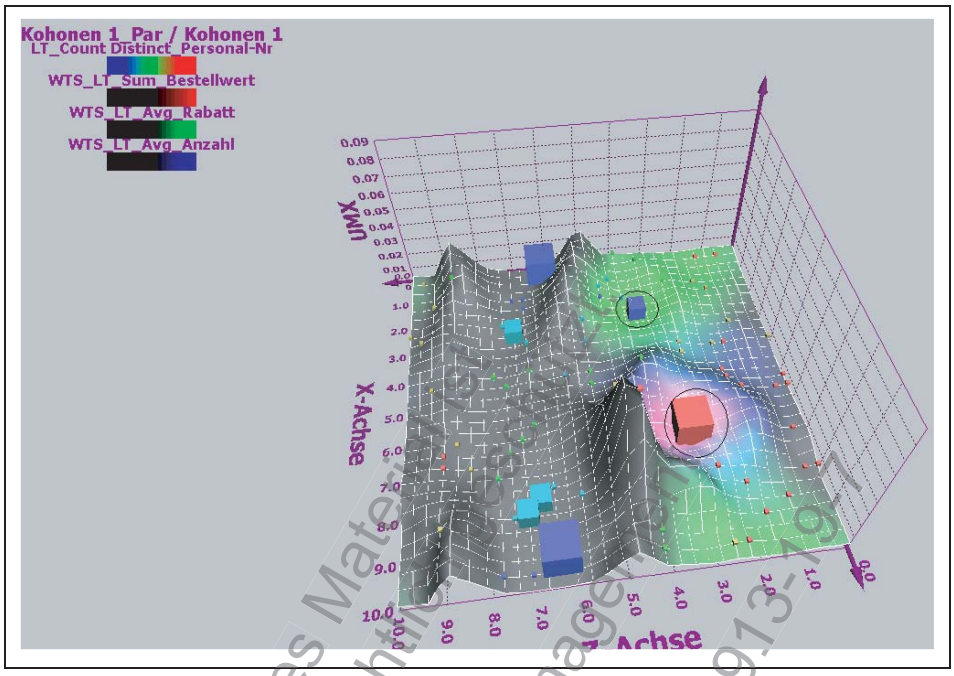
Die Bestellvorgänge in einem Unternehmen sollen mit der Zielrichtung untersucht werden, auffällige Rabattierungen durch Mitarbeiter zu identifizieren. Mehrere Mitarbeiter verkaufen unterschiedliche Produkte in unterschiedlichen Mengen zu verschiedenen Konditionen an verschiedene Kunden. Diese Situation kann in den meisten Unternehmen als Standard betrachtet werden.

Für den Anfang ist eine einfache Liste mit Verkaufsvorgängen ausreichend, in der alle wesentlichen Informationen über die Bestellvorgänge enthalten sind. Diese Ebene der Daten sollte immer am Anfang einer Analyse (Data Preparation) stehen, so dass später ein Rückgriff auf den einzelnen Geschäftsvorfall möglich ist. Im nächsten Schritt werden die Daten in einer Aggregation für die weitere Analyse vorbereitet. Die Datenverdichtung erfolgt in diesem Beispiel auf den einzelnen Kunden.

Um unterschiedliche Dateninhalte objektiv vergleichen zu können, muss eine Logik geschaffen werden, die beispielsweise Eurowerte und Verkaufsstückzahlen mit einer einheitlichen Methodik aufbereitet. Daher werden bei der Data Preparation die einzelnen Spalten auf einen einheitlichen Wertebereich zwischen 0 und 1 transformiert (der Wert 0 steht dabei für den kleinsten, der Wert 1 für den höchsten Ausgangswert), wobei die Zwischenwerte die Verteilung in den Daten widerspiegeln. So ist eine Vergleichbarkeit der Werte untereinander gewährleistet.

Diese Werte werden anschließend in das neuronale Netz überführt, um in den Daten nach Zusammenhängen und Auffälligkeiten zu suchen. Die nachfolgende Grafik repräsentiert diese anschaulich.

Abbildung 10: Softwarebeispiel RayQ



Die Software operiert mit dem RGB-Farbraum und stellt Informationen über Farben zur Verfügung. Die Würfelfarbe bildet den Datenbereich der Anzahl von Bestellungen beim gleichen Kundenbetreuer ab. Über weitere Farben (Blau/Rot/Grün) auf den Flächen werden Hypothesen einer Analyse abgetragen. Hier besteht auch die Chance, im Sinne des spielerischen Umgangs mit verschiedenen Hypothesen (Einfärbung der Flächen) einen Mehrwert an Erkenntnis zu gewinnen.

Im Beispiel wurden auf der Ebene folgende Hypothesen eingefärbt:

- Blau: Je blauer, desto mehr unterschiedliche Kundenbetreuer bedienen die Kunden.
- Rot: Je roter, desto größer die Anzahl der bestellten Stücke.
- Grün: Je grüner, desto höher der eingeräumte Rabatt für die Kundenbestellungen.

Als Ergebnis des Trainings repräsentiert die Software die Kunden als Würfel in einer Landschaft. Große Würfel sind mehrere Kunden, kleine Würfel einzelne Kunden. Die Landschaft hat die Aufgabe, ähnliche Daten nahe beieinander und unähnliche räumlich distanziert zu verorten. Die Ähnlichkeit bestimmt sich hierbei aus allen angelernten Faktoren.

4 Arten von Dokumentenmissbrauch

4.1 Fälschung

Die Fälschung ist der Oberbegriff für alle Totalfälschungen, Verfälschungen oder fälschlich ausgestellte Urkunden; häufig wird der Begriff auch als Synonym für „Totalfälschung“ gebraucht.

4.1.1 Totalfälschung

Beim gesamten Dokument handelt es sich um eine Fälschung.

4.1.2 Verfälschung

In einem echten Dokument werden Veränderungen vorgenommen. Verfälschungen können z. B. erfolgen durch:

- mechanische Rasuren;
- chemische Rasuren;
- Hinzufügen oder Überschreiben von Daten;
- Austausch von Schriftzeichen;
- Überkleben/Abdecken;
- Entfernen von kompletten Seiten;
- Austausch oder Verändern von Lichtbildern (integriert oder herkömmlich eingebrachten Bildern des Inhabers).

4.1.3 Fälschlich ausgestellte Urkunde

Hierbei handelt es sich um ein echtes Dokument, das als Blanko-Vordruck entwendet und von nicht autorisierter Stelle ausgefüllt worden ist, also beispielsweise vom Fälscher ausgestellt wurde.

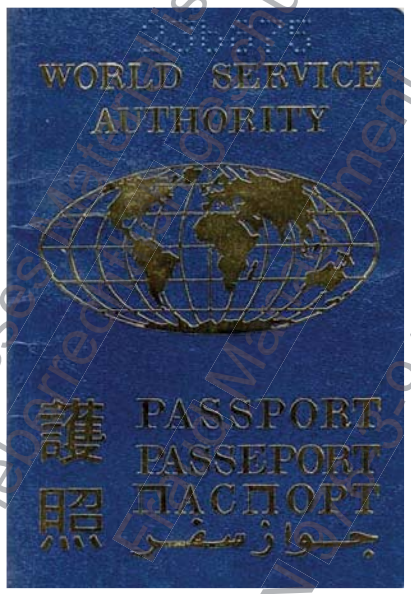
4.2 Phantasiedokument

Phantasiedokumente oder auch Pseudodokumente bzw. fingierte Dokumente sind nach Aussehen und Inhalt einem echten Dokument nachempfunden, jedoch nicht von einer

rechtlich anerkannten existenten Behörde bzw. Institution eines völkerrechtlich anerkannten Staates oder einer Organisation ausgestellt und daher rechtlich ungültig.

Während Pseudodokumente frei erfundene Staats- oder Organisationsbezeichnungen tragen, handelt es sich bei einem fingierten Dokument zwar um ein solches mit der Bezeichnung eines existierenden Staates bzw. einer existierenden Organisation, es entspricht jedoch keinem existierenden Musterdokument. Häufig werden derartige Fingierungen auch als Totalfälschungen bezeichnet. Bei dem in der folgenden Abbildung dargestellten Dokument handelt es sich um ein Phantasiedokument der nicht existenten World Service Authority.

Abbildung 17: Phantasiedokument



4.3 Ausweismissbrauch

Beim Ausweismissbrauch „benutzt“ der Delinquent einen „echten“ Ausweis, weil die abgebildete Person im Ausweis dem Delinquenten sehr ähnlich sieht. Das benutzte Dokument bleibt also völlig unverändert in Originalzustand. Der Ausweismissbrauch darf auf keinen Fall unterschätzt werden. Je besser ein Dokument gegen Total- oder Verfälschung abgesichert ist, desto größer ist die Wahrscheinlichkeit einer missbräuchlichen Benutzung.

zuholen. Ist das Unternehmen durch einen professionellen Incident-Response-Prozess gut aufgestellt, können die hier entstandenen Informationen und Erkenntnisse gleich für das computer-forensische Verfahren übernommen werden. Die gewonnenen Daten können im Weiteren für eine Beurteilung des Täterverhaltens oder für eine gerichtliche Beweisführung genutzt werden.

6 Vorgehensweisen

Ein kleiner Einblick in die Umsetzung der Handlungsmöglichkeiten soll die Thematik anhand der Vorgehenssystematik in der Computer-Forensik darstellen. Der Prozess der Computer-Forensik lässt sich in die folgenden fünf Schritte einteilen, die im weiteren Verlauf dieses Beitrages näher erläutert werden:

- Vorbereitung;
- Beweiserhebung und -sicherung;
- Untersuchung;
- Bewertung;
- Dokumentation.

6.1 Vorbereitung

Auch wenn alle Schritte grundsätzlich gleichwertig sind, so zeigt die Praxis, dass es an der Vorbereitung am meisten mangelt. Nur wenn die Organisation präventiv entsprechend aufgestellt ist, nur wenn die Voraussetzungen geschaffen wurden und nur, wenn all diese Prozesse ineinander greifen, kann erfolgreich ermittelt werden. Dabei wird der Erfolg nicht nur an der Identifizierung des Täters gemessen, sondern auch an der Gerichtsfestigkeit der Beweise.[9]

Ein Konzept für die Behandlung von Sicherheitsvorfällen muss vorab erstellt werden. Nicht nur den Administratoren und Sicherheitsbeauftragten, auch der Unternehmensleitung muss klar sein, dass ein Sicherheitsvorfall sich jederzeit ereignen kann.[10] Alarmierungsregelungen müssen getroffen und im Idealfall permanent überprüft oder „geübt" werden. Weisungsbefugnisse und Notfallkompetenzen müssen entwickelt und der Veränderung des Alltages angepasst werden. Ein Monitoring-Konzept für die Vorfalls-

[9] Vgl. auch den Beitrag von Zawilla zur Vorgehensweise bei Sonderuntersuchungen.

[10] Vgl. auch den Beitrag von Bédé zu Krisenmanagement im Unternehmen.

behandlung ist wichtig. Damit wird geregelt, welche über den Alltagsbetrieb hinaus notwendigen Daten protokolliert und regelmäßig ausgewertet werden sollen. Sinnvoll ist hier die Einbindung von Datenschutz und Betriebsrat.[11] Eine erweiterte Protokollierung, beschränkt auf aktuelle sicherheitsrelevante Vorfälle, ist oft im Interesse von Datenschutzaspekten, kann doch so das Gebot der Datensparsamkeit unterstützt werden.[12]

Auch unter Datenschutzaspekten sollte bedacht werden, dass nicht nur die Frage der Datenerhebung, sondern auch die Frage der Berechtigung auf Daten eine zentrale Rolle spielt. Dabei stehen Datenerhebung und Datenschutz nur scheinbar im Widerspruch: Daten, die nicht erhoben werden, sind auch nicht gegen unberechtigten Zugriff zu sichern. Ein Berechtigungskonzept und eine Löschungsstrategie brauchen dafür nicht erstellt zu werden.

Im Gegensatz dazu sind manche Kontrollen (oder eine Aufklärung) ohne Protokolldaten nicht möglich oder eine Protokollierung ist an anderer Stelle vorgeschrieben. Oft wird in diesem Zusammenhang übersehen, dass Protokolldaten nicht nur belastende, sondern im Sinne der potenziellen Täter auch entlastende Umstände liefern können, denn es geht nicht immer nur um Kompromittierung, sondern auch um eine entlastende Wahrheitsfindung.

6.1.1 Einbindung von Ermittlungsbehörden

Die Frage, wann und unter welchen Umständen die Ermittlungsbehörden informiert werden sollen, lässt sich ohne konkreten Vorfall entspannt diskutieren. Die Zeit, die bei der Festlegung der Regeln in einem Ernstfall so gewonnen wird, ist besonders wertvoll. Es empfiehlt sich daher, bereits im Vorfeld – ohne konkreten Vorfall – mit den Ermittlungsbehörden oder Sicherheitsspezialisten Kontakt auf zu nehmen. Die Suche nach den zuständigen Stellen oder Personen lässt sich so im Schadensfall erheblich reduzieren. Ansprechpartner und auch Auskünfte sind mit einer professionellen Vorbereitung schneller zu erlangen.

6.1.2 Menschlicher Faktor

Die Zusammensetzung eines Response-Teams ist von besonderer Bedeutung. Es hat sich gezeigt, dass nicht nur die technischen Kompetenzen auf den betreffenden Spezialgebieten von Bedeutung, sondern auch die menschlichen Fähigkeiten und die Erfahrung der

[11] Vgl. auch den Beitrag von Röck zu Arbeitsrecht sowie von Christ zu Datenschutz und Mitarbeiterkontrollen.

[12] Vgl. auch den Beitrag von Kob zu Daten- und Informationssicherheit.