Bundeskriminalamt

# Innentäter in Unternehmen

**Zusammenstellung aktueller inländischer Forschungsbeiträge zum Forschungsstand und Handlungsempfehlungen zur sogenannten Innentäterschaft**

**IZ 34**

**Julia Weber**

**Stand: 04.08.2017**

BKA

## Inhaltsverzeichnis

## 1. Einleitung und methodisches Vorgehen

Das Schadenspotenzial für Unternehmen durch Innentäter stellt, insbesondere im Zuge der zunehmenden Bedrohung durch das Tatmittel Internet, eine spezielle Bedrohung dar. Sowa beschreibt, dass im Jahr 2015 der größte finanzielle Schaden für Unternehmen durch Vorfälle in der Lieferkette, Betrug durch interne Mitarbeiter oder durch Cyberspionage verzeichnet wurde (Sowa 2017: 1[1]). Vorhandene Schutzmaßnahmen sind anscheinend oftmals nicht geeignet um ein auffälliges Verhalten frühzeitig zu erkennen.

Im August 2017 erfolgte eine Literaturrecherche zum Thema „Innentäter in Unternehmen". Hierzu wurde anhand einer umfassenden stichwortgestützten Suche[2] innerhalb von Suchportalen, Internetseiten von Forschungsinstituten und Lehrstühlen sowie Internetpräsenzen einzelner Behörden und Unternehmen nach Veröffentlichungen externer nationaler Forschungsbeiträge recherchiert. Das Ziel des vorliegenden Berichtes war es der Frage nachzugehen, welche Erkenntnisse zu Innentätern vorliegen und wie groß die Gefahr der Kriminalität durch interne Mitarbeiter in Unternehmen heutzutage ist. Zusätzlich sollte dargestellt werden, welche präventiven Ansatzmöglichkeiten es für Unternehmen gibt und wie die Anzahl bzw. das potenzielle Risiko für Unternehmen Opfer von Straftaten durch Innentäter zu werden verringert werden kann.

Grützner/Jakob definieren Innentäter als

> *„[…] Menschen […], die in Unternehmen und Organisationen gezielt und mit Vorsatz dolose Handlungen durchführen. Innentäter können durch Angreifer gezielt in Organisationen positioniert worden sein oder Menschen werden durch verschiedene Umstände zu Innentätern." (Grützner/Jakob, Compliance von A-Z 2. Auflage 2015).*[3]

Diese Definition zielt somit potenziell auf IT-Verantwortliche und IT-Nutzer, aber auch auf alle Personen, die über internes Know-How verfügen können wie bspw. Mitarbeiter, Lieferanten, Partner, Kunden oder anderweitige Dienstleister.

Bei der Recherche fällt auf, dass die Thematik im wissenschaftlichen Kontext eher im Rahmen der Bearbeitung spezieller Delikte und Themenfelder wie Produkt- und Markenpiraterie, Korruption, Geheimnisverrat, Insiderhandel, IT-Sicherheit, Wirtschaftsschutz oder Compliance sowie bei der Gesamtbetrachtung „Täterprofile und –motive" erwähnt wird. Daher lässt sich eine Forschungslücke in Bezug auf eine spezielle Betrachtung der Innentäterschaft feststellen. Innentäterschaft ist nicht phänomenspezifisch - die gesamte Breite unternehmensschädigender Delikte kann durch Innentäter begangen werden. Es zeigt sich eine Bandbreite vom „bewussten" Täterverhalten wie bei Korruption, Untreue, Insiderhandel, Geheimnisverrat etc. bis hin zu „unbewusstem" Täterverhalten wie beispielsweise beim Social Engineering. Konkretere und aktuelle Informationen zur Thematik bieten die Studien der verschiedenen Unternehmensberatungen, die die aktuellen Probleme und Herausforderungen der Unternehmen zeitnah aufgreifen und in Befragungen oder bei Fachtagungen

[1] Aleksandra Sowa: „Compliance-Schicht - Die Check-Phase des Managements der Informationssicherheit" in: Management der Informationssicherheit – Kontrolle und Optimierung. Bonn: Springer, 2017.

[2] Folgende Suchbegriffe wurden zur Recherche verwendet: Innentäter, Fraud management, Bilanzbetrug, Mitarbeiterkriminalität, Mitarbeiterbeteiligung, Unternehmenskriminalität, Whistleblowing/Whistleblower, Betriebsspionage, Informationsschutz, Datenmissbrauch, -diebstahl, Personaldelikt, Supply Chain Security, Sicherheit in der Lieferkette, Know-how Schutz

[3] In Abwandlung der Definition des Bundesamtes für Sicherheit in der Informationstechnik (BSI) werden potenzielle Innentäter unter der Prämisse von kriminellem vorsätzlichen Verhalten u.a. als: „[…]*Personen mit (privilegiertem) Zugriff auf bzw. Zutritt zu IT-Komponenten, IT-Diensten, Installationen, Dokumenten oder sonstigen ggf. kritischen Informationen und Geräten [beschrieben]*." (BSI 2013: 1). Die Definition von Grützner/Jakob ist weiter gefasst und betont klar die Notwendigkeit eines kriminellen Charakters, womit eben nicht jeder Mitarbeiter unter pauschalen Verdacht auf Innentäterschaft gestellt werden kann.

umsetzen. Zudem haben sich viele Beratungsfirmen auf die Schulung von Unternehmen und Mitarbeitern spezialisiert, um Wirtschaftskriminalität in diesen Bereichen zu verhindern. Bei diesen Firmen liegt viel (Erfahrungs-)Wissen vor, das von Unternehmen eingekauft und genutzt werden kann. Hier finden sich aussagekräftige qualitative Informationen zur Thematik.

## 2. Studien und Artikel zu Innentätern in Unternehmen

### 2.1 Studien von Wirtschaftsprüfungsgesellschaften und andere Veröffentlichungen

**Ernst &Young (2016): „Global Fraud Survey – Ergebnisse für Deutschland" und Ernst & Young (2017): „Human Instinct, Machine Logic – which do you trust most in the fight against fraud and corruption?" Europe, Middle East, India and Africa Fraud Survey.**

Gegenstand: Befragung von ca. 2800 Unternehmen in 62 Ländern weltweit. Vorrangig befragt wurden Vorstandsmitglieder sowie Mitarbeiter u.a. aus den Abteilungen Interne Revision und Rechnungswesen. Die Befragung fand von Oktober 2015 bis Januar 2016 statt. In Deutschland wurden 50 Befragungen durchgeführt.

Ziele: Empirische Befunde zu Wirtschaftskriminalität in Unternehmen erheben und im internationalen Vergleich darstellen.

Forschungsfragen: Inwieweit berücksichtigen Unternehmen Präventionsmaßnahmen und wie werden diese umgesetzt? Wie ist die Einstellung der Führungsebenen zu Wirtschaftskriminalität und inwiefern gibt es länderspezifische Unterschiede?

Ergebnisse:

- Ca. 23 Prozent der befragten Manager geben an, dass sie, um ihre Karriere voran zu treiben, zu mindestens einer der folgenden Verhaltensweisen bereit wären: Externe täuschen, das eigene Management mit falschen Informationen versorgen und unethisches Verhalten bei Kunden, Lieferanten etc. ignorieren.
- Jeder zehnte Manager würde Behörden täuschen, um sich bzw. das Unternehmen nach vorne zu bringen. Diese Zurückhaltung oder Falschinformation richtet sich jedoch nicht nur gegen Dritte, sondern jeder zehnte würde auch das eigene Management täuschen (E&Y 2017)[4].
- Aufgrund dessen, dass inzwischen zwei von drei Unternehmen Antikorruptionsrichtlinien implementiert haben und diese auch strengstens verfolgt werden, ist jeder sechste Manager eines deutschen Unternehmens der Meinung, dass die eigene Wettbewerbsposition durch eben diese Richtlinien geschmälert wird.
- Barzahlungen oder die absichtliche falsche Darstellung von Finanzergebnissen sind in Deutschland ein Tabu – weltweit wird dies von jedem 25. Manager als akzeptabel betrachtet.
- Überraschend ist, dass gerade die jüngere Manager-Generation unethischem Verhalten offener gegenüber steht, als die ältere. So würden 25 Prozent der Generation Y Geldzahlungen anbieten, um ihre Karriere am Laufen zu halten (im Gegenzug dazu nur 14 Prozent der älteren Manager-Generation) (E&Y 2017).
- 77 Prozent der deutschen Befragten denken, dass die strafrechtliche Verfolgung von Einzelnen helfen wird, Leute in Führungspositionen davon abzuhalten Korruption, Betrug etc. zu begehen (S.7). Die Mehrheit ist der Ansicht, dass Aufsichts- und

[4] Ernst and Young Europe, Middle East, India and Africa Fraud Survey 2017: "Human instinct Machine Logic – which do you trust most in the fight against fraud and corruption?".

Strafverfolgungsbehörden bei Fällen von bspw. Korruption diese konsequent verfolgen und es zur Verurteilung kommt. Im weltweiten Vergleich hat nur jeder dritte diese Auffassung.

- Nahezu die Hälfte der Befragten hat bereits einmal in Betracht gezogen, ihren Arbeitsplatz aufgrund von unethischem Verhalten in ihrem Unternehmen zu kündigen. Besonders auffällig ist, dass eine hohe Anzahl der Befragten eventuelle Besorgnis über unethisches Verhalten nicht meldet. Die Gründe hierfür reichen von Besorgnis über die zukünftige Karriere (51 Prozent), Angst um persönliche Sicherheit (46 Prozent) und Loyalität zu den Kollegen (30 Prozent) bis Loyalität zum Unternehmen (24 Prozent). Kenntnisse über interne Whistleblowing-Hotlines sind nur bei ca. 1/3 der Befragten vorhanden. Wenn etwas gemeldet wird, dann zu 57 Prozent einer Strafverfolgungsbehörde.

Empfehlungen gibt die Studie aus dem Jahr 2017 folgende:

- Anomalien in den Arbeitsstunden der Angestellten beobachten, Versuche auf Daten zuzugreifen, die nur begrenzt zugänglich sind sowie der Gebrauch von unautorisierten Datenträgern sollten kontrolliert werden. Zudem sollen Risikoanalysen durchgeführt und spezielle Schutzmaßnahmen bei erhöhtem Risiko umgesetzt werden. Augenmaß bei den eingesetzten Kontrollmaßnahmen und transparente Information sowie Sensibilisierung der Mitarbeiter, um dem Spannungsverhältnis zwischen zwingender Kontrolle und Privatsphäre bzw. Rechten der MA zu wahren.

Bewertung: Erkenntnisse zu Ansichten und Einstellungen von Managern sind relevant, um Einblicke in Unternehmenskulturen und ethische Standards zu erhalten. Diese haben direkten Einfluss auf die Mitarbeiter und somit auf potentielle Innentäter. Interessant sind zudem die Ergebnisse bzgl. der Hinweisgebersysteme – hier sollte man ggf. überlegen, solche Hotlines bei den Mitarbeitern mehr zu bewerben.[5]

**BfV und ASW Bundesverband (2015): Veröffentlichung zur 9. Sicherheitstagung am 13. Mai 2015.**

Gegenstand: Darstellung der Gefahr, die von Innentätern ausgeht und wie einzelne Unternehmen beispielhaft Innentäter versuchen zu identifizieren und wie man präventiv gegen Innentäter vorgehen kann.

Ziele: Darstellung der Hintergründe zur Innentäterschaft und Betonung der anhaltenden Gefahr, die von Innentätern ausgeht. Die Balance zwischen Strafrecht, Zivilrecht und Arbeitsrecht finden, einen verstärkten Informationsaustausch zw. Behörden und Netzwerken vorantreiben sowie die Anpassung von Befugnissen und der Reaktionsgeschwindigkeit auf neue Gefahren. Zudem soll eine Bewusstseinsstärkung für das Phänomen der Innentäter im Unternehmen erreicht werden. Wirtschaftsschutz soll gemeinsam mit Unternehmen, Sicherheitsbehörden und verschiedenen Verbänden entwickelt werden. Ein weiteres Ziel ist die Etablierung einer „human Firewall“ durch aufmerksame Mitarbeiter.

Ein Konzept eines Komitees zur Überwachung der Einhaltung von Richtlinien (Personalabteilung, der Group Legal, der Corporate Security und Internal Audit) soll angeregt werden.

Leitfragen: Was sind Motive, Einstellungen und Möglichkeiten die zu einer Innentäterschaft führen können? Wie groß ist die Bedrohung durch Innentäter für die Unternehmen? Wie kann man Innentäter identifizieren und wie kann man diese dolosen Handlungen unterbinden oder vermeiden?

Ergebnisse:

[5] Anmerkung: Das Thema des Hinweisgebertums und des Whistleblowings wird in einigen Fachartikeln thematisiert. Hierzu sind bspw. lesenswert: „Wirtschaftskontrolle durch Whistleblowing? Empirische Befunde zu Entscheidungsprozessen von Hinweisgebern“ von Kölbel, Ralf und Nico Herold aus dem Jahr 2015 und „Whistleblowing zur Erkennung schwerer Kriminalität?: Einsatz internetbasierter Hinweisgebersysteme zwecks Gewinnung von Ermittlungsansätzen“ von Dubs, Stefan aus dem Jahr 2014.

- Innentäter bergen durch Zugangsmöglichkeiten zu Daten, Räumen und Netzwerken ein hohes Schadenspotenzial - Hierarchieebenen bilden für einen Innentäter keine Grenzen
- Wichtig: kein Generalverdacht, das Vertrauen als Grundlage der Zusammenarbeit bewahren.
- Präventiv richten die Maßnahmen sich nach dem Arbeitsumfeld und den aus der Arbeitsplatzbeschreibung resultierenden Zugangsberechtigungen. Maßnahmen sind:
    1. personell (Aufgabenteilung, Awareness-Trainings für Mitarbeiter),
    2. technisch (durch Barrieren und erhöhen der Entdeckungsmöglichkeiten),
    3. prozessual (Abgleich mit Sanktionslisten, Pre-employment checks/screening (PES), Access Management, individuelle Zuteilung von Zugriffsrechten) oder
    4. intelligence (Open-Source-Analysen, Monitoring und Sammlung von Informationen von Verbänden und Behörden).
- Wie sind die Motive des Täters geprägt? (psychisch, ideologisch oder materiell) und was sind Absichten? (vorsätzlich/geplant, billigende Inkaufnahmen, (grobe) Fahrlässigkeit)
- Falschangaben bei der Bewerbung: ist es Betrug? → Falschangaben zu Berufs- oder Stellenbezeichnungen, Kauf von Titeln und Diploma oder Urkunden (§267, 263, 132a StGB)
- Ursachen/Begünstigung von Betrug: Digitalisierung, Online-Auftritt der Firmen, Onlinebewerbungen, Kandidatenpool, Globalisierung und international unterschiedliche Berufsbezeichnungen, Druck auf die Bewerber, Diploma Mills, Sprachliche Hürden
- Was wird bei einem PES überprüft? Bildungsabschluss, Arbeitsverhältnis, Praktika, Referenzen, Firmenbeteiligungen, Kreditwürdigkeit, Sanktionslisten (bei individual Compliance Checks u.a. auch Abgleich mit Korruptions- oder Anti-Terror-Listen), mediale Berichterstattung
- Wer überprüft die Daten? Experten, persönlicher Kontakt, interne Datenbank, Arbeitgeber, Behörde, eigene Recherche, Partnernetzwerke, kostenpflichtige Compliance-Datenbanken → wichtig: Transparenz für Bewerber und Arbeitsgeber, einheitliches Vorgehen
- Mögliche Schäden:
    - Zeitverlust durch neue Rekrutierung
    - Reputationsschaden und Haftungsrisiken
    - Verschlechterung der Kundenbeziehung und niedrigere Arbeitsmoral
- Verantwortung für Mitarbeiter übernehmen durch:
    - Talententwicklung- und -förderung
    - Arbeitssicherheit und Arbeitszeitmodelle
    - Nachwuchsförderung und diversity
    - Leistungsvergütung und Aus- und Weiterbildung
- Identifizierte Risiken:
    - Auf Geschäfte bezogen
    - Finanzielle und rechtliche Risiken
    - Produkt- und Markenpiraterie und Spionage
    - Personalbereich
    - E-Crime sowie
    - Umwelt- und Sicherheitsrisiken
- Business Profiling:
    - Zusammenhang zwischen Unternehmensloyalität und der Anzahl an Fehltagen: Innentäter sind illoyal und weisen dementsprechend mehr Fehltage als loyale Mitarbeiter auf. Unternehmen verursachen durch schlechte Führung und ein

schlechtes Arbeitsumfeld den daraus resultierenden Rückgang der Loyalität ihre Innentäter selbst → allerdings nur auf einen speziellen Tätertyp zu beziehen, auf Täter, die u.a. aus „Engagement" handeln, trifft dies sicher nicht zu.
    - Wichtig an einem Unternehmen ist den MA: Respekt, interessanter Job, Zeit für Privatleben, Grundgehalt
    - Empirische Täterprofile[6]: der melancholische Individualist, manipulative Helfer, optimistische Hedonist, loyale Skeptiker, gewissenhafte Perfektionist, objektive Beobachter, willensstarke Kämpfer, dynamische Sieger bewertet anhand der Eigenschaften Loyalität, Integrität, Regeltreue, Risikoneigung
    - Bspw. Unterschied dynamischer Sieger (1) gewissenhafter Perfektionist (3): 1 ist loyaler als 3 und auch seine Integrität ist wesentlich höher genau wie die Regeltreue. 3 ist sehr risikofreudig. Edward Snowden wäre bspw. ein gewissenhafter Perfektionist
    - Bewusstsein für Charaktereigenschaften von verschiedenen Tätertypen identifizieren und Zusammenhänge sichtbar machen, Risiken identifizieren, MA und Führungskräfte unterstützen
- Thema der Unternehmenspsychopathen wird angesprochen – so gäbe es funktionale Psychopathen („Top-Performer") und dysfunktionale Psychopathen (keine Kontrolle, verantwortungslos) → es gibt auch Schulungsangebote zu Business Profiling für Unternehmen, aber auch für Privatpersonen

Bewertung: Eine aufschlussreiche Zusammenstellung, da von potenziellen Opfern, den Unternehmen, selbst entwickelte Strategien oder Leitgedanken zur Minimierung von Innentätern präsentiert werden. Bei solchen Tagungen wird das Zusammenwirken von allen beteiligten Akteuren (Behörden, Verbände, Unternehmen) gelebt und Wissen zusammengetragen. Der Austausch von Best-Practise-Ansätzen und das Lernen voneinander werden ermöglicht. In einem weiteren Schritt wäre eine wissenschaftliche Aufbereitung der Ergebnisse solcher Tagungen zur Entwicklung von gesicherten Thesen, um daraus effektive und praktische Handlungsempfehlungen abzuleiten, sinnvoll.

**KPMG (2017): „Neues Denken, neues Handeln" Studienteil B: Cyber.**

Gegenstand: Vorrangig geht es in der Studie, die auf Experteninterviews beruht, um die Bedrohung und Folgen durch Cyber-Angriffe und -Risiken für Unternehmen. Betont wird, dass aufgrund der Betroffenheit von selbst gut geschützten Unternehmen und des zukünftig vermehrten Einsatzes von Open-Source-Software die Anfälligkeit für Cyber-Angriffe wachsen wird. Dies zeigen Fallbeispiele, die den leichtfertigen Umgang mit Malware oder externen Datenträgern darstellen. Aufgrund dessen sieht KPMG die Notwendigkeit, dass ein erhöhter Bedarf an Cyber-Versicherungen bestehen wird.
Ziele: Überblick über die Gefahr durch die Zunahme von Cyber-Risiken und der zunehmenden Digitalisierung in der Wirtschaft sowie einige konkrete Handlungsempfehlungen. Entwicklung eines Prognosemodells zur Simulation der Cyber-Versicherungsprämie.
Forschungsfragen: Welche strategische Relevanz und welches Potenzial hat eine Cyber-Versicherung für das Kompositgeschäft der Versicherer im deutschsprachigen Raum? Welche Produktgestaltung ist mit Blick auf die unterschiedlichen Kundensegmente und Versicherungsumfänge am sinnvollsten? Wie sehen die Risiken konkret aus und wie können sich die Versicherer die für ein professionelles Cyber-Versicherungsgeschäft unabdingbaren Fähigkeiten aneignen? Wie sollte die Tarifierung in

[6] Diese werden genauer in den Unterlagen des Tagungsbandes unter der Präsentation von Ralf Kopp, Geschäftsführer der KOPP GmbH, ausgeführt (ab S.28).

einem Geschäft ohne Vergangenheitswerte gestaltet werden und wie reguliert man Schäden in einem Geschäft, zu dem es praktisch keine Schadenerfahrung gibt? Wie bildet man die Cyber-Sparte in seiner Organisation ab? Bleibt es bei einem relativ überschaubaren Prämienvolumen von einigen hundert Millionen Euro Jahresprämie in Deutschland oder entwickelt sich dieses Feld tatsächlich zu einer ernst zu nehmenden Sparte? Lohnt sich der Aufwand, der mit dem Einstieg in das Cyber-Geschäft verbunden ist, angesichts der schwer greifbaren Risiken überhaupt?

Ergebnisse:

- Die meisten der Cyber-Angriffe werden intern begangen; "typische“ Innentäter sind: aktuelle oder ehemalige Mitarbeiter sowie Akteure aus dem Umfeld des Unternehmens wie bspw. Geschäftspartner oder Service-Firmen (KPMG 2017: 22). Der kleinere Teil der Außentäter besteht aus OK-Tätern, Hobby-Hackern, ausländischen Nachrichtendiensten und nicht identifizierten Tätern. Diese Ergebnisse werden auch durch die **Bitkom Studie aus dem Jahr 2015** bestätigt (52 Prozent aller Angriffe konnten früheren oder aktuellen Mitarbeitern zugeordnet werden).
- Täterprofil: „Der typische Cyber-Kriminelle ist: mit 60-prozentiger Wahrscheinlichkeit Innentäter, also Teil der Organisation, die er angreift, männlich und zwischen Mitte 30 bis Mitte 50 Jahre alt, bereits mindestens sechs Jahre im Unternehmen beschäftigt, meist eine Führungskraft, eine respektierte, freundliche Person.“. Zudem listet KPMG typische Versicherungsleistungen bei einem Cyber-Angriff nach dem Prinzip „Find it, Fix it, Run it“ auf.
- Diskutiert werden sowohl Versicherungen für gewerbliche, als auch für Privatkunden: gewerbliche Versicherungen bieten meist mehr Schutz als private, allgemein bieten die gängigen Versicherungen geringen bis keinen Versicherungsschutz gegen Cyber-Angriffe → Handlungsbedarf

Bewertung: Für eine eingehendere Beschäftigung mit dem Thema Cyber-Risiken sicher von hoher Relevanz – besonders interessant ist die Profilerstellung. Auch die einzelnen Leistungen der Versicherung bei einem Angriff auf das Unternehmen, unterteilt in herkömmlich versicherte Schadensfälle und solche die unter einer Cyberversicherung inbegriffen sind, sind sehr detailliert beschrieben[7].

**Bitkom und BfV (2017): „Wirtschaftsschutz in der digitalen Welt“.**

Gegenstand: CATI[8] Befragung von über 1000 Unternehmen ab 10 Mitarbeitern zu ausgewählten Fragestellungen. Zielgruppe waren vorrangig Führungskräfte, die sich mit dem Themenbereich Wirtschaftsschutz beschäftigen. Die Umfrage fand von Januar bis März 2017 statt.

Ziele: Darstellung der Betroffenheit von Unternehmen durch Wirtschaftskriminalität (Schaden) sowie der Motive und Profile der Täter.

Forschungsfragen: Welche Unternehmen sind betroffen? Auf was haben es die Täter abgesehen und wie wertvoll waren diese Informationen? Woher kommen die Täter aus den Unternehmen? Wie werden die Unternehmen auf Straftaten aufmerksam und wie werden die Straftaten verfolgt? Welche Sicherheitsmaßnahmen ergreifen die Unternehmen zu ihrem Schutz?

Ergebnisse:

[7] Siehe hierzu Anlage.
[8] Computer Assisted Telephone Interview

- Jedes zweite Unternehmen wurde in den letzten zwei Jahren Opfer von Datenklau, Spionage oder Sabotage (insg. 53 Prozent der Befragten). Besonders betroffen waren mittelgroße (100 – 499 Mitarbeiter; 65 Prozent) bis große (500+ Mitarbeiter; 60 Prozent) Unternehmen.
- 30 Prozent der befragten Unternehmen gaben an, dass IT- oder Telekommunikationsgeräte entwendet wurden. Ob dies in Bereicherungsabsicht über die technischen Geräte oder zum Zwecke des Datendiebstahls erfolgte ist nicht feststellbar. Analoges und digitales Social Engineering folgen mit jeweils 20 und 18 Prozent. Der Diebstahl von sensiblen Daten lag bei 17 Prozent der Befragten vor.
- Relevanz der gestohlenen Daten: in 62 Prozent der Fälle von Datenklau wurden, laut der Studie, unkritische Business-Informationen gestohlen[9].
- In 62 Prozent der Fälle gehen die Unternehmen davon aus, dass der Täterkreis aus aktuellen oder ehemaligen Mitarbeitern besteht. Somit kann die Mehrheit der Fälle dem Umfeld des Unternehmens zugeordnet werden.
- 37 Prozent der Handlungen wurden von Deutschland aus vorgenommen, 23 Prozent aus dem osteuropäischen Raum und 18 Prozent von Russland aus.
- Meldung von Fällen: 30 Prozent sind durch Hinweise von Mitarbeitern gemeldet worden und 30 Prozent sind zufällig aufgefallen. Bei Bekanntwerden solcher Handlungen schaltet jedes dritte Unternehmen die Polizeibehörden oder anderweitige staatliche Stellen ein. Das Motiv für eine interne Aufarbeitung der Vorfälle und der Verzicht auf eine Strafanzeige ist in 41 Prozent der Fälle ein gefürchteter Imageschaden.
- Besonders organisatorische Sicherheitsaspekte werden von Unternehmen zum Schutz eingesetzt. Hauptsächlich sind dies: die Festlegung von Zugriffsrechten sowie Kennzeichnung von Betriebsgeheimnissen. Zudem führen mehr als die Hälfte der Unternehmen Sicherheits-Checks durch und schulen ihre Mitarbeiter. Alle befragten Unternehmen setzen bei der technischen Sicherheit auf Passwortschutz, Firewalls, Virenscanner und Backups.
- Empfehlungen lauten:

1. Steigerung der technischen IT-Sicherheit durch: Ergänzung des Basisschutzes um eine Verschlüsselung und eine Angriffserkennung, ein Security Information Event Management (Erkennung von Abweichung des Normalen und Überwachung von vernetzen Geräten)
2. Erhöhung der Unternehmenssicherheit durch: präventives Risikomanagement (Identifizierung von externen und internen Gefahren und Schwachstellen, Einrichtung von Zugriffsrechten für sensible Daten, Einrichtung eines Notfallmanagements)
3. Personelle Sicherheit erhöhen durch: Sicherheitskultur und IT-Experten mit Produktions-Know-How

Bewertung: Die Studie von Bitkom zeigt die Bedeutung des Faktors „Mensch“ auf und stellt dar, dass Unternehmen bei Verdachtsfällen doch eher intern ermitteln und anschließend über die Hinzuziehung staatlicher Organe entscheiden, da viele der Unternehmen Imageschäden fürchten. Hier gilt es seitens der Aufsichts- und Strafverfolgungsbehörden weitere Sicherheit zu bieten und die Meldung von Straftaten innerhalb des Unternehmens an die Strafverfolgungsbehörden zu fördern. Zudem trifft die Studie auch Aussagen über den Wertgehalt des gestohlenen/ unterschlagenen Materials.

[9] Kommunikationsdaten wie E-Mails (41%), Finanzdaten (36%), Kundendaten (17%), Geistiges Eigentum (11%), Mitarbeiterdaten (10%), Business-Informationen wie Marktanalysen (1%). Allerdings sollte man darauf hinweisen, dass auch das Zusammenspiel verschiedener auf den ersten Blick unkritischer Informationen Möglichkeiten für kriminelle Handlungen eröffnen kann.

**Pricewaterhouse Coopers (PwC) (2016): „Wirtschaftskriminalität in der analogen und digitalen Wirtschaft 2016".**

Gegenstand: Die achte Studie zu Wirtschaftskriminalität im Auftrag von PwC wurde von September bis November 2015 durchgeführt. Grundlage ist ein standardisierter Fragebogen mit Hilfe dessen Personen aus 720 Unternehmen telefonisch interviewt wurden.

Ziele: Herausarbeitung von aktuellen Entwicklungen im Bereich der Wirtschaftskriminalität unter dem Gesichtspunkt der Industrie 4.0. Identifizierung von Schwachstellen und Ansätzen für Verbesserungsmöglichkeiten für die Unternehmen. Speziell sollen die Unterschiede und ggf. Überschneidungen zwischen der analogen und digitalen Begehung von Straftaten und deren Verhältnis herausgearbeitet werden.

Forschungsfragen: Wie stellt sich die Sicherheitslage in deutschen Unternehmen dar? Inwiefern gibt es Unterschiede zu den Vorjahren?

Ergebnisse:

- Die Mehrheit der angezeigten Fälle bezieht sich auf Daten- oder Wissensverlust und erfolgt durch Entwenden oder Kopieren von firmeninternen Dokumenten (42 Prozent)
- Eingehende Sensibilisierung des Personal- und Geschäftsablaufs ist essentiell
- Die Annahme, dass Wirtschaftskriminalität nur andere Unternehmen betrifft und nicht das eigene, ist weiterhin weit verbreitet.
- Möglichkeiten zur Zertifizierung des IT-Risk-Managements sind nur unzureichend bekannt → „Nur jedem zweiten Unternehmen […] [wäre] der Prüfungsstandard 980 des Instituts der Wirtschaftsprüfer in Deutschland (IDW PS 980) für CMS bekannt" (PwC 2016: 6).
- Gefahren innerhalb der Lieferkette haben viele Unternehmen erkannt und fordern von ihren Lieferanten den Nachweis über ein Compliance-Management-System.
- Für international tätige Unternehmen stellt die Rekrutierung loyaler Mitarbeiter im Ausland ein Problem dar.
- Häufigste Delikte im Zusammenhang mit klassischen Formen der Wirtschaftskriminalität: Vermögensdelikte (56 Prozent), Verstöße gegen Patent- und Markenrecht (17 Prozent), Korruption (neun Prozent) und wettbewerbswidrige Absprachen (sieben Prozent). E-Crime Straftaten: Vermögensdelikte die Mehrheit der Taten (Computerbetrug (23 Prozent), Manipulation von Konto- oder Finanzdaten (18 Prozent) und Ausspähen und Abfangen von Daten (16 Prozent).
- Weitere Sensibilisierung von Mitarbeitern, dass bei jeglicher Art der Kommunikation potenziell Wissen abfließen kann, ob gewollt oder ungewollt (vor allem bei Unternehmenswerten wie Offenheit und Transparenz). Hintergrund: mögliche Beeinflussung oder Abwerbung von Mitarbeitern auf Messen oder Tagungen
- Mitarbeiter besitzen eine essentielle Rolle bei der Erstentdeckung von Straftaten im Unternehmen → informelle Sozialkontrolle[10].
- Beziehung des Täters zum Unternehmen: Daten- und Wissensverlust wurde in 43 Prozent der Fälle durch interne Täter verursacht, der Anteil der internen Täter an anderen Wirtschaftsdelikten ist mit 57 Prozent der höchste. Knapp über die Hälfte aller Delikte mit Bezug zu Wirtschaftskriminalität wurden durch interne Täter begangen. Interne Täter verzeichnen bzgl. Daten- und Wissensverlust nicht die höchsten Prozentwerte – externe Täter ohne Geschäftsbeziehung machen 63 Prozent aus.

[10] In 35 Prozent der Fälle bei Daten- oder Wissensverlust und bei 30 Prozent bei anderen Wirtschaftsdelikten kam der Hinweis von interner Seite.

- Allgemeines Profil von Tätern der Wirtschaftskriminalität: männlich, zwischen 30 und 50 Jahren alt, anderweitig beschäftigt oder mittleres bis Top-Management, seit sechs bis 20 Jahren im Unternehmen angestellt.

Bewertung: Eine Umfrage, die neue Trends und bestehende Schwierigkeiten deutlich herausstellt. Schwerpunkte liegen auf der eingehenden Beschäftigung mit dem Mitarbeiter und dessen zentralen Rollen sowohl bei der Begehung von Straftaten als auch bei deren Aufklärung. Die Studie von PwC weist hinsichtlich der Häufigkeit der Straftatbegehung durch externe Täter Unterschiede zur zuvor erläuterten Bitkom-Studie auf.

## 2.2 Studien von sonstigen Forschungseinrichtungen und -instituten

**Udo Lindemann et al. (2017): „Know-How-Schutz im Wettbewerb – Gegen Produktpiraterie und unerwünschten Wissenstransfer".**

Gegenstand: Die gesamte Publikation beschäftigt sich mit Produktpiraterie und dem Vorgang des Wissenstransfers. Die vorliegende Auswertung bezieht sich auf Kapitel 3 „Schutz von Technologiewissen" und behandelt kritische Situationen, in denen Mitarbeiter zu Tätern werden können.

Ziele: Identifizierung der Motive für Wissenstransfer und erfolgreicher Strategien für Unternehmen für den Schutz ihres Wissens.

Forschungsfragen: Wie können Unternehmen unerwünschten Wissenstransfer vermeiden? Wie wird wertvolles von weniger wertvollem Wissen unterschieden? Wie können Unternehmen wertvolles Wissen schützen und durch was sind Situationen in denen Wissen transferiert wird charakterisiert?

Ergebnisse: Das Handeln von Mitarbeitern führt im Ergebnis dazu, dass Wissen von Mitarbeitern (MA) aus den Unternehmen an andere weitergetragen wird. Dies kann der Fall sein, wenn die Interessen des Mitarbeiters nicht im Einklang mit denen des Arbeitgebers stehen. Folgende Motive können dies befördern:

- Verbesserung der eigenen finanziellen Situation (durch bspw. Spionage)
- Arbeitsplatzwechsel zur Konkurrenz/ Gründung eines eigenen Unternehmens → Verbesserung der eigenen sozialen Stellung, Aufstiegswille, Patriotismus
- Negative Emotionen und Angstgefühle→ situationsbedingte, spontane Wissenspreisgabe
- Falscheinschätzung einer Situation → passiver, ungewollter Wissenstransfer

Situationen des Wissenstransfers:

- Push (Impuls vom Wissensgeber)
    1. Durchführung einer Geschäftstätigkeit vom Unternehmen: bspw. in Outsourcing-Situationen ist Wissenstransfer vonnöten, nicht nur Dokumente werden ausgetauscht sondern auch Erfahrungen, Muster oder Werkzeuge. Gefahr: Transfer von mehr Wissen als vom Zulieferer benötigt wird → schwierige Abgrenzung. Dies ist laut Ansicht des Autors bei Offshoring-Situationen weniger kritisch, da hier die Kontrollmöglichkeit größer ist, wobei auch ein gewisses Grundmisstrauen ggü. den anderen Niederlassungen besteht. Die Zusammenarbeit mit Zulieferern, besonders solche mit einem hohen Systemverständnis, schließen grundsätzlich auch die Gefahr eines unerwünschten Wissenstransfers ein. Bei Entlassungen bspw. besteht auch die Gefahr, dass persönliches Wissen unerwünscht weitergegeben wird. Auch die Kundengewinnung ist geprägt von akutem Wissenstransfer (Vorführung von Werbeunterlagen, Gespräche etc.). Auch bei der Zulassung oder Zertifizierung von Produkten, insbes. in Schwellenländern, könnte hier von der Prüfbehörde Wissen an andere über das Produkt weitergetragen werden.

2. Motive des MA unterscheiden sich von denen des Unternehmens: Vorsätzliche Weitergabe von internem Wissen an Wettbewerber oder Geheimdienste. Durch Illoyalität kann an jeder Stelle in jeder erdenklichen Form Wissen abfließen. Dies kann bspw. auch nach einer Provokation[11] des Wissensgebers an den Wissensempfänger geschehen, wenn sich dieser nicht mehr verpflichtet fühlt das empfangene Wissen im Interesse des Unternehmens zu verwenden. Zudem ist es schwierig in einem produktiven Arbeitsfeld zu überprüfen, welcher MA sich wie viel Wissen aneignet. Bzgl. des unreflektierten Weitergebens von Wissen kann es sein, dass der MA unter zu großem Zeitdruck steht um eine Wissensselektion vorzunehmen.

- Pull (Wissensempfänger geben den Impuls) → Spionageaktivitäten von innen heraus durch MA oder extern an den Schwachpunkten des Sicherheitssystems, hohe Marktmacht von Kunden „zwingt" zum Transfer - alleine durch das Fehlen von Zugangskontrollen zu sensiblen Bereichen fließt kein Wissen ab, es erleichtert die Handlung.

Deshalb ist es zunächst essentiell, dass das Unternehmen definiert, was genau wertvolles Wissen ist. Angeboten werden durch die Autoren verschiedene Ansatzpunkte zum Schutz des Wissens:

- Mitarbeiterverhalten in Situationen des Wissenstransfers verbessern: erfolgreiche Bindung an das Unternehmen (finanzielle Anreize, interessantes Jobprofil, soziale Faktoren), Sensibilisierung für o.g. Situationen, Aufklärung über zu schützendes Wissen
- Senkung des Nutzens von transferiertem Wissen – hauptsächlich für Technologien mit langer Einarbeitungszeit → stetige Weiterentwicklung eigener Technologien

Bewertung: Ist für Unternehmen der Investitionsgüterindustrie von besonderer Relevanz – die Vorgehensweise, wie verschiedene Formen des Wissens vor der Analyse zu klassifizieren sind, könnten hilfreich sein. Die Empfehlungen sind eher allgemein gehalten, ergeben im Gesamtkontext des Buches jedoch Sinn. Besonders interessant ist die detaillierte Darstellung der spezifischen Situationen und die Identifikation der push- und pull-Faktoren für einen Wissenstransfer.

**Achim Hecker, Roland Füss, Stephan Gundel (2008): „Charakteristik wirtschaftskrimineller Delikte". In: Zfo, 77 (3). S. 143 – 149.**

Gegenstand: Eine Online-Befragung interner Revisoren aus Deutschland, Österreich und der Schweiz, die auf den Antworten von 329 Unternehmen basiert. Die Befragung der Revisoren entstand durch die Kooperation mit dem deutschen Institut für interne Revision (DIIR), dem Institut für interne Revision Österreich (IIRÖ) und dem Schweizerischen Verband für Interne Revision (SVIR). Die Studie behandelt die Delikte Untreue/Betrug und Diebstahl (Massendelikte) sowie Korruption, Wettbewerbsdelikte und Geldwäsche (qualifizierte Delikte).

Ziele: Charakterisierung von verschiedenen Deliktstypen (Korruption, Betrug, Diebstahl, Wettbewerbsdelikte, Geldwäsche) . Durch die Charakterisierung soll eine verbesserte Prävention und Bekämpfung in den Unternehmen ermöglicht werden.

Forschungsfragen: Inwieweit sind Deutschlands Manager kriminell? Was charakterisiert die einzelnen Deliktstypen und die Täter, die diese Delikte begehen?

Ergebnisse:

- 35 Prozent der Befragten geben an, dass Untreue-und Betrugshandlungen am häufigsten registriert wurden, 34 Prozent nennen Diebstähle. Korruption wurde von zwölf Prozent genannt, Wettbewerbsdelikte von sieben und Geldwäsche von vier Prozent.

[11] Wie bspw. Abmahnung, Maßregelung durch den Vorgesetzten oder eine anderweitige Situation, die der Mitarbeiter als unfair empfindet.

- Besonders betroffen von Betrugs- oder Untreuedelikten sind Versicherungen (85 Prozent), Industrieunternehmen (81 Prozent) und Kredit- oder Finanzdienstleister (70 Prozent)
- Die hier befragten internen Revisoren haben im Wesentlichen drei Unternehmensbereiche identifiziert, die meistens von Wirtschaftskriminalität betroffen sind: Materialwirtschaft, Vertrieb und Einkauf. Die Autoren begründen dies mit den nur eingeschränkten Kontrollmöglichkeiten in diesen Bereichen und dem damit hohen Autonomiegrad des Täters. Wenig betroffen sind Bereiche wie Personalwesen oder Logistik.
- Anfällige Geschäftsprozesse sind laut der Studie: Beschaffungs- und Zahlungsverkehr sowie der Verkauf. Besonders Beschaffungstätigkeiten nehmen eine zentrale Rolle ein: 50 Prozent aller gemeldeten Korruptionsfälle und 32 Prozent der Diebstähle werden bei diesen Funktionen registriert. Bzgl. der Geldwäsche ist insbesondere der Zahlungsverkehr betroffen. Bzgl. Auftragstätigkeiten sind deutlich weniger Straftaten zu verzeichnen.
- Die Durchführung ist bis auf Diebstahlsdelikte meist systematisch geplant und häufig wurde sich konventioneller Mittel bedient um die Tat durchzuführen. Der Tatbegehungszeitraum erstreckt sich von fünf Jahren bei Wettbewerbsdelikten bis zu 13 Jahren bei Korruption
- Auffällig ist, dass die Massendelikte meist von männlichen Mitarbeitern ohne Führungsverantwortung zwischen 30 – 50 Jahren begangen wurden. Allerdings können die Täter auch Lieferanten oder Kunden sein. Die Altersspanne ist hierbei bei Tätern der Korruption um zehn Jahre größer als bei Geldwäsche oder Wettbewerbsdelikten. Täter der qualifizierten Delikte sind meist höher gebildet und sind länger (6-20 Jahre) Teil des Unternehmens. Der Brutto- sowie der immaterielle Schaden der durch diese Straftaten verursacht wird, fällt bei qualifizierten Delikten weitaus höher aus als bei Betrug oder Diebstahl.
- Motive für die Tatbegehung: bei nahezu allen Delikten spielen Habgier und ein aufwändiger Lebensstandard eine relevante Rolle. Finanzielle Engpässe motivieren Täter der qualifizierten Delikte, aber auch Täter der Geldwäsche. Suchtverhalten spielt bei Geldwäsche und Diebstahl eine Rolle – Geltungsbedürfnis ist bei den meisten der Massendelikte ein Faktor für die Tatbegehung. Die Gelegenheit ist bei allen Delikten bis auf Geldwäsche durch mangelnde interne Kontrolle entstanden. Die alleinige Bearbeitung von Sachverhalten hat bei drei der fünf Delikte eine Gelegenheit geboten – die Massendelikte wurden zudem durch die Zusammenarbeit mit Externen vorangetrieben. Wettbewerbsdelikte und Geldwäsche wurden durch die Anhäufung von zu viel Macht möglich. Gerechtfertigt wurden alle Delikte durch ein mangelndes Werte- und Unrechtsbewusstsein, Korruptions- und Diebstahlstätern kamen die unzureichenden Kontrollen einer Einladung gleich, Wettbewerbstäter streiten die finanziellen Konsequenzen für das Unternehmen ab und Geldwäsche -Tätern mangelt es an Loyalität
- Schlussfolgerungen der vorliegenden Studie: ausreichende Ressourcen für Prävention und Bekämpfung einplanen, risikoorientierte Prävention und Bekämpfung anhand der besonders gefährdeten Bereiche im Unternehmen, frühzeitige Reaktion auch auf schwache Hinweise, Mitarbeitern auf unteren Hierarchieebenen müssen die Tatgelegenheiten genommen werden, gleiches gilt für die Mitarbeiter des unteren und mittleren Managements.

Bewertung: Eine sehr aufschlussreiche Studie, die die Heterogenität der Wirtschaftskriminalität und ihrer Täter anerkennt und berücksichtigt. So können deliktsspezifische Profile erstellt werden, die den Unternehmen helfen, Gefahren und Risiken besser einschätzen zu können. Es stellt sich

allerdings die Frage, ob die Aussagen noch aktuell gültig sind oder ggf. spezifische Verschiebungen innerhalb und zwischen den Deliktstypen stattgefunden haben.[12]

**Julia Hugendubel (2016): „Tätertypologien in der Wirtschaftskriminologie".**

Gegenstand: Die Dissertation beschäftigt sich mit der Zusammenstellung und der Analyse verschiedener Typologien zu Wirtschaftsstraftätern mittels einer qualitativen Inhaltsanalyse. Hierbei wird zwischen empirischen und konzeptionellen Studien unterschieden.

Ziele: Impulsgebung für die Bekämpfung von Wirtschaftskriminalität in Unternehmen sowie Betrachtung des Phänomens der Bildung von Tätertypen unter dem Gesichtspunkt der sozialen Kontrolle.

Forschungsfragen: Inwiefern können Wirtschaftstätertypologien als Instrument sozialer Kontrolle fungieren? Welche Arten von Wirtschaftsstraftätertypologien gibt es und welcher Zweck wird mit der Tätertypenbestimmung verfolgt? Wie soll die mit der Tätertypenbildung verfolgte Zielsetzung erreicht werden und ist dies realisierbar? Werden möglicherweise andere, nicht intendierte Effekte mit der Tätertypenbestimmung erzielt und welche Konsequenzen sind ggf. damit verbunden? Wie sind diese Folgen aus rechtlicher, kriminalpolitischer und kriminologischer Perspektive zu bewerten? Welche Bedeutung haben Compliance-Maßnahmen für die Prävention von Wirtschaftskriminalität?

Ergebnisse:

| **Tätertypologien i. d. Wirtschaftskriminologie** | | | |
|---|---|---|---|
| **Konzeptionelle Studien** | | | |
| **Grundlage** | **Tätertyp** | **Motive/Merkmale** | **Besonderheiten** |
| Sutherland | white collar criminal | kein spezielles | nicht zwingend als eigener Typus zu sehen, eher ein Hinweis, dass Kriminalität nicht nur ein Phänomen der Unterschicht ist; konzentriert sich auf Unternehmen als Kollektiv, weniger auf den Mitarbeiter per se |
| Wheeler | risk seeker | Angst vor Statusverlust und finanziellem Verlust; Gier | |
| | revenge seeker | Unzufriedenheit über die Behandlung im Unternehmen | Rechtfertigung für die Straftat; teilw. auch ideologisch motiviert |
| | tax protesters | ideologischen Ursprungs | |
| Becker und Holzmann | klassischer Agent Täter | extrinsisch | typische Delikte: Diebstahl, Veruntreuung, Betrug, Korruption; Grundlage: prinzipal-Agent-theorie |
| | Guided Agent Täter | Kosten-Nutzen-Bilanz, ausschweifender Lebensstil, finanzielle Anreize | Vorkommen in „stark maskulin geprägten Kulturen" |
| | Steward Täter | intrinsisch, um Ziele des Unternehmens durchzusetzen, ist jedes Mittel recht, solidarisch, altruistisch; | hohe Identifikation mit dem Unternehmen |
| | Missguided Steward Täter | intrinsisch, durch Enttäuschung o.ä. des Unternehmens folgt die Abwendung zur Verfolgung eigener Interessen | |

[12] Anmerkung: Zu weiteren Ausführungen bzgl. Awareness, Fraud Triangle und Red Flags[12]: Schaaf, Christian: „Mitarbeiterkriminalität wirksam bekämpfen". In: Management und Wissen 2013. Allerdings bildet dieser Artikel die Vielfältigkeit der Innentäter nur bedingt ab.

| Empirische Studien[13] | | | |
|---|---|---|---|
| **Grundlage** | **Tätertyp** | **Motive/Merkmale** | **Besonderheiten** |
| Collins und Schmidt | | Täter neigen zu Unverantwortlichkeit, Unzuverlässigkeit und Missachtung von Regeln und Normen, niedrige Sozialisation | Unterschiede zwischen Wirtschaftskriminellen und solchen ohne Strafen in vergleichbaren Positionen sind feststellbar |
| | risk takers | unethisch, manipulativ | |
| Blickle et al. | | überwiegend von Männern begangen, hohe verhaltensbezogene Selbstkontrolle und ein häufiges Vorkommen von hedonistischen Persönlichkeiten sowie ausgeprägte Gewissenhaftigkeit | Erweiterung der Studie von Collins und Schmidt; Hypothesen: Je ausgeprägter die hedonistischen Züge einer Person sind, desto narzisstischer ist eine Person veranlagt (bestätigt); je geringer die verhaltensbedingte Selbstkontrolle ausgeprägt ist, desto höher ist die Wahrscheinlichkeit für diese Person, eine Wirtschaftsstraftat zu begehen (bestätigt). Keine signifikante Korrelation findet sich zwischen Gewissenhaftigkeit und der Begehung von Wirtschaftsstraftaten. |
| Bannenberg | 1. Tätertyp | undefinierbar, jedermann | Präventionsmaßnahmen: Sensibilisierung, Formulierung deutlicher Verhaltensregeln/ Unternehmensleitlinien, ethische Grundsätze, Kontrolle, Sanktion bei Entdeckung. |
| | 2. Tätertyp | längere Verbindung zur Tatumgebung | „Betrügerpersönlichkeiten“ (Lügen, Fälschungen, Täuschen, verfügen über geringe & vortäuschen einer hohen Qualifikation, Hang zur Selbstdarstellung, Manipulation, kriminelle Energie, chaotischer Lebensstil, extreme Rechtfertigungsstrategie, nach Verurteilung keine Einsicht o.ä.); „typische Täter der strukturellen Korruption“ (auffällig unauffällig, meist männlich, deutsch, über 40 Jahre, meist keine Vorstrafen, geordneter Lebensstil, gute Qualifikation [oft zweiter Bildungsweg) und damit einhergehende Machtposition, Anspruch an hohen *Lebensstandard und gesellschaftlichen Status, ehrgeizig, engagiert,* extreme Rechtfertigungsstrategie] eingeteilt. |
| | 3. Tätertyp | Wirtschaftsdelikte und OK | „Betrügerpersönlichkeiten“ (Lügen, Fälschungen, Täuschen, geringe Qualifikation und vortäuschen einer hohen, Hang zur Selbstdarstellung, Manipulation, kriminelle Energie, chaotischer Lebensstil, extreme Rechtfertigungsstrategie, nach Verurteilung keine Einsicht o.ä.); „typische Täter der strukturellen Korruption“ (auffällig unauffällig, meist männlich, deutsch, über 40 Jahre, meist keine Vorstrafen, geordneter Lebensstil, gute Qualifikation [oft zweiter Bildungsweg) und damit einhergehende Machtposition, Anspruch an hohen Lebensstandard und gesellschaftlichen Status, ehrgeizig, engagiert, extreme Rechtfertigungsstrategie] eingeteilt. |

[13] Die Studien von KPMG und PwC werden in diesem Zusammenhang nicht näher aufgelistet, da eine aktuelle PwC Studie bereits Teil dieses Berichts ist und die KPMG Studie auf globale Täterprofile ausgelegt ist.

| | | | |
|---|---|---|---|
| Schneider und Rölfs Partner | | | Straftäter meist männlich, deutsch, durchschnittlich 46 Jahre alt, 24 % sind vorbestraft, überdurchschnittlich hohes Bildungsniveau (Ebene Top-Management) |
| | 1. Gelegenheitssucher | | a. Der mit dem Belastungssyndrom; b. Der Krisentäter |
| | 2. Gelegenheitsergreifer | | a. Der Abhängige; b. Der Krisentäter |
| | 3. Der Unauffällige | | |
| | | | Prävention: für Gelegenheitsergreifer wird ein Sensibilisierungsprogramm mit Schulungen empfohlen, Unternehmensrichtlinien, „Tone from the top“. Gelegenheitssuchern soll präventiv durch die regelmäßige bspw. bei einschneidenden unternehmerischen Ereignissen wie Beförderung oder Einstellung Forderung nach einem polizeilichen Führungszeugnis Einhalt geboten werden. |
| Cleff, Naderer, Volkert | 1. Der egozentrische Visionär | selbstbewusst, ehrgeizig, zielstrebig, nicht emotional, überlegtes und berechnendes Handeln, Ziele sind materieller Natur, Finanzierung des teuren Lebensstils | |
| | 2. Der frustrierte Visionär | erfolgsorientiert, „Macher“, hohe Intelligenz, scheitern an seinen eigenen hohen Ansprüchen, ideell und sozial motiviert, subjektiv unzureichende Unterstützung bei der Realisierung seiner Visionen, Realitätsverlust, legt Wert auf Statussymbole | |
| | 3. Der narzisstische Visionär | übersteigertes Selbstbild, nicht kritikfähig, risikofreudig | |
| | 4. Der Abhängige | stark emotional, abhängig von sozialen Beziehungen, Verlustängste, fremdbestimmtes Handeln, keine eigenen Ziele, Geld dient zur Aufrechterhaltung der sozialen Beziehungen | |
| | 5. Der Naive | niedrige Bildung, Ziele/Werte von außen vorgegeben, will pflichtbewusst handeln, scheu, verschlossen, leicht überfordert, leichtgläubig | |

- Tätertypologien sollen mehrheitlich zur privaten sozialen Kontrolle eingesetzt werden, anwendungsbezogen jedoch sowohl der Betriebs- als auch der Unternehmenskriminalität zuzuordnen
- Können nur über Persönlichkeitstests erkannt werden, Tätertypologie fungiert als Baustein von Compliance-Maßnahmen, wird vorrangig in der Privatwirtschaft eingesetzt

- Empirische Studien haben teilweise wenig Aussagekraft (Unzulänglichkeiten in der Methodik (Repräsentativität, Kontrolle der Antworten, nur wenige Studien überprüfen die Ergebnisse anhand einer Vergleichsgruppe); angestrebt werden sollte eine realtypische, quantitative Bestimmung von Tätertypen
- Tätertypenbestimmung ist für eine Unterscheidung zwischen Wirtschaftsstraftätern und Nicht-Wirtschaftsstraftätern nicht geeignet → zu große Möglichkeit von „false positives"

Bewertung: Eine eingehende, differenzierte Betrachtung der Tätertypologie von Wirtschaftskriminalität, die deutlich die Schwierigkeiten dieser Thematik aufzeigt und begründet. Zudem wird hier deutlich, wie vielseitig und heterogen Wirtschaftskriminalität und ihre Täter sind – eine Verallgemeinerung ist, auch bei teilweise wiederkehrenden Profilen, nicht möglich.

**Simon Kirsch (2014): „Informationsschutz im Unternehmen – Prävention von Wissensabfluss und die Erkennung von Innentätern anhand derer Verhaltensmerkmale".**

Gegenstand: Das Buch von Simon Kirsch beschreibt die Problematik des immer weiter ansteigenden Wettbewerbsdrucks zwischen Unternehmen, sowohl national als auch international. Aufgrund dessen beschreibt Kirsch verschiedene Formen der Informationsgewinnung, bspw. durch Nachrichtendienste oder durch Industriespionage und Konkurrenzausspähung. Ein weiterer zentraler Weg, um an unternehmensinterne Informationen zu gelangen führt über die Mitarbeiter, auf welchen in dieser Arbeit ein besonderer Fokus liegt. Zudem wird die zentrale Bedeutung von Informationen am heutigen Wirtschaftsmarkt deutlich herausgestellt – wertige Informationen sind der Grundstein eines Wettbewerbsfähigen Unternehmens und sollten daher gut geschützt werden. Die Ausführungen von Kirsch basieren auf einer Darstellung von Sekundärliteratur und eigenen Überlegungen.

Ziele: Ziel ist es zu analysieren, wo sich Schwachstellen bzgl. des Informationsschutzes befinden und folglich Vorschläge für deren Verbesserung herauszuarbeiten. Zudem soll eine eingehende Betrachtung der Innentäterproblematik erfolgen. Ein grundlegender Fokus liegt darauf, das Phänomen der Wirtschafts- und Industriespionage zu untersuchen und zu analysieren – hierbei sollen Erscheinungsformen, Ursachen und schließlich mögliche Präventionsmaßnahmen erläutert werden.

Forschungsfragen: Wo können innerhalb des Informationsschutzes Schwachstellen identifiziert werden? Welche präventiven Maßnahmen lassen sich für die Wirtschaft darstellen und welche Wirkung würden diese erzielen? Sind Innentäter aufgrund von Verhaltensänderungen erkennbar?

Ergebnisse:

- Als erstes wird ein Beispiel beschrieben, in dem zwei Mitarbeiter in einem sozialen Netzwerk von einer Person angesprochen wurden gegen eine bestimmte Geldsumme Informationen des Unternehmens preiszugeben. Zuvor hatte er sich das Vertrauen der Mitarbeiter unter dem Vorwand der Eröffnung neuer beruflicher Möglichkeiten erschlichen (Social Engineering). Kritisiert wird hier vom Autor, die häufige Betreuung/Beauftragung des Informationsschutzes der IT-Abteilungen. Eine eingehende Einbindung aller beteiligten Akteure sei jedoch vonnöten (hierzu zählen: Revision und Compliance, Unternehmenssicherheit, Datenschutz, Fachbereich IT, Informationsmanagement).
  - ➔ Ernennung eines Gesamtverantwortlichen für den Informationsschutz (CISO), wichtig hierbei: abteilungsunabhängige Positionierung, ABER Beteiligung und Nutzung der verschiedenen involvierten Abteilungen im Gremium
  - ➔ Interner Arbeitskreis unter Leitung des CISO für den Informationsschutz
  - ➔ Etablierung von internen Handlungsgrundlagen
  - ➔ Informationsschutz ist Chefsache

- Bzgl. der Phänomenologie von Wirtschafts- und Industriespionage Tätern stellt Kirsch dar, dass 68 Prozent der Täter Einzeltäter sind und ohne zusätzliche unternehmensinterne Personen agieren. Wenn man die Verteilung der Innentäter betrachtet, stellt man fest, dass diese in 89 Prozent der Fälle für den Informationsabfluss verantwortlich sind. 20 Prozent sind nur indirekt als Innentäter zu bezeichnen. Die Zahl der Wiederholungstäter ist in diesem Feld mit 91 Prozent sehr hoch – bei 67 Prozent der Täter dauerte der Zeitraum wirtschaftskrimineller Handlungen bis zu fünf Jahre.
- Laut Autor sind potenziell alle Bereiche innerhalb einer Organisation gefährdet – besonders sei jedoch der Mittelstand in Gefahr.
- Täterprofile sind grundsätzlich aufgrund der Bandbreite der Ursachen, Motive und möglichen Ziele schwer zu generalisieren. Auch Faktoren wie bewusste oder unbewusste Beteiligung am Wissensabfluss müssen in Betracht gezogen werden. Durch ihre oftmals lange Betriebszugehörigkeit und Führungsebene der Innentäter gehören sie zu der Tätergruppe mit dem höchsten Gefährdungspotenzial innerhalb des Phänomens der Wirtschaftskriminalität. Berufliche Eigenschaften dieser Tätergruppe sind u.a.: Durchsetzungswillen, Risikobereitschaft, Aufstiegsorientierung.
- Einige Unternehmen unterschätzen die Gefahr, die von Mitarbeitern ausgeht aufgrund der Geheimhaltungsverpflichtung im Arbeitsvertrag und der grundlegenden Annahme der Loyalität
- Potenzieller Kreis der Innentäter erweitert sich durch externes Personal bspw. im Rahmen einer Inhouse-Tätigkeit, im Rahmen von Outsourcing, Nachfrage nach Freiberuflern und Beratungsfirmen. Der Abfluss kann bspw. auf Kongressen, messen oder Tagungen von statten gehen. Aber auch soziale Netzwerke bieten genügend Möglichkeiten den Mitarbeiter als direkte Informationsquelle auszunutzen (mittels Social Engineering).
  - ➔ Unterschieden werden muss zwischen technischer[14] und nicht-technischer[15] sowie bewusster[16] und unbewusster Abschöpfung von Informationen durch Mitarbeiter.
  - ➔ Die kleinste Tätergruppe besteht aus Mitarbeitern, welche ohne jegliches Druckmittel bewusst den Informationsabfluss betreiben. Hier besteht keine Identifizierung mit den Unternehmenszielen und –werten (Stichwort „innere Kündigung“). Oft werden die Taten über die Vernachlässigung des Arbeitgebers gerechtfertigt. Bei einer inneren Kündigung, so Kirsch, gebe es deutliche Anzeichen der Veränderung in Verhalten und Psyche[17]. Für die Demotivation eines Mitarbeiters gibt es zahlreiche Gründe: Über-oder Unterforderung, Mobbing, negatives Betriebsklima, um nur einige zu nennen.
- Kirsch stellt dar, dass Befragungen ergeben, dass zu wenig im Bereich Awareness getan wird ➔ viele Mitarbeiter können klassifizierte und vertrauliche Dokumente nicht einordnen. Über das Betriebsklima ließe sich auf die vorhandene Loyalität der Mitarbeiter schließen, deshalb sind regelmäßige Zufriedenheitsbefragungen der Mitarbeiter sinnvoll.
- Präventive Maßnahmen gegen Informationsabfluss:
  - ➔ Information über behördliche Unterstützungsmaßnahmen, Veranlassung von Auditierungen, Meldung von Vorfällen an die zuständigen Behörden
  - ➔ Integration von Leitlinien/Handlungsrichtlinien in die Unternehmenspolitik

[14] Bspw. die Installation einer Schadsoftware auf dem Computer
[15] Bspw. Social Engineering
[16] Bspw. durch eine Erpressung mittels Honey Trapping hervorgerufen. Nicht ablehnbare Geldangebote können hierunter auch gefasst werden.
[17] Erledigung des Nötigsten, soziale Isolierung von den Kollegen, Desinteresse ggü. Unternehmensthemen, überdurchschnittliche Anzahl an Fehltagen.

- ➔ Durchführung von Awarenessprogrammen, Information für die Mitarbeiter, Bereitstellung von Anlaufmöglichkeiten (Ombudsleute), bei ausscheidenden Mitarbeitern möglichst schnell den Nachfolger einarbeiten, den Ausscheidenden über sein Stillverschweigen informieren, frühzeitiger Ausschluss aus Gremien
- ➔ Analyse externer Gefahren durch bspw. Lieferanten

Fazit: Das Buch bezieht sich grundlegend auf das Phänomen der Wirtschaftsspionage und erläutert dieses auch dezidiert. Gut aufgebaut ist die Arbeit von Kirsch, da sich nach jedem Einzelkapitel eine Art Übersicht zu Handlungsempfehlungen für den spezifischen Bereich findet – das erleichtert den Überblick und lässt die Empfehlungen nicht allgemein wirken – führt allerdings häufiger zu Dopplungen in den Empfehlungen. Für einen schnellen Einblick in die Problematik der Innentäterschaft ist das Buch zu empfehlen.

## 3. Fazit

Die Recherche hat gezeigt, dass das Thema „Innentäter" im wissenschaftlichen Diskurs aktuell eher wenig zur Sprache kommt[18] – die Umfragen der Unternehmensberatungen bieten hier umfassendere Informationen an. Die grundlegende Schwierigkeit bei der Darstellung des Forschungsstandes ist, dass die Informationen zu Innentätern nicht „gebündelt" in speziellen Studien vorliegen, sondern mühsam in den vielfältigen Publikationen zur Wirtschaftskriminalität zusammengesucht werden müssen. Ein spezifisches Profil des „einen" Innentäters gibt es nicht, weil dieses deliktsspezifisch betrachtet werden muss. Aus den analysierten Berichten lassen sich folgende wesentliche Aspekte zusammenfassen:

Welche Situationen können kritisch für einen Informationsabfluss durch Mitarbeiter sein?

- Outsourcing-Situationen
- Generelle Zusammenarbeit mit Lieferanten
- Kundengewinnung
- Entlassung von Mitarbeitern
- Zulassung/Zertifizierung von Produkten (insbes. in Schwellenländern)
- Hohe Marktmacht von Kunden
- Alleinbearbeitung von Sachverhalten durch den Mitarbeiter, zu große Machtfülle

Wer sind die Innentäter?

- Meist männlich und eine respektierte, freundliche Person
- Überwiegend zwischen 30 und 50 bzw. 60 Jahren alt
- Meist mittleres bis Top-Management, bei bestimmten Delikten wie Diebstahl oder Untreue/Betrug auch ohne Führungsverantwortung
- Meistens seit sechs bis 20 Jahren im Unternehmen
- Meist höher gebildet (bei Korruption, Geldwäsche und Wettbewerbsdelikten), je nach Delikt auch eine schlechtere Bildung (s. Betrug, Untreue/Diebstahl)

Wieso begehen sie die Straftaten?

- Persönlicher oder finanzieller Profit,
- Aufwändiger Lebensstandard,
- Engagement/Geltungsbedürfnis,
- Niedrige Hemmschwelle und Mangel an Unrechtsbewusstsein,
- Ehrgeiz/Verbesserung der sozialen Stellung/Habgier,
- Frustration/Wut,

[18] Jedoch gibt es vor dem hier angesetzten Zeitraum mehr Artikel, die sich mit Innentäterschaft befassen (von ca. 2002 bis 2011).

- Günstige Gelegenheit durch unzureichende interne Kontrollen,
- Abwerbung oder Beeinflussung durch Konkurrenz / anderweitige Abhängigkeit,
- Gründung eines Konkurrenzunternehmens,
- Falscheinschätzung der Situation.

Welche Maßnahmen kann das Unternehmen ergreifen?

- Gute Arbeitsbedingungen schaffen und den Mitarbeiter an das Unternehmen binden (finanzielle Anreize, interessanter Job),
- Ausbildung und Erweiterung von Soft Skills,
- Eine Vertrauensbasis schaffen,
- Sensibilisierung der Mitarbeiter für kritische Situationen, in denen potenziell internes Wissen durch Dritte abgeschöpft werden könnte (Etablierung einer Information Security Policy) wie bspw. die Videos zu CEO Fraud, Social Engineering oder das geplante Video zu Innentätern von EXPLOQII[19],
- Bestimmung von Personenfaktoren (s. bspw. Hannoversche Korruptionsskala),
- Pre-Employment-Checks, Abgleich mit Sanktionslisten,
- Definition und Identifikation von Situationen, in denen ein ungewollter Wissenstransfer stattfinden kann und eine vorherige Einigkeit innerhalb der Unternehmensführung über die verschiedenen Arten von Informationen im Unternehmen und deren Wert,
- Klare Artikulierung von Unternehmensrichtlinien und ethischen Werten,
- Eingehende Prüfung der gesamten Lieferkette und eventuelle Forderungen an den Lieferanten (bspw. i. Bez. auf ein Compliance-Management-System),
- Vier-/oder Mehr-Augen-Prinzip,
- Ein über die Grenzen des Unternehmens gehendes Sicherheitsmanagement, das Maßnahmen zur Prozesssicherung und Minimierung des Risikos entwickelt und auch durchführt (Franke, Lommatzsch 2015: 24[20]). Die sog. Supply Chain Security überwacht die Prozesse von der Entwicklung bis zur Ablieferung des Produktes beim Endkunden. Gefahren in der Lieferkette sind u.a. bei Produkt-und Markenpiraterie, aber auch bei Frachtdiebstählen zu verorten,
- Eventuelle Systemschwachstellen und IT-Komponenten überprüfen und verbessern (Zugangs- und Zugriffkontrollen, auffälliges Verhalten einzelner Mitarbeiter beobachten), Durchführung einer Risikoanalyse.

Anhand der Forschungsbeiträge wird ersichtlich, dass Innentäter einen deutlichen Anteil der Straftaten in Unternehmen ausüben und deshalb nicht unterschätzt werden dürfen. Die vielfältigen Möglichkeiten für einen Mitarbeiter zum Täter gegen das eigene Unternehmen zu werden machen eine Kontrolle schwierig. Ein erster Schritt ist jedoch die Stärkung der Awareness und Sensibilisierung der Mitarbeiterschaft zur Meldung von verdächtigen Aktionen. Durch die verbreitete Umsetzung von Systemkontrollen und durch die Beschränkung des Zugriffs auf spezifisches Wissen ist ein weiterer Schritt in Richtung Know-How-Schutz getan. Um einen umfassenden Blick in das Themenfeld „Innentäter“ zu gewinnen, wäre es, aufgrund der Heterogenität der Straftaten die durch Innentäter begangen werden, notwendig deliktsspezifisch vorzugehen. Die Bandbreite der Straftaten erstreckt sich von unerlaubtem Zutritt zu Räumlichkeiten, über Spionage und Datendiebstahl bis zur Korruption und Geldwäsche. Die Motivlagen sind sehr unterschiedlich und kaum vergleichbar. So kann man nur deliktsspezifische Aussagen über Täterprofile treffen - die Profile können im Hinblick auf Alter, berufliche Erfahrung und Stellung im Unternehmen, Motiven, Persönlichkeitsmerkmalen sowie bzgl. der eventuellen Vorstrafen stark schwanken (Hecker, Füss, Gundel 2008: 144 -146). Eben

[19] Mehr Informationen zu den Videos unter: https://cloud.exploqii.com/de/products.
[20] Franke, Ulrich und Jutta Lommatzsch: „Haftungsrisiken für Unternehmensleitungen“ in: WIK (5), 2015. Seiten: 24-25.

diese Vielfalt der Innentäterschaft macht eine jeweilige spezifische Analyse und Erarbeitung fallbezogener Handlungsempfehlungen notwendig. Bei der Recherche fällt auf, dass es Veröffentlichungen und Studien zu Motiven und Tätertypologien in der Wirtschaftskriminalität allgemein gibt, diese beinhalten u.a. auch Ausführungen, die direkt und indirekt Innentäterschaft ansprechen[21]. Insgesamt lässt sich festhalten, dass Unternehmen sich nicht durch gewisse technische Vorkehrungen in einer absoluten Sicherheit wiegen dürfen, wie Linssen/Litzcke/Schön beschreiben (2017: 90, 91) – der Faktor Mensch ist flexibel, präsent und kann auch technische Barrieren umgehen. Eine eingehende wissenschaftliche Betrachtung von Innentäterschaft wäre an dieser Stelle hilfreich.

[21] Siehe hierzu u.a.: Bongartz, Bärbel: „Strukturelle Bedingungen wirtschaftskrimineller Handlungen". Forum Verlag Godesberg GmbH: Mönchengladbach, 2016. S. 42 - 45. Bei den zusammengefassten Tätertypologien wird unterschieden zwischen dem „Gelegenheitsgreifer", der aufgrund unzureichender Sicherheitsvorkehrungen und seiner Position handelt und dem „Gelegenheitssucher", der meist vorbestraft ist und aktiv nach einer Gelegenheit zur Tatbegehung sucht. Außerdem wird ein Tätertyp identifiziert, der ein Belastungssyndrom aufweist, welches sich aus einer Ansammlung bestimmter persönlicher Schicksalsschläge formiert und ab einem Wendepunkt im Leben/in der Biografie straffällig wird. Zudem gebe es den „Krisentäter", der bspw., um seinen Lebensstandard aufrechtzuerhalten, Straftaten begeht. Meist sei diese Art des Täters ein „Gelegenheitsgreifer". Zusätzlich gebe es den „abhängigen" (von bspw. anderen Personen) Täter, der aufgrund von externem Druck handelt sowie den Typ des „unauffälligen" Täters, der nicht näher ausgeführt wird. Im Zuge von Täterprofilen werden verschiedene Motivationen der Täter aufgeführt (egozentrischer, frustrierter, naiver, abhängiger und narzisstischer Visionär).

## Literaturverzeichnis


Bitkom (2015): „Spionage, Sabotage und Datendiebstahl - Wirtschaftsschutz im digitalen Zeitalter“. URL: https://www.bitkom.org/noindex/Publikationen/2015/Studien/Studienbericht-Wirtschaftsschutz/150709-Studienbericht-Wirtschaftsschutz.pdf Stand: 02.08.2017).

Bitkom und BfV (2017): „Wirtschaftsschutz in der digitalen Welt“. URL: https://www.bitkom.org/Presse/Anhaenge-an-PIs/2017/07-Juli/Bitkom-Charts-Wirtschaftsschutz-in-der-digitalen-Welt-21-07-2017.pdf (Stand: 30.07.2017).

Bongartz, Bärbel (2016): „Strukturelle Bedingungen wirtschaftskrimineller Handlungen“. S. 42 ff.

Bundesministerium für Verfassungsschutz (BfV), ASW Bundesverband (2015): „9. BfV/ASW-Sicherheitstagung“. URL: https://www.verfassungsschutz.de/de/arbeitsfelder/af-wirtschaftsschutz/sicherheitstagung/tagungsband-2015-09-sicherheitstagung-2015 (Stand: 30.07.2017).

Dubs, Stefan (2014): „Whistleblowing zur Erkennung schwerer Kriminalität?: Einsatz internetbasierter Hinweisgebersysteme zwecks Gewinnung von Ermittlungsansätzen“ .

Ernst &Young (April 2016): „Global Fraud Survey – Ergebnisse für Deutschland“. URL: http://www.ey.com/Publication/vwLUAssets/EY-global-fraud-durvey-ergebnisse-fuer-deutschland/$FILE/EY-global-fraud-durvey-ergebnisse-fuer-deutschland.pdf (Stand: 29.07.2017).

Ernst & Young (2017): „Human Instinct, Machine Logic – which do you trust most in the fight against fraud and corruption?“. Europe, Middle East, India and Africa Fraud Survey. URL: http://www.ey.com/Publication/vwLUAssets/ey-human-instinct-machine-logic/$FILE/ey-human-instinct-machine-logic.pdf (Stand: 29.07.2017).

Franke, Ulrich und Jutta Lommatzsch (2015): „Haftungsrisiken für Unternehmensleitungen“. In: *WIK* (5). Seiten: 24-25.

Hecker, Achim, Roland Füss, Stephan Gundel (2008): „Charakteristik wirtschaftskrimineller Delikte“. In: *Zfo*, 77 (3). S. 143 – 149.

Hugendubel, Julia (2016): „Tätertypologien in der Wirtschaftskriminologie“. Frankfurt am Main; Bern; Bruxelles ; New York ; Oxford ; Warszawa ; Wien.

Kirsch, Simon (2014): „Informationsschutz im Unternehmen - Prävention von Wissensabfluss und die Erkennung von Innentätern anhand derer Verhaltensmerkmale“. Norderstedt: .

Kölbel, Ralf und Nico Herold (2015): „Wirtschaftskontrolle durch Whistleblowing? Empirische Befunde zu Entscheidungsprozessen von Hinweisgebern“.

KPMG (2017): „Neues Denken, neues Handeln“ Studienteil B: Cyber. URL: https://assets.kpmg.com/content/dam/kpmg/ch/pdf/neues-denken-neues-handeln-cyber-de.pdf (Stand: 02.08.2017).

Lindemann, Udo et al. (2017): „Know-How-Schutz im Wettbewerb – Gegen Produktpiraterie und unerwünschten Wissenstransfer“. Berlin/Heidelberg.

Linssen, Ruth, Sven Litzcke, Felix Schön (2017): „Nicht nur die Aufgabe birgt ein potenzielles Korruptionsrisiko, sondern auch der Mensch, der sie ausführt: Möglichkeiten der Messung personenbedingter Risiken zur Optimierung der Korruptionsprävention“. In: *CCZ*, 89.

Pricewaterhouse Coopers (PwC) (2016): „Wirtschaftskriminalität in der analogen und digitalen Wirtschaft 2016“. URL: https://www.pwc.de/de/risiko-management/assets/studie-wirtschaftskriminalitaet-2016.pdf (Stand: 15.07.2017).

Schaaf, Christian (2013): „Mitarbeiterkriminalität wirksam bekämpfen“. In: Management und Wissen.

Sowa, Aleksandra (2017): „Compliance-Schicht - Die Check-Phase des Managements der Informationssicherheit“. In: *Management der Informationssicherheit – Kontrolle und Optimierung*. Bonn.

**Anlagen**

Anl.1: „Auflistung der Versicherungsdienstleistungen bei einem Cyberangriff“. KPMG 2017. S.23.