Bundeskriminalamt

KRIMINALISTISCHES INSTITUT

Aktuelles aus der kriminalistisch-kriminologischen Forschung

MONITORINGBERICHT

Innentäter in Unternehmen 2

Aktuelle inländische Forschungsbeiträge, wesentliche Ergebnisse und Handlungsempfehlungen

Referat IZ 34
Heike Bruhn
Julia Weber

2020
2

Vorbemerkung

Das Kriminalistische Institut ist die kriminalistisch-kriminologische Forschungseinrichtung des Bundeskriminalamtes. Wissenschaftlerinnen und Wissenschaftler arbeiten gemeinsam mit Kriminalbeamtinnen und Kriminalbeamten daran, das Wissen über Ausmaß, Entstehungsgründe und Tatbegehungsformen von Kriminalität zu vertiefen.

Das Format „Aktuelles aus der kriminalistisch-kriminologischen Forschung“ (KKF-Aktuell) dient dazu, die Arbeitsergebnisse des Kriminalistischen Instituts zeitnah und bedarfsträgerorientiert für die polizeiliche Praxis nutzbar zu machen. Die Inhalte sollen dazu beitragen, die Erkenntnisbasis für die Entwicklung und Fortschreibung kriminalstrategischer und kriminalpräventiver Konzepte und Maßnahmen zu verbreitern und empirisch zu untermauern.

Forschungsberichte geben die Ergebnisse und polizeifachliche Relevanz eigener Studien des Kriminalistischen Instituts wieder. Monitoringberichte hingegen enthalten die wesentlichen Ergebnisse externer Studien zu einem polizeilich relevanten Themenfeld und bewerten deren polizeifachliche Relevanz.

Inhaltsverzeichnis

„If you think technology can solve your security problems, than you don´t understand the problems and you don´t understand the technology.“
(Bruce Schneier)

...denn spätestens beim Thema Innentäter stoßen technische Lösungen oftmals an ihre Grenzen.

Wesentliche Ergebnisse und Handlungsempfehlungen

- Innentäterschaft ist kein fiktives Phänomen und kann in jedem Unternehmen vorkommen. Seit 2016 bleibt die Einschätzung der Unternehmen im Rahmen der Bitkom-Studien mit jeweils über 60% konstant, dass Innentäter (insbesondere ehemalige Mitarbeiter) die größte Tätergruppe ausmachen. Einschlägige Dunkelfeldstudien und Befragungen zeichnen ein beunruhigendes bis alarmierendes Bild und gehen von einem sehr großen, wachsenden Dunkelfeld aus. Die generelle unternehmerische Beschäftigung mit der Thematik ist daher geboten.
- Laut Bitkom-Studie 2018 steht insbesondere der Mittelstand im Fokus der Angreifer, wenn es um Spionage, Sabotage und Datendiebstahl geht. Das Spezialwissen in KMU sowie deren Datenzugänge zu großen Konzernen sind besonders schutzwürdig.
- Tätertypus und Tatmotive können sehr unterschiedlich sein. Eine Betrachtung des Einzelfalles ist unerlässlich.
- Zusätzlich zu personalen Risikofaktoren oder der Persönlichkeitsstruktur können auch Tatgelegenheitsstrukturen das Täterverhalten beeinflussen. Unternehmen haben diesbezüglich erheblichen Einfluss und können präventiv tätig werden, z.B. durch
    - o das Etablieren von Präventionsmaßnahmen, Sicherheitsprozessen und Detektionsmöglichkeiten (Kontrollen);
    - o Schulungsmaßnahmen zum Thema sowie
    - o ausreichender Schulung am Produkt, so dass sicherheitsrelevantem Fehlverhalten durch Unkenntnis vorgebeugt wird;
    - o transparente Arbeitsprozesse, die Fehleinschätzungen von Situationen vorbeugen;
    - o Verbot des Einsatzes privater Geräte im geschäftlichen Kontext u.v.m..
- Das Artikulieren von Verhaltensregeln und Installieren von Präventionsmaßnahmen (z.B. feste Prozesse zur Einstellung neuer Mitarbeiter und zum Ausscheiden von Mitarbeitern sowie ein geregelter Umgang mit Informationsweitergaben an Dritte) signalisieren kein Misstrauen, sondern bieten Mitarbeitern Transparenz, Klarheit und Handlungssicherheit.
- Entfremdung des Mitarbeiters vom Unternehmen kann Innentäterschaft begünstigen. Gelebte Kommunikation im Sinne einer kontinuierlichen Informationskultur und konstruktiven Fehlerkultur sowie ein faires Führungsverhalten sind dagegen hilfreiche Mittel.
- Das Erkennen persönlicher Krisen bei Mitarbeitern und ihre Unterstützung in Notlagen,

Wesentliche Ergebnisse und Handlungsempfehlungen

z.B. durch das Angebot institutionalisierter Ansprechpartner für die Mitarbeiterunterstützung (innerbetriebliche oder externe Sozialberatung), kann etwaiges situationsbedingtes Fehlverhalten vorbeugen.

- Der ausscheidende/ ehemalige Mitarbeiter gewinnt zunehmend als Innentäter an Bedeutung (Mitnahme von Kundendaten, Projektinformationen, Vertragsunterlagen etc.). Etablieren Sie ein Security-Exit-Management.
- Mitarbeiter sind wertvolle Hinweisgeber, da sie Expertise über die konkreten praktischen Arbeitsabläufe besitzen und vorhandene Schwachstellen häufig als erste erkennen (siehe[1]) Hören Sie ihren Mitarbeitern zu, wenn es um Sicherheit geht und binden Sie sie aktiv in Konzepte ein.
- Mitarbeiter können Sicherheitsgarant oder Sicherheitsrisiko für ein Unternehmen sein. Neben der fachlichen Rolle, die sie im Unternehmen ausfüllen, sind sie immer auch Teil der Unternehmenssicherheit. Für diesen Gedankenraum sollte Awareness geweckt werden. Eine Aufnahme der Thematik Wirtschaftsschutz in einschlägigen Studiengängen mit dem Ziel, das Unternehmenssicherheitsbewusstsein und insbesondere das Informationssicherheitsbewusstsein bereits bei Studenten und Berufsanfängern zu erhöhen, ist daher wünschenswert.

Weiterer Forschungsbedarf:

- Die Datenlage ist defizitär. Ein belegbarer realistischer Überblick über den tatsächlichen Umfang und die tatsächliche Bedrohungslage lässt sich auf Grundlage der verfügbaren amtlichen Statistiken nicht gewinnen. Dazu bedürfte es weiterer Forschung (Hellfeldanalysen und Dunkelfeldforschung) sowie eines erhöhten Anzeigeverhaltens z.B. durch eine Steigerung der Anzeigebereitschaft aufgrund Awareness-Bildung und dem Ausbau der vertrauensvollen Zusammenarbeit im Rahmen des Wirtschaftsschutzes.
- Eine Vielzahl der angebotenen Präventionsmaßnahmen ist nicht durch entsprechende Evaluationsforschung belegt. Diesbezügliche Forschung wäre sinnvoll, damit Unternehmen ihr Geld und ihre Energie in Maßnahmen investieren können, die nachgewiesenermaßen eine Präventionswirkung und Awareness-Steigerung bewirken.

[1] „Häufig sind es aber auch Mitarbeiter, die auf der anderen Seite dafür sorgen, dass kriminelle Handlungen aufgedeckt werden. Sechs von zehn betroffenen Unternehmen (62 Prozent) sind so erstmals auf Angriffe aufmerksam geworden. Mehr als die Hälfte (54 Prozent) erhielt Hinweise auf Angriffe durch eigene Sicherheitssysteme, bei fast drei von zehn (28 Prozent) war es hingegen reiner Zufall.“ S. Pressinformation des Bitkom: „Angriffsziel deutsche Wirtschaft: mehr als 100 Milliarden Euro Schaden pro Jahr“, URL: **https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-100-Milliarden-Euro-Schaden-pro-Jahr** (Stand: 03.02.20).

1 Forschungsanlass

Das Phänomen der Innentäterschaft rückt in den letzten Jahren vermehrt in den Fokus der Betrachtung, wenn von Wirtschaftskriminalität, Wirtschaftsspionage, Cyberangriffe und Sabotage gesprochen wird. Der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) hat nach Auswertung von 2400 Schadensfällen im Jahr 2019 festgestellt, dass Innentäter für 63% der Fälle von Wirtschaftskriminalität verantwortlich sind und geht davon aus, dass jährlich 5 bis 10% der deutschen Unternehmen von eigenen Mitarbeitern betrogen werden.[2]
Mitarbeiter haben weitreichende Innenansichten in ihre Firma und verfügen - gegenüber Außentätern - über kritische Zugangsmöglichkeiten sowie umfassende kollegiale Kontakte und Netzwerke, um relevantes Wissen und Daten abzuschöpfen. Sorglosigkeit im Umgang mit sensiblen Informationen und die vermeintliche Vertrauenssituation zum unerkannten Innentäter erleichtern die Tatbegehung und unternehmensschädigendes Verhalten erheblich.
Bei der Recherche fällt auf, dass es wenige Forschungsarbeiten speziell zum Thema Innentäter gibt. Die Thematik wird 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“ angesprochen und teilweise beleuchtet. In Bezug auf eine spezielle Betrachtung der Innentäterschaft lassen sich daher Forschungslücken und weiterer Forschungsbedarf feststellen. Innentäterschaft ist nicht phänomenspezifisch - die gesamte Breite unternehmensschädigender Delikte kann durch Innentäter begangen werden. Es zeigt sich eine Bandbreite vom bewussten, vorsätzlichen bis hin zum unbewussten, fahrlässigen Täterverhalten.
Bereits 2017 wurde ein erster Monitoringbericht zum Thema „Innentäter in Unternehmen“ erstellt, der in diesem zweiten Bericht, aufgrund entsprechender Nachfrage, seine Fortsetzung und Aktualisierung erfährt.[3]

2 Forschungsfragen

Das Ziel des vorliegenden Berichtes ist es, wie bereits in der ersten themengleichen Sekundäranalyse, der Frage nachzugehen, welche aktuellen Erkenntnisse zu Innentätern im nationalen Raum vorliegen und wie groß die Gefahr der Kriminalität durch interne Mitarbeiter in Unternehmen heutzutage ist. Zusätzlich soll dargestellt werden, welche präventiven Ansatzmöglichkeiten sowie Detektionsmöglichkeiten es für Unternehmen gibt und wie das potenzielle Risiko für Unternehmen Opfer von Straftaten durch Innentäter zu werden, verringert werden kann. Die entsprechenden Erkenntnisse aus beiden Monitoringberichten fließen zusammengefasst im Kapitel 5 (Fazit) bei der Beantwortung folgender Fragen ein:

- Wer sind die Innentäter?

[2] Vgl. Schareika, Nora: „Diese Mitarbeiter betrügen am häufigsten ihre Unternehmen“. In: WirtschaftsWoche auf **www.wiwo.de** vom 04.09.19. Url: **https://www.wiwo.de/erfolg/management/wirtschaftskriminalitaet-diese-mitarbeiter-betruegen-am-haeufigsten-ihre-unternehmen/24979364.html** (Stand: 03.02.20).
[3] Der Bericht steht auf dem Informationsportal der Initiative Wirtschaftsschutz zum Download bereit. URL: **https://www.wirtschaftsschutz.info/SharedDocs/Artikel/DE/BKA-Kurzfassung-Innentaeter.html** (Stand: 03.02.20)

- Welche Situationen und Indikatoren können kritisch für einen möglichen Schadensfall durch Mitarbeiter sein?
- Welche Erscheinungsformen gibt es?
- Warum wird ein Mitarbeiter zum Innentäter?
- Welche Maßnahmen kann das Unternehmen ergreifen?

3 Methodik und Definition

Die erste Literaturrecherche zum Monitoringbericht „Innentäter in Unternehmen“ erfolgte im August 2017. Hierzu wurde anhand einer umfassenden stichwortgestützten Suche innerhalb von Suchportalen, Internetseiten von Forschungsinstituten und Lehrstühlen sowie Internetpräsenzen einzelner Behörden und Unternehmen nach Veröffentlichungen externer nationaler Forschungsbeiträge recherchiert. Diese Ergebnisse flossen in den Monitoringbericht „Innentäter in Unternehmen“ mit Stand 08/2017 ein.[4] Im August 2019 erfolgte aufgrund von Nachfragen eine methodengleiche zweite Literaturrecherche zur inhaltlichen Aktualisierung des Monitoringberichtes.[5]
Es gibt keine einheitliche Definition oder Terminologie zur Innentäterschaft, was die Vergleichbarkeit der verschiedenen Veröffentlichungen und Studien erschwert. Unterschieden wird in der Literatur zumeist zwischen dem Innentäter im engeren Sinne, d.h. allen Mitarbeitern eines Unternehmens, die in einem andauernden Beschäftigungsverhältnis stehen oder aus diesem kürzlich ausgeschieden sind, und dem Innentäter im weiteren Sinne. Dazu zählen befristete Beschäftigungsverhältnisse und alle weiteren geschäftlichen Kontakte, z.B. Leiharbeitskräfte, Praktikanten, Hospitanten, Diplomanden, Doktoranden, Lieferanten, Reinigungsfirmen, externe Dienstleister sowie Berater, Geschäfts- und Kooperationspartner, Rechtsanwälte etc. und Kunden, sofern sie gegenüber Außenstehen einen erweiterten Zugang zum Unternehmen oder Zugriff auf interne Informationen haben.
Den beiden Monitoringberichten zum Thema „Innentäter“ liegt die Definition des Innentäters von Grützner/Jakob zugrunde. Sie 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.“

Im Folgenden werden die aktualisierten Ergebnisse aus den recherchierten Beiträgen und ein Gesamtfazit präsentiert.

---

[4] Der Bericht steht auf dem Informationsportal der Initiative Wirtschaftsschutz zum Download bereit. URL: **https://www.wirtschaftsschutz.info/SharedDocs/Artikel/DE/BKA-Kurzfassung-Innentaeter.html** (Stand: 03.02.20)
[5] 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.

4 Ergebnisse

Konkrete und aktuelle Informationen zur Thematik bieten die Studien des Digitalverbandes Bitkom und der verschiedenen Unternehmensberatungen, die die aktuellen Probleme und Herausforderungen der Unternehmen zeitnah aufgreifen und in Befragungen untersuchen. Die Erkenntnisse sowie entwickelten Gegenmaßnahmen und Präventionshinweise werden veröffentlicht und bei Fachtagungen diskutiert. Zudem haben sich viele Beratungsfirmen auf die Schulung von Unternehmen und Mitarbeitern spezialisiert, um Wirtschaftskriminalität in diesen Bereichen vorzubeugen oder zu detektieren. Bei diesen Firmen liegt (Erfahrungs-)Wissen vor, das von Unternehmen eingekauft und genutzt werden kann.
Daneben verfügen das Bundesamt für Verfassungsschutz und die Landesämter für Verfassungsschutz im Bereich Wirtschaftsschutz über eine fundierte Expertise. Sowohl im persönlichen Beratungskontakt, auf Fachtagungen als auch in einschlägigen Veröffentlichungen, Broschüren und Flyern findet man dort umfassende und praxisnahe Informationen. Beispielhaft seien hier die folgenden genannt, die u.a. im Rahmen der „Initiative Wirtschaftsschutz“ auf dem Informationsportal[6] veröffentlicht wurden:

- Know-How-Schutz
- Personalauswahl
- Sicherheitslücke Mensch.

4.1 Veröffentlichungen von Sicherheitsbehörden und Verbänden

4.1.1 Bitkom (2019): Wirtschaftsschutz in der digitalen Welt[7]

Gegenstand: Periodisch erscheinende Dunkelfeldstudie des Digitalverbandes Bitkom zum Thema Wirtschaftsschutz. Befragt wurden branchenübergreifend 1.070 Geschäftsführer und Sicherheitsverantwortliche von Unternehmen ab 10 Mitarbeitern in Deutschland im Rahmen einer disproportional geschichteten Zufallsstichprobe. Dadurch wurde gewährleistet, dass Unternehmen aus den unterschiedlichen Branchen und Größenklassen in für statistische Auswertungen ausreichender Anzahl vertreten sind. Die Aussagen der Befragungsteilnehmer ergeben ein repräsentatives Bild für alle Unternehmen ab 10 Mitarbeitern in Deutschland. Als Methode wurde eine CATI-Befragung (computergestützte, mündliche, telefonische Befragung) im Zeitraum 29.04.19 – 14.06.19 gewählt.

Ziele: Erkenntnisgewinn zu Umfang und Betroffenheit deutscher Unternehmen von Datendiebstahl, Industrie- und Wirtschaftsspionage oder Sabotage in den letzten 2 Jahren. Darüber hinaus wurde eine Selbsteinschätzung zu den entstandenen Schäden sowie weitere Informationen zu Tätern, internen Sicherheitsmaßnahmen und Zusammenarbeitswünschen der Wirtschaft mit staatlichen Stellen erhoben.

---

[6] Initiative Wirtschaftsschutz – Das Informationsportal. URL: **https://www.wirtschaftsschutz.info/DE/Home/home_node.html** (Stand: 04.02.20).
[7] Bitkom (2019): „Wirtschaftsschutz in der digitalen Welt“. URL: **https://www.bitkom.org/sites/default/files/2019-11/bitkom_wirtschaftsschutz_2019_0.pdf** (Stand: 12.02.20) sowie Pressemitteilung Bitkom: „Angriffsziel deutsche Wirtschaft: mehr als 100 Milliarden Euro Schaden pro Jahr“ v. 06.11.19. URL: **https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-100-Milliarden-Euro-Schaden-pro-Jahr** (Stand: 12.02.20).

Forschungsfragen: Waren die Unternehmen innerhalb der letzten 2 Jahre von Datendiebstahl, Industriespionage oder Sabotage betroffen und falls ja, von welchen digitalen oder analogen Arten? Welche Schäden wurden festgestellt? Was wissen die Unternehmen über die Täter? Wie gelang die Detektion der Vorfälle? Wie entwickelt sich die Anzahl der Cyberattacken nach Einschätzung der Unternehmen in den nächsten 2 Jahren?

Ergebnisse:

- 3 von 4 Unternehmen wurden Opfer von Sabotage, Datendiebstahl oder Spionage (75%). 13% vermuteten betroffen gewesen zu sein (2017: 53% betroffene Unternehmen und 26% vermutlich betroffene, 2015: 51% betroffene Unternehmen und 28% vermutlich betroffene).

- Die häufigsten Delikte sind:
  - Diebstahl von IT- oder Telekommunikationsgeräten,
  - analoges Social Engineering,
  - Diebstahl von sensiblen digitalen Daten bzw. Informationen,
  - digitale Sabotage von Informations- und Produktionssystemen oder Betriebsabläufen,
  - analoger Diebstahl von sensiblen physischen Dokumenten, Unterlagen, Mustern, Maschinen, Bauteilen o.ä.,
  - digitales Social Engineering,
  - Ausspähen von digitaler Kommunikation.

- Durch Sabotage, Datendiebstahl oder Spionage entsteht der deutschen Wirtschaft jährlich ein Gesamtschaden von 102,9 Milliarden Euro. Der Schaden ist damit fast doppelt so hoch wie noch vor zwei Jahren (2016/2017: 55 Milliarden Euro p.a.).

Ehemalige Mitarbeiter stellen die größte Tätergruppe

Etwa ein Drittel der Betroffenen (33%) sagt, dass sie von früheren Mitarbeitern vorsätzlich geschädigt wurden. Ein knappes Viertel (23%) sieht vormals Beschäftigte in der Verantwortung, ohne ihnen ein absichtliches Fehlverhalten zu unterstellen.

- Eigene derzeitige Mitarbeiter ohne Absicht stellten 14% der Täter, eigene derzeitige Mitarbeiter vorsätzlich 0%.

- Vier von zehn Betroffenen (38 Prozent) führen Angriffe auf Einzeltäter bzw. sogenannte Hobby-Hacker zurück. Bei einem Fünftel geht die Spur jeweils zur organisierten Kriminalität (21%) oder zu konkurrierenden Unternehmen (20%). Bei 12% stammen Attacken von ausländischen Nachrichtendiensten.

- 39% der Angriffe kamen aus Deutschland, gefolgt von Osteuropa ohne Russland (28%), China (27%) und Russland (19%).

- Die Detektion der Vorfälle geschah am häufigsten durch eigene Mitarbeiter (62%), gefolgt von Hinweisen auf Angriffe durch eigene Sicherheitssysteme, z.B. Virenscanner oder Firewalls (54%), Hinweise durch die interne Revision bzw. interne Ermittlungseinheit (39%), anonyme Hinweise/ Ombudsmann (29%). Bei 28 Prozent war die Entdeckung reiner Zufall.

- Für die Zukunft prognostiziert eine breite Mehrheit der Unternehmen (82%) eine weitere Verschärfung der Sicherheitslage. Sie gehen davon aus, dass die Zahl der Cyberattacken auf ihr Unternehmen in den nächsten zwei Jahren zunehmen wird.

Bewertung: Die Bitkom-Studien sind derzeit die wichtigsten Dunkelfeldstudien im Themenfeld Wirtschaftsschutz. Die jährlichen Erhebungen erlauben gewisse Vergleiche zu den Vorjahren und bilden wesentliche Entwicklungen ab. Seit 2016 bleibt die Einschätzung der Unternehmen konstant (jeweils über 60%), dass Innentäter (insbesondere ehemalige Mitarbeiter) die größte Tätergruppe ausmachen. Ein eindeutiger Beleg für die Relevanz der Thematik Innentäterschaft, wenn man Wirtschaftsschutz ernsthaft betreiben möchte.

4.1.2 GDV (2019): Versicherer warnen vor hohen Schäden durch kriminelle Mitarbeiter[8]

Gegenstand: Auswertung von ca. 2.400 Schadensfällen aus der Vertrauensschadenversicherung durch den Gesamtverband der Deutschen Versicherungswirtschaft (GDV).[9] Eine Studie oder vertiefende Berichte zu den Ergebnissen liegen gemäß Auskunft des GDV vom 13.02.20 nicht vor. Am 04.09.19 fand ein Pressegespräch des GDV zur Veröffentlichung der Ergebnisse zum Thema: „Wirtschaftskriminalität: Tabuthema Innentäter“ statt.[10] Gesprochen wurde über die Apekte:

- Risikofaktor Innentäter: Typische Fallkonstellationen und wie sie zu verhindern sind (Rüdiger Kirsch, Vorsitzender der AG Vertrauensschadenversicherung im GDV)

- Täterprofile: Wann und warum werden Mitarbeiter kriminell? (Prof. Dr. jur. Hendrik Schneider, Lehrstuhl für Strafrecht, Juristenfakultät, Universität Leipzig; Inhaber des Büros für Gutachten & Strafverteidigung, Wirtschafts-& Medizinstrafrecht, Wiesbaden)

- Kriminelle Mitarbeiter als Haftungsrisiken für Geschäftsführer und Vorstände (Jesko Trahms, Rechtsanwalt, Partner, Fachanwalt für Strafrecht; BDO Legal Rechtsanwaltsgesellschaft mbH)

Ziele/ Forschungsfragen: Wer sind die Täter im Bereich Betrug und Untreue zum Nachteil von Unternehmen, was wissen wir über sie und welche Schäden verursachen sie?

Ergebnisse:

- In den untersuchten Fällen handelten zu 63% Innentäter, 37% der Fälle wurden von externen Tätern begangen.

- Die 63% Innentäter waren für 75% der Gesamtschäden von 225 Mio € verantwortlich.

---

[8] Gesamtverband der Deutschen Versicherungswirtschaft (GDV): „Versicherer warnen vor hohen Schäden durch kriminelle Mitarbeiter“. Medieninformation vom 04.09.2019. URL: **https://www.gdv.de/de/medien/aktuell/versicherer-warnen-vor-hohen-schaeden-durch--kriminelle-mitarbeiter-50522** (Stand: 13.02.19).

[9] Eine Vertrauensschadenversicherung entschädigt Unternehmen, wenn interne oder externe Vertrauenspersonen Gelder veruntreuen oder das Unternehmen betrügen.

[10] Vgl. URL: **https://www.gdv.de/de/themen/news/pressegespraech--wirtschaftskriminalitaet--tabuthema-innentaeter--50186** (Stand: 17.02.20).

• Im Schnitt erbeuten kriminelle Mitarbeiter fast 115.000 Euro, bevor sie auffallen. Externe Betrüger kommen durchschnittlich gerade mal auf die Hälfte dieser Summe.

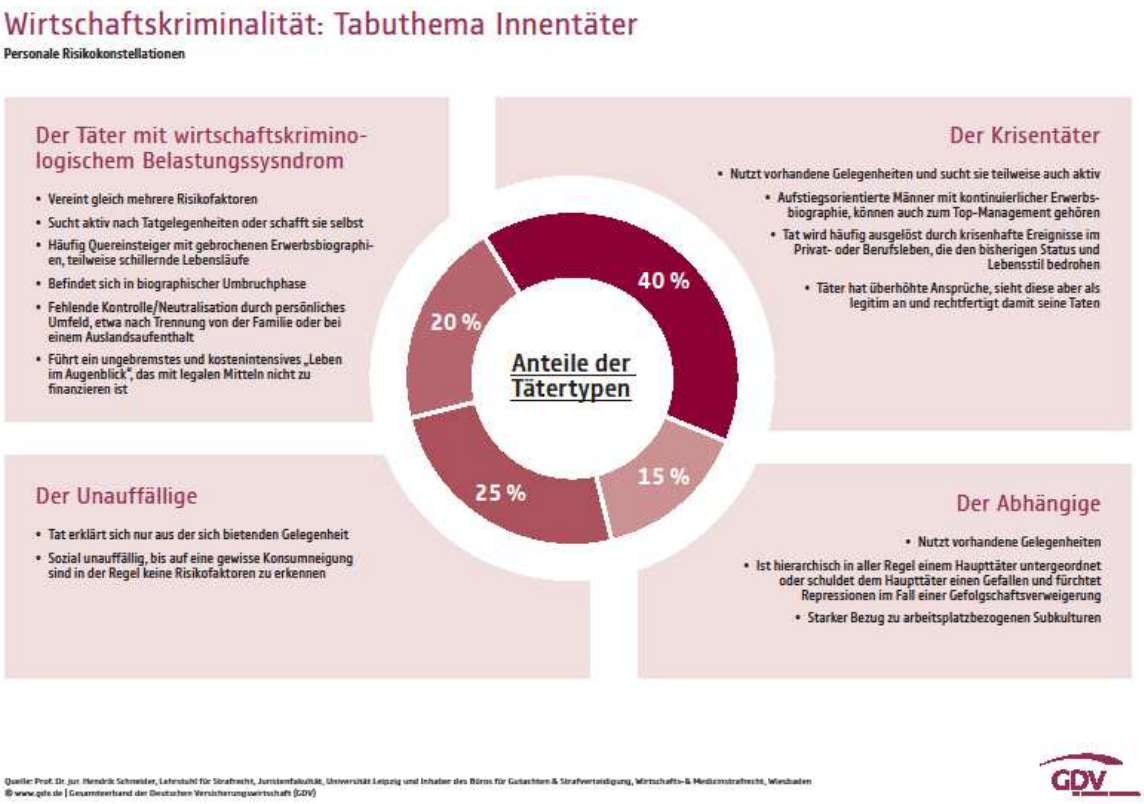
• 5 bis 10% der deutschen Unternehmen werden jedes Jahr von eigenen Mitarbeitern betrogen.

• Die Täter sind in der Regel über 40 Jahre alt, meist männlich, besitzen die deutsche Staatsangehörigkeit, mit überdurchschnittlichem Bildungshintergrund. Sie sind zumeist schon längere Zeit in ihrem Unternehmen beschäftigt und bekleiden häufig verantwortliche Positionen.

• Tätertypen (personale Risikofaktoren)[11]:
  - o Der Krisentäter
    - ▪ Nutzt vorhandene Gelegenheiten und sucht sie teilweise auch aktiv.
    - ▪ Aufstiegsorientierte Männer mit kontinuierlicher Erwerbsbiographie, können auch zum Top-Management gehören.
    - ▪ Tat wird häufig ausgelöst durch krisenhafte Ereignisse im Privat- oder Berufsleben, die den bisherigen Status und Lebensstil bedrohen.
    - ▪ Täter hat überhöhte Ansprüche, sieht diese aber als legitim an und rechtfertigt damit seine Taten.
    - ▪ Anteil an allen Tätern: rund 40%.
  - o Der Unauffällige
    - ▪ Tat erklärt sich nur aus der sich bietenden Gelegenheit.
    - ▪ Sozial unauffällig, bis auf eine gewisse Konsumneigung sind in der Regel keine Risikofaktoren erkennbar.
    - ▪ Anteil an allen Tätern: rund 25%.
  - o Der Täter mit wirtschafskriminologischem Belastungssyndrom
    - ▪ Vereint gleich mehrere Risikofaktoren.
    - ▪ Sucht aktiv nach Tatgelegenheit oder schafft sie selbst.
    - ▪ Häufig Quereinsteiger mit gebrochenen Erwerbsbiographien, teilweise schillernde Lebensläufe.
    - ▪ Befindet sich in biographischer Umbruchphase.
    - ▪ Fehlende Kontrolle/ Neutralisation durch persönliches Umfeld, etwa nach Trennung von der Familie oder bei einem Auslandsaufenthalt.
    - ▪ Führt ein ungebremstes „Leben im Augenblick“, das mit legalen Mitteln nicht zu finanzieren ist.
    - ▪ Anteil an allen Tätern: rund 20%.
  - o Der Abhängige
    - ▪ Nutzt vorhandene Gelegenheiten.

[11] Vgl. Handout „Personale Risikokonstellationen“ zum Pressegespräch des GDV am 04.09.20. Das Dokument wurde dem BKA am 13.02.20 vom GDV zur Verfügung gestellt.

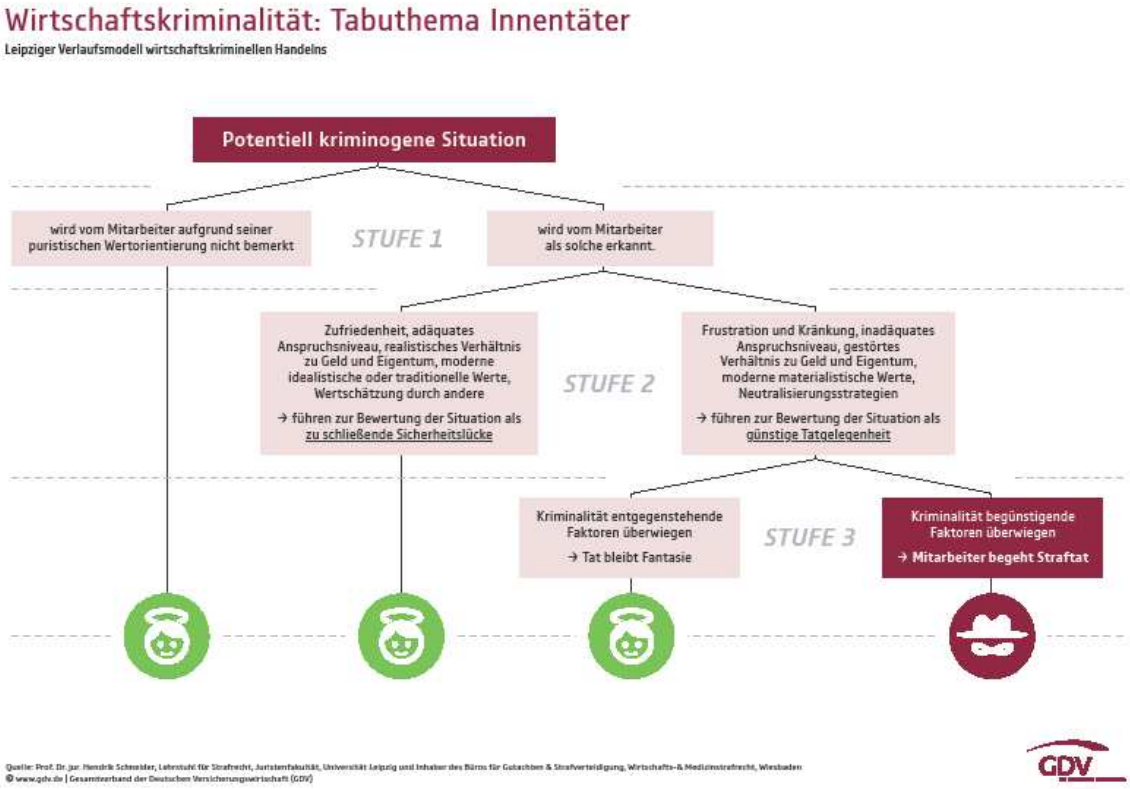
- Ist hierarchisch in aller Regel einem Haupttäter untergeordnet oder schuldet dem Haupttäter einen Gefallen und fürchtet Repressionen im Falle einer Gefolgschaftsverweigerung.
- Starker Bezug zu arbeitsplatzbezogenen Subkulturen.
- Anteil an allen Tätern: rund 15%.



Quelle: Prof. Dr. jur. Hendrik Schneider, Lehrstuhl für Strafrecht, Juristenfakultät, Universität Leipzig und Inhaber des Büros für Gutachten & Strafverteidigung, Wirtschafts-& Medizinstrafrecht, Wiesbaden. © www.gdv.de | Gesamtverband der Deutschen Versicherungswirtschaft (GDV).

• Gemäß dem Leipziger Verlaufsmodell für wirtschaftskriminelles Handeln können Frustration und Kränkung, ein inadäquates Anspruchsniveau, ein gestörtes Verhältnis zu Geld und Eigentum, moderne materialistische Werte sowie Neutralisierungsstrategien dazu führen, dass potentielle kriminogene Situationen verstärkt als günstige Tatgelegenheit für strafbares Handeln ausgenutzt werden. Zufriedenheit am Arbeitsplatz, ein adäquates Anspruchsniveau, ein realistisches Verhältnis zu Geld und Eigentum, moderne idealistische oder traditionelle Werte sowie Wertschätzung durch andere führen dagegen eher zur Bewertung der Situation als zu schließende Sicherheitslücke.[12]

[12] Vgl. Handout „Wirtschaftskriminalität: Tabuthema Innentäter - Leipziger Verlaufsmodell wirtschaftskriminellen Handelns" zum Pressegespräch des GDV am 04.09.20. Das Dokument wurde dem BKA am 13.02.20 vom GDV zur Verfügung gestellt.



Quelle: Prof. Dr. jur. Hendrik Schneider, Lehrstuhl für Strafrecht, Juristenfakultät, Universität Leipzig und Inhaber des Büros für Gutachten & Strafverteidigung, Wirtschafts-& Medizinstrafrecht, Wiesbaden. © www.gdv.de | Gesamtverband der Deutschen Versicherungswirtschaft (GDV).

- Unternehmen mit einem guten Betriebsklima, fairer Entlohnung und einer menschenorientierten Führung können die Risikofaktoren minimieren.
- Folgende Schutzmaßnahmen werden empfohlen:
  - o einen Compliance-Beauftragten benennen.
  - o ein Hinweisgeber-System aufbauen.
  - o einen verbindlichen Verhaltenskodex verabschieden.
  - o die Mitarbeiter regelmäßig schulen.
  - o bei Zahlungen strikt das Vier-Augen-Prinzip beachten.
  - o Polizeiliches Führungszeugnis bei der Besetzung exponierter Stellen anfordern.

Bewertung: Bei dieser Auswertung handelt es sich um eine der wenigen Hellfeldanalysen in diesem Themenfeld. Ca. 2.400 Schadensfälle im Bereich Betrug und Untreue zum Nachteil von Unternehmen wurden dabei ausgewertet. Auch wenn es in diesen Deliktsfeldern nicht erstaunt, dass die Mehrzahl der Täter Innentäter sind, so ergeben sich doch wesentliche gesicherte Erkenntnisse zum Phänomen der Innentäterschaft sowie konkrete Schadenshöhen. Leider stehen die erhobenen Daten nicht für weitere Forschungszwecke zur Verfügung und können daher nicht tiefergehend untersucht werden. Allerdings ist der Ansatz des GDV als Datenbesitzer richtungsweisend, sich diesem

wichtigen Thema zu öffnen und die bestehende Erkenntnislage durch Aktenauswertungen zu bereichern. Die gemeinsame Präsentation und Diskussion der Ergebnisse durch mehrere Experten aus verschiedenen Perspektiven (hier: Verband, Wissenschaft, Praktiker) ist der richtige Weg, sich dem Thema Innentäterschaft ganzheitlich zu widmen.

4.1.3 Bitkom (2018): Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie [13]

Gegenstand: Mit der vorliegenden Dunkelfeldstudie untersuchte der Digitalverband Bitkom wiederholt mittels CATI Befragung von über 500 Unternehmen ab 10 Mitarbeitern im Mai 2018, wie es um die deutsche Industrie beim Thema Wirtschaftsschutz bestellt ist. Zielgruppe waren vorrangig Führungskräfte, die in ihrem Unternehmen das Thema Wirtschaftsschutz verantworten. Dazu zählen Geschäftsführer sowie Führungskräfte aus den Bereichen Unternehmenssicherheit, IT-Sicherheit, Risikomanagement oder Finanzen.

Ziele: Darstellung des Digitalisierungsniveaus der deutschen Industrie, der Betroffenheit von Unternehmen, der aufgetretenen Schäden, des Täterkreises, der Aufklärung und Untersuchung der Fälle sowie von Sicherheitsvorkehrungen. Thematisiert werden darüber hinaus die Themen „Zukünftige Bedrohungsszenarien und Eignung von IT-Sicherheitsmaßnahmen“ und „Cyber-Versicherungen“. Ziel ist, das Zusammenspiel aller Bereiche eines Unternehmens und den Sicherheitsverantwortlichen zu erhöhen, damit der Schutz gegen Cyberspionage, Cybersabotage und Cybercrime nachhaltig erhöht werden und ein umfassender Wirtschaftsschutz gelingen kann.

Forschungsfragen: Welche Digitalstrategien gibt es und wie hoch ist der Grad der Digitalisierung? Welche Unternehmen sind von Spionage, Sabotage und Datendiebstahl betroffen? Was wissen wir über die Täter? Schützt sich die Wirtschaft heute schon ausreichend? Welche Schäden treten auf?

Ergebnisse:

- Der überwiegende Teil aller Industrieunternehmen in Deutschland ist von digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl betroffen oder vermutet betroffen zu sein. 68% der Industrieunternehmen gaben an, in den vergangenen zwei Jahren Opfer von Datendiebstahl, Industriespionage oder Sabotage gewesen zu sein. Weitere 19% waren vermutlich betroffen.

- Der Mittelstand ist im Fokus der Angreifer (73% der Unternehmen in der Größe von 100 bis unter 500 Mitarbeitern waren betroffen). Der Mittelstand in Deutschland ist besonders innovativ und stark in die Lieferketten von großen Konzernen eingebunden. Insofern liegt es nahe, dass es Angreifer zum einen auf das Spezialwissen der KMU abgesehen haben. Und zum anderen KMU als Einfallstore nutzen, um an die Daten großer Konzerne zu gelangen.

- In der Regel schützen sich Großkonzerne besser. Unternehmen mit mehr als 500 Mitarbeitern sind erkennbar weniger angegriffen worden (60%). 68% der Unternehmen mit 10 bis 99 Mitarbeiter waren Opfer von Spionage, Sabotage und Datendiebstahl.

- Häufigstes Delikt war in den letzten zwei Jahren der Diebstahl von IT- und Telekommunikationsgeräten (32%). Die Täter können es hierbei auf die Hardware oder auf die Daten, die sich auf

[13] Bitkom (2018): „Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie“. URL: **https://www.bitkom.org/sites/default/files/file/import/181008-Bitkom-Studie-Wirtschaftsschutz-2018-NEU.pdf** (Stand: 23.09.2019).

der Hardware befinden, abgesehen haben. Gefolgt vom Diebstahl sensibler digitaler Daten bzw. Informationen (23%) und dem analogen Diebstahl von sensiblen physischen Dokumenten, Unterlagen, Mustern, Maschinen o. ä (21%).

• Digitale IT-Angriffe haben große Schäden bei den Wirtschaftsunternehmen verursacht. Fast die Hälfte (47%) erlitt Schäden durch digitale Angriffe (insbesondere Kosten für Rechtsstreitigkeiten, Imageschäden bei Kunden oder Lieferanten, Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen, Patentrechtsverletzungen und Ausfall, Diebstahl oder Schädigung von Informationssystemen).

• Der Schaden als Folge digitaler Wirtschaftsspionage, Sabotage und Datendiebstahls liegt nach konservativen Berechnungen bei rund 43,4 Mrd. Euro innerhalb der letzten zwei Jahre.

Ehemalige Mitarbeiter stellen die größte Tätergruppe

Zwei Drittel der geschädigten Unternehmen (68%) gaben an, durch insbesondere ehemalige oder eigene derzeitige Mitarbeiter (7%) geschädigt worden zu sein. „Damit bleibt der mit Abstand größte Täterkreis im eigenen Haus."[14] Die Tatgelegenheit wird überwiegend während der aktiven Mitarbeit geschaffen.

• Der Täterkreis umfasst Innentäter, wie ehemalige Mitarbeiter (61%) und eigene derzeitige Mitarbeiter (7%) bis hin zu Außentätern, wie Privatpersonen/ Hobby-Hacker (29%), konkurrierende Unternehmen (22%), Organisierte Kriminalität (Banden) (17%), Kunden (15%) und Lieferanten (14%) sowie ausländische Nachrichtendienste (11%) und externe Dienstleister/ Berater (9%), wobei die Innentäter die größte Gruppe darstellen.

• Bei Innentätern darf nicht grundsätzlich von einem Tatvorsatz ausgegangen werden. Fehlende Sensibilisierung und Awareness in Kombination mit Gedankenlosigkeit sind häufig ursächlich für ein Fehlverhalten.

• 36% der Angriffe kamen aus Deutschland, gefolgt von Russland (24%). China, Japan und Osteuropa (ohne Russland) waren in jeweils knapp 17% bzw. 18% der Fälle der Ausgangspunkt der Attacken.

• In 61% der Fälle wurden Mitarbeiter auf die dolosen Handlungen aufmerksam. Damit lässt sich festhalten: Ein effektiver Schutz vor Spionage, Diebstahl oder Sabotage sind motivierte, gut geschulte und aufmerksame Mitarbeiter. Wer hier investiert, sorgt am besten vor.

• Das eigene Sicherheitssystem/ Virenscanner/ Firewall lieferten in 40% Hinweise zur Aufdeckung der Vorfälle und in 38% der Fälle die Interne Revision bzw. interne Ermittlungseinheit.

• Die überwiegende Mehrheit der Betroffenen hat Strafanzeige gestellt (78%). Es ist wichtig, dass sich Betroffene grundsätzlich an Ermittlungsbehörden wenden. Denn diese können nur dann erfolgreich arbeiten, wenn sie auch Kenntnis von den Delikten haben. Nur durch die Zusammenarbeit mit staatlichen Stellen können ein realistisches Lagebild erstellt, neue Angriffswege rechtzeitig erkannt und andere Unternehmen gewarnt und geschützt werden.

[14] Ebd., S. 28.

• 90% derjenigen, die betroffen waren und den Vorfall gemeldet haben, haben dies bei der Polizei getan. Dieses Bild zeichnet sich durch alle Größenklassen ab. Ein Grund für diese hohe Prozentzahl könnten die in einigen Landeskriminalämtern eingerichteten Zentralen Anlaufstellen Cybercrime (ZAC) sein. Gerade für mittelständische Unternehmen sind sie ein wichtiger Ansprechpartner – sowohl für präventive Maßnahmen als auch im Ernstfall.

Empfehlungen:

• IT-Sicherheit im Unternehmen zur Chefsache machen, eigene Wirtschaftsschutz-Beauftragte oder Informations-Sicherheitsbeauftragte bestimmen, die die Themen in die Breite tragen.

• Aufbau und Pflege eines robusten IT-Sicherheitsmanagements.

• Etablierung eines präventiven und permanenten Risikomanagements.

• Ergänzung des Basisschutzes um Verschlüsselung und eine spezielle Angriffserkennung. Die Überwachung vernetzter Geräte und Erkennung von Anomalien beispielsweise durch ein Security Information Event Management ist ebenso empfehlenswert, wie die Beachtung von Security by Design bei allen Schnittstellen und vernetzten Geräten.

• Regelmäßige arbeitsplatzspezifische Schulungen und die Sensibilisierung der Mitarbeiter zu Themen wie Spionage, Sabotage und Datendiebstahl.

• Hintergrundchecks von Mitarbeitern auf sensiblen Positionen.

• Einrichtung von Möglichkeiten zur anonymen Meldung von Missständen und Vorfällen.

• Sicherheitszertifizierungen.

• Förderung und Teilnahme am fachlichen Austausch aller beteiligten Akteure (Unternehmen und Sicherheitsbehörden).

Bewertung: (S. Bewertung zu 4.1.1): Die Bitkom-Studien sind derzeit die wichtigsten Dunkelfeldstudien im Themenfeld Wirtschaftsschutz. Die jährlichen Erhebungen erlauben Vergleiche zu den Vorjahren und bilden wesentliche Entwicklungen ab. Seit 2016 bleibt die Einschätzung der Unternehmen konstant (jeweils über 60%), dass Innentäter (insbesondere ehemalige Mitarbeiter) die größte Tätergruppe ausmachen. Ein eindeutiger Beleg für die Relevanz der Thematik Innentäterschaft, wenn man Wirtschaftsschutz ernsthaft betreiben möchte.

4.1.4 Bundesamt für Sicherheit in der Informationstechnik (2018): Empfehlung: IT in der Produktion - Industrial Control System Security – Innentäter[15]

Gegenstand: In der Vergangenheit sind Industrielle Steuerungen mangels Vernetzung fast nur durch Angriffe vor Ort bedroht gewesen. Mit dem Aufkommen der neuen Cyber-Bedrohungen ist auch die Innentäterproblematik durch immer weiter gehende Arbeitsteilung noch relevanter ge-

[15] Bundesamt für Sicherheit in der Informationstechnik (2018): Industrial Control System Security - Innentäter. BSI – Veröffentlichungen zur Cybersicherheit. BSI-CS 061/ Version 2.0 vom 11.07.2018. Url: **https://www.bsi.bund.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_061.pdf?__blob=publicationFile&v=6** (Stand: 05.02.20)

worden. Im Fokus stehen dabei nicht nur Angriffe gegen die industriellen Anlagen eines Betreibers selbst. Auch die gesamte Lieferkette ist zu berücksichtigen, denn alle beteiligten Dienstleister und Geschäftspartner bilden als potenzielle Innentäter jeweils einen zusätzlichen Angriffsvektor.

Definition Innentäter im Bereich Industrielle Steuerungen[16]:

Potenzielle Innentäter sind sämtliche Personen mit (privilegiertem) Zugriff auf bzw. Zutritt zu IT-Komponenten, IT-Diensten, Installationen, Dokumenten oder sonstigen ggf. kritischen Informationen und Geräten. Insbesondere sind hierbei folgende Personenkreise zu nennen:

- *Personen mit unmittelbarem physischen Zugriff auf Steuerungsanlagen (z. B. Bediener, Ingenieure)*
- *Personen mit privilegierten Rechten (z. B. Administratoren)*
- *Personen mit indirektem Zugang, z. B. auch zum Office-Netz oder zu Verwaltungsgebäuden*
- *Mitarbeiter von Dienstleistern (z. B. Wartung oder Softwareentwicklung), Lieferanten, etc..*

Ziele: Das 4-seitige Dokument bietet eine praxisnahe Kurzübersicht zum Thema „Industrial Control System Security“ und gibt eine Reihe von Informationen über und Empfehlungen zum Umgang mit der Bedrohung durch Innentäter.

Ergebnisse:

- Kein Generalverdacht gegen eigene Mitarbeiter und Externe.
- Mögliche Angriffsarten:
  - Verlust bzw. Diebstahl von Informationen (Data Leakage) durch Zugriffsmöglichkeiten auf Fileserver, Datenträger oder IT-Systeme oder auf physische Dokumente,
  - Social Engineering,
  - Sabotage.
- Allgemeine organisatorische Sicherheitsmaßnahmen:
  - Inventarisierung (Erfassen von Zugriffsmöglichkeiten/ Nutzerprofilen und somit potenziellen Möglichkeiten für eine Innentäterschaft sowie die dazugehörenden Privilegien. Dies beinhaltet die Dokumentation sämtlicher Zugriffsmöglichkeiten bzw. Accounts für Benutzer, Administratoren und Externe, wobei Funktions-/Gruppen-Accounts besonders kritisch zu hinterfragen sind).
  - Festschreibung von Policies für unterschiedliche Gruppen von Mitarbeitern (z.B. Verhaltensregeln für die Verwendung von Wechseldatenträgern oder Regelungen zum Umgang mit und der Weitergabe von Dokumenten).
  - Sensibilisierung und Schulung der Mitarbeiter über bestehende Policies.

[16] Ebd., S. 1.

- Identitäts- und Berechtigungsmanagement (z.B. unmittelbarer Widerruf von Berechtigungen (IT & physisch) bei Wegfall der Notwendigkeit).
- Etablierung eines Change Managements (keine Ad hoc Änderungen („auf Zuruf") an Systemen, Prinzip der Rollenteilung, Vier-Augen-Prinzip).
- Durchsetzung einer strikten Zutrittskontrolle.
- Zentrale Schlüsselverwaltung („Schlüsselbuch").
- Meldestelle, um vertraulich auf Missstände hinweisen zu können (Whistleblower).

• Ergänzende technische Maßnahmen:
  - Zentrale Bündelung der Maßnahmen (z.B. in Form eines Security Information& Event Management (SIEM) sowie eines Identity & Access Managements (IAM / IDM).
  - Sicherer Authentisierungsmechanismen (z. B. Token) und individuelle Accounts mit hinreichender Authentisierung (z. B. Multi-factor).
  - Unterstützung der Zugangskontrollsysteme bei Nutzung digitaler Ausweise durch technische Maßnahmen und z.B. Videoüberwachung im Rahmen der rechtlichen Möglichkeiten.
  - Absicherung bei Steuerungen (z. B. Speicher-programmierbare Steuerungen, SPS) durch Bedienereingriff mit einer Authentisierung oder nach dem Vier-Augen-Prinzip.
  - Einrichtung technischer Sicherheitskomponenten (Firewalls, uni-direktionale Gateways) für die verschiedenen Zugriffsmöglichkeiten.
  - Verwendung der in IT-Systemen verfügbaren Mechanismen für Timeouts von Nutzersitzungen sowie passwortgeschützte Bildschirmschoner.
  - Umsetzung von Virenschutz auf Netzwerk- und ggf. Hostebene für Server, Workstations und Terminals (alternativ kann auch Application Whitelisting zur Beschränkung der zulässigen Applikationen und Prozesse umgesetzt werden, Wechseldatenträgerschleuse).
  - Einsatz von Device Control Lösungen, um die Verwendung von unzulässigen Wechseldatenträgern und USB-Geräten zu verhindern.

• Detektion von Schadensfällen:
  - Automatisiertes Monitoring von IT-Systemen sowie deren Konfigurationen und Logdateien.
  - Automatische Detektion neuer IT-Systeme und Netzwerkkomponenten im Netz (z. B. WLAN Access Point).

• Sicherheitsmaßnahmen bei externen Mitarbeitern (Fremdfirmen):
  - Fester Ansprechpartners für IT-Sicherheitsfragen in der Fremdfirma.
  - Juristische Regelungen zur Geheimhaltung (Non-disclosure Agreements, NDA).
  - Verbindliche Absprachen über die Rechte und Pflichten der Fremdfirma bei der Datenverarbeitung (z.B. schriftliche Erlaubnis zur Nutzung von Outsourcing oder Clouddiensten).
  - Prüfung der Policies und diesbezüglichen Regelwerke in der Fremdfirma.

- Security-Check externer Service-Notebooks mit anschließender Ausstellung eines Besucher-Zertifikats für den Netzwerkzugriff.
- Verschlüsselte Datenübertragung.
- Forderung einer Zertifizierung gemäß etablierter Standards (z.B. IT-Grundschutz oder ISO 27000).
- Zutrittsregelungen für kritische Einsatzbereiche (z.B. Begleitung, nur zu bestimmten Tageszeiten).
- Einrichtung von Zugängen zu internen IT-Systemen nur mit einer zeitlichen Beschränkung.
- Zugriffe auf und Änderungen an kritischen IT-Systemen unterliegen einem hinreichend sicheren und detaillierten Logging-Mechanismus.
- Right to Audit: Das beauftragende Unternehmen ist berechtigt, die Einhaltung der Sicherheitsvorgaben zu prüfen bzw. durch Dritte prüfen zu lassen.

Bewertung: Diese Kurzempfehlungen des BSI im Rahmen der Veröffentlichungen zur Cyber-Sicherheit bieten der Zielgruppe prägnante, praxisnahe und umfassende Handlungsempfehlungen für Sicherheitsmaßnahmen gegen Innentäter im Bereich Industrielle Steuerungen und Anlagen. Übersichtlich aufgebaut und verständlich geschrieben wird ein breites Angebot an Handlungsoptionen in einer Kurzdarstellung von 4 Seiten dargeboten, das dem Anspruch einer soliden Information in jeder Hinsicht genügt.

4.2 Studien und sonstige Veröffentlichungen

4.2.1 Dr. Andreas Blume (2018): Innentäterspionage in innovationsgetriebenen Großunternehmen[17]

Gegenstand: Vorstellung von Aspekten eines ganzheitlichen präventiven und reaktiven Interventionskonzeptes gegen Innentäterspionage aus Sicht einer Corporate Security in einem innovationsgetriebenen Großunternehmen. Betrachtet wird in dieser Arbeit der vorsätzlich handelnde Innentäter, und nicht der fahrlässig handelnde.

[17] Dr. Blume, Andreas (2018): „Innentäterspionage in innovationsgetriebenen Großunternehmen“. Frankfurt, Verlag für Polizeiwissenschaft. ISBN: 978-3-86676-538-2.

Ziele: Blick der Konzernsicherheit auf die Erstellung von strategischen Security-Konzepten für innovationsgetriebene Großunternehmen in Deutschland, die mit hoher Wahrscheinlichkeit im Fokus von Spionagebemühungen vieler Akteure stehen. Derartige Unternehmen haben einen erheblichen Bedarf an effektivem Informationsschutz. Die aus Phänomenologie und Ätiologie abgeleiteten Erkenntnisse sollen im Rahmen einer strategischen Sichtweise die wesentliche Bausteine (Anforderungen) einer Anti-Innentäterspionage-Strategie auf ein mittleres Abstraktionsniveau überführen. Beispiele zur konkreten Ausgestaltung veranschaulichen diese Anforderungen. Zur Zielsetzung dieser Arbeit gehört nicht die Erstellung eines detaillierten Schutzkonzeptes für ein spezifisches Unternehmen.

Definition Innentäter

Als Innentäter wird eine natürliche Person definiert, die aufgrund eines Beschäftigungsverhältnisses besondere Kenntnisse und Fertigkeiten besitzt, durch die sie Zugang zu unternehmensbezogenen Informationen oder Prozessen hat, die einem außenstehenden Täterkreis nicht oder nur unter erheblichen Schwierigkeiten zugänglich sind und diese Informationen missbraucht (angelehnt an Fleischer 2016).

Forschungsfragen: Welche Erkenntnisse und Ansatzpunkte für wirksame präventive und reaktive Gegenmaßnahmen lassen sich auf Basis einer kriminologischen Analyse des Phänomens Innentäterspionage und seiner Ursachen identifizieren? Wie kann man ein effektives, ganzheitliches Schutzkonzept gegen Innentäterspionage ausgestalten?

Ergebnisse:

- Trotz eines vernachlässigbaren Hellfeldes war, ist und bleibt Innentäterspionage für innovationsgetrieben (Groß-)Unternehmen ein erhebliches finanzielles Risiko. Obwohl in etwa jedem zweiten innerbetrieblich identifizierten Spionagefall ein Innentäter involviert ist und in für Spionage gefährdeten Unternehmen ein ausgeprägteres Bedrohungsbewusstsein vorhanden ist, als man vom Hellfeld aus schließen könnte, werden paradoxerweise Schutzmaßnahmen schwerpunktmäßig nach wie vor auf externe Angreifer fokussiert. Gründe hierfür sind:
    - Die Datenbasis im Hinblick auf die tatsächliche Verbreitung von Innentäterspionage ist unzureichend. Darüber hinaus erschwert eine Vielzahl materiell-rechtlicher Normen die statistische Erfassung des Phänomens zusätzlich.
    - Die Vielfältigkeit der Erscheinungsformen und Tatbegehungsmöglichkeiten, wovon einige leicht kaschierbar sind.
    - Das Argument, man müsse Mitarbeitern (Bewerbern, Geschäfts- und Kooperationspartnern) (doch) vertrauen können.
    - Schwierigkeiten bei der Identifizierung kritischer Aktivitäten.
    - Hürden im Hinblick auf das interne Meldeverhalten von Verdachtsmomenten.
    - Die Notwendigkeit, ausreichend ausgebildetes Ermittlungspersonal vorzuhalten.
    - Eine erschwerte Sanktionierung aufgrund eines weit verbreiteten Geheimhaltewillens von Vorfällen.
- Jede Reduzierung von Motiven, Rechtfertigungen und Tatgelegenheiten für mögliche Täter wirkt risikoreduzierend. Daher ist die Umsetzung eines interdisziplinären, präventiven und reaktiven Schutzkonzeptes für Unternehmen lohnenswert.

- Präventive und reaktive Maßnahmen:
    - o Systematische Erfassung, Klassifizierung und Segmentierung schützenswerter Informationen.
    - o Stringente Zugangskontrollen nach dem Need-to-Know, Need-to-See und Need-to-Go Prinzip.
    - o eine durch Hintergrundprüfung abgesicherte Personalauswahl (Pre-Employment-Screening von Bewerbern auf kritische Funktionen).
    - o konsequente Durchführung von Risikobewertungen hinsichtlich der Aufgaben, die fremdvergeben werden können oder nicht.
    - o eine auch auf Security-Kriterien gestützte Selektion der Geschäfts- und Kooperationspartner.
    - o Security-Trainings, um ein hinreichendes Wachsamkeitsniveau aufrechterhalten zu können (situations- und zielgruppenspezifische Schulungen).
    - o Adäquates Führungsverhalten (u.a. Interesse für die Belange und Sorgen der Mitarbeiter, Wertschätzung, Entscheidungsteilhabe bzw. ausreichende Information).
    - o Konzept zur Detektion und Unterbindung unerwünschter Aktionen der Informationssicherheit und des -transfers der Mitarbeiter.
    - o Ein professionelles Freisetzungsmanagement (u.a. Austrittsgespräche mit Mitarbeitern, Freisetzungsbelehrung).
    - o Professionelle Unterstützung von Mitarbeitern in persönlichen Krisen/ Notlagen und/ oder ggf. Weiterleitung an professionelle Sozialberater.
    - o Detektion kritischer Verhaltensindikatoren von Mitarbeitern.
    - o Einrichtung von Meldestellen für Mitarbeiter.
    - o Konsequente Durchführung interner Ermittlungen.
    - o Verhängung von wirksamen und abschreckenden Maßnahmen im Schadensfall.
    - o Regelmäßige Evaluation und Weiterentwicklung des Schutzkonzeptes.

Bewertung: Die Veröffentlichung bietet umfassende Kenntnisse und praxisnahe Maßnahmen für die Zielgruppe an. Neben Definitionen, einem theoretischen Bezugsahmen, phänomenologischen Aspekten zur materiell-rechtlichen Einordnung, Erscheinungsformen sowie Strukturdaten und Statistiken, wird der Entstehungsprozess zur Innentäterschaft mit Motiven, Persönlichkeitsstrukturen und Rechtfertigungsstrategien ausführlich erläutert. Der Schwerpunkt der Arbeit liegt dann schlussfolgernd auf der Darstellung eines ganzheitlichen Schutzkonzeptes, in dem die einzelnen Interventionsaspekte (Risikobeurteilung, Informationsklassifizierung, Personalauswahl und -freisetzung, Kooperationen und Geschäftspartner, Security-Kultur, Führungsverhalten, technische und physische Sicherheit, Detektion und Reaktion, Meldewege und Ermittlungen, Sanktionen sowie die regelmäßige Anpassung und Weiterentwicklung des Konzeptes) ausführlich erläutert werden. Großunternehmen bzw. ihre Corporate Security, die sich der Thematik umfassend stellen möchten, finden hier ein aktuelles Werk mit einem umfänglichen Portfolio an Interventionsmaßnahmen, das explizit für die Praxis geschrieben wurde.

4.2.2 Dennis, Buroh (2017): So wird man zum Innentäter. In Computerwoche von IDG[18]

Gegenstand: Beschreibung des Phänomens Innentäter, Übersicht über verschiedene Motivlagen, Fallbeschreibungen (Hacker inside – so greifen Insider an), Maßnahmen zum Unternehmensschutz. Es handelt sich um eine Sekundäranalyse.

Ziele: Kurze Übersicht, Sensibilisierung und Aufklärung darüber, dass allein technische Maßnahmen keine ausreichende Sicherheit gewährleisten können und der Faktor Mensch in diesem Zusammenhang häufig unterschätzt wird.

Ergebnisse: Der Autor zieht, über die Erkenntnisse deutscher Veröffentlichungen, amerikanische Literatur hinzu. So beschreibt er ergänzend die psychologischen Risikofaktoren, die Mitarbeiter überhaupt erst anfällig für eine Innentäterschaft machen:

- An erster Stelle steht die psychische und gesundheitliche Verfassung, die sich unmittelbar auf die Wahrnehmungs- und Urteilsfähigkeit des Mitarbeiters auswirkt, insbesondere auf dessen soziale Interaktion und Performance am Arbeitsplatz.
- Die daraus gebildete Persönlichkeit des Einzelnen, seine sozialen Fähigkeiten und seine Vorgehensweise in der Entscheidungsfindung sind die Faktoren, die im Weiteren dessen Eigenwahrnehmung und dessen Wahrnehmung der Umgebung beeinflussen. Sie bestimmen die Wahrscheinlichkeit sozialer Konflikte und möglicher Isolation. Nach außen hin zeigt sich dies beispielsweise durch:
    - Probleme in der Zusammenarbeit,
    - Impulsivität,
    - das Gefühl über den Regeln zu stehen,
    - die Schwierigkeit bei der Übernahme von Verantwortung und
    - der Tendenz, eher andere für Fehler verantwortlich zu machen.
- Kommen persönliche Stressfaktoren wie finanzielle Schwierigkeiten, Krankheiten oder negative private Veränderungen außerhalb der Arbeitswelt hinzu, können die beruflichen Stressfaktoren (Ärger mit dem Vorgesetzten, drohende Entlassung oder unerfüllte Erwartungen) weiter verstärkt werden. In jedem Fall festigt sich so eine verstimmte Grundhaltung, die in der Regel mehr und mehr offensichtlich zu Tage tritt. Interessant ist dabei die Umkehr der Wertewelt aus der Perspektive des Innentäters:
    - Falsches Benehmen und Vorteilsnahme werden als lohnend eingestuft, harte Arbeit nicht.
    - Kollegen wollen einem eher schaden und müssen besiegt werden, so wie das ganze Unternehmen, das die eigenen Interessen nicht schützen will.
    - Offensichtlicher Ärger schlägt um in das Gefühl, provoziert zu werden und nun quasi zum Handeln gezwungen zu sein.
- Laut begleitender empirischer Forschung der ABPP-Wissenschaftler (American Board of Professional Psychology) ist der klassische Innentäter:
    - Männlich,

[18] Buroh, Dennis (31.03.2017): „So wird man zum Innentäter“. In Computerwoche - Voice of digital von IDG. URL: **https://www.computerwoche.de/a/so-wird-man-zum-innentaeter,3330434** (Stand: 23.08.19).

- 37 Jahre alt und
- hat eine technische Position inne (Ingenieur, Wissenschaftler, Manager oder Programmierer).
- Die Mehrheit dieser Täter hat Vereinbarungen in Sachen geistiges Eigentum unterschrieben.

• Als Handlungsmuster beschreibt er:
- Data Leakage,
- Social Engineering,
- Sabotage

und hebt das unbeabsichtigte Fehlverhalten von Mitarbeitern als meistgenannten Grund hinter "erfolgreichen" Hackerangriffen hervor.[19]

• Sein Fazit in Bezug auf die erforderliche Unternehmenssicherheit:

• Compliance-Richtlinien alleine reichen nicht aus, um Innentäter beziehungsweise Hacks und Angriffe durch diese zu verhindern. Klare Verhaltensregeln - auch im Umgang von Kollegen und Führungskräften untereinander - sowie geeignete, interne Kontrollsysteme sind zusätzlich unabdingbar.

• Die größte Herausforderung für die IT-Sicherheit bleibt die (frühzeitige) Erkennung krimineller oder schädlicher Aktivitäten. Allerdings kann bereits das einfache Monitoring von Mitarbeiteraktivitäten auf kritischen Systemen bei einem Sicherheitsvorfall die Kapazitäten der IT-Security-Abteilung sprengen. Zudem kann ein solches Vorgehen bei den überwachten Mitarbeitern zu großem Unmut führen, da ihre gesamte Arbeitsleistung unter Generalverdacht steht. Ein generelles Aufzeichnen aller Aktivitäten des Mitarbeiters - ohne dass dabei eine konkrete Gefahr für das Unternehmen besteht - verstößt gegen das Computergrundrecht.

• Der Versuch, IT-Sicherheit nur mit technischen Mitteln zu erreichen, ist sehr wahrscheinlich zum Scheitern verurteilt. Durch das Outsourcing von Abteilungen oder Dienstleistungen sinkt diese Wahrscheinlichkeit noch einmal. Denn weitere neue und ungeschulte Personen, die in die IT-Sicherheit einbezogen werden müssen, eröffnen zusätzliche Schwachstellen und Fehlerquellen im Unternehmen. Im Umgang mit kritischen Systemen und im IT-Sicherheitsmanagement ganz allgemein nimmt der Faktor Mensch die Hauptrolle ein.

• Unternehmen sollten sich in jedem Fall aktiv mit dem Thema Innentäter auseinandersetzen. Ein einfaches Monitoring oder Fokussieren auf Log-Files ist hier nicht ausreichend und vermittelt darüber hinaus allzu oft ein falsches Gefühl von Sicherheit. Ein schlichtes Log-File-Management-Monitoring bildet zudem keinen kompletten Nachweis zur Sicherstellung der EU-Datenschutz-Grundverordnung dar. Eine komplette Prozessabbildung durch Applikations-Log-Files wird nie möglich sein, zumal nicht sämtliche Prozessschritte der Anwender in einer einzelnen Applikation durchgeführt oder angezeigt werden können.

• Durch aktive Schulungsmaßnahmen für die Mitarbeiter werden mögliche Fehlerquellen minimiert. Gleichzeitig erlaubt dieses Vorgehen eine Protokollierung der Mitarbeiter-Aktivitäten

[19] Vgl. URL: **https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/cybersicherheitslage/umfrage2015_ergebnisse.pdf?__blob=publicationFile&v=4.** Sowie: **http://www.computerwoche.de/a/kriminelle-hacker-unterschaetzte-gefahr.** Quellenangabe Buroh: **https://www.computerwoche.de/a/so-wird-man-zum-innentaeter,3330434,** S. 8.

in der Produktionsumgebung. Beim Monitoring sollte weiterhin immer auf die Erfassung von Metadaten geachtet werden, so dass eine schnelle Auswertung und Datensparsamkeit gemäß BDSG gewährleistet werden kann. Die Kombination von Schulungs- und Monitoring-Applikationen ist somit ausdrücklich zu empfehlen.

Bewertung: Das Ziel der Sensibilisierung wird mit diesem Artikel erreicht, sowie die eindringliche Erkenntnis, dass ein Schutzkonzept, ohne Einbeziehung des Faktors Mensch, defizitär bleibt. Für den schnellen Überblick ist dieser Artikel daher zu empfehlen. Die vorgeschlagenen Maßnahmen konzentrieren sich im Wesentlichen allerdings auf Schwächen und Defizite und es werden wenige konkrete, praxisnahe und erfolgversprechende Handlungsempfehlungen gegeben. Beim eher „unerfahrenen" Leser, der sich vielleicht das erste Mal mit der Thematik beschäftigt, könnte daher ein Gefühl der Verunsicherung zurückbleiben. An dieser Stelle müsste dann weitere, konkrete Literatur bzw. Beratungsleistung eingeholt werden.

4.2.3 Dirk Fleischer (2016): Wirtschaftsspionage: Phänomenologie – Erklärungsansätze – Handlungsoptionen. In: Veko-online – Vernetzte Kompetenz im Sicherheitsmanagement[20]

Gegenstand: Fleischer widmet in seinem Werk ein Kapitel dem Thema Innentäter. Dabei bietet er phänomenologische Aspekte zum Innentäter im Deliktsbereich Wirtschaftsspionage an. Er verwendet folgende Definition:

> ***Definition Innentäter***
>
> *„Im Allgemeinen wird hierunter eine natürliche Person verstanden, die aufgrund eines Beschäftigungsverhältnisses besondere Kenntnisse und/oder Fertigkeiten besitzt, durch die sie unmittelbaren oder mittelbaren Zugang zu unternehmensbezogenen Informationen oder Prozessen hat, die einem außerhalb des Unternehmens stehenden Täterkreis nicht oder nur unter erheblichen Schwierigkeiten zur Verfügung stehen."*

Er unterscheidet zwischen Innentätern im engeren Sinn und Innentätern im weiteren Sinn. Innentäter i. e .Sinn sind Mitarbeiter, die in einem andauernden Beschäftigungsverhältnis stehen oder erst kürzlich aus diesem ausgeschieden sind. Zu Innentätern i. w. Sinn zählt er externe Beschäftigte, wie Subunternehmer, Dienstleister, Lieferanten oder Berater.

Ziel: Umfassende Betrachtung des Phänomens Wirtschaftsspionage, wobei die Innentäterschaft einen Aspekt darstellt.

Forschungsfrage: Welche Bedeutung hat der Innentäter im Deliktsfeld Wirtschaftsspionage? Eigene empirische Daten werden hierzu nicht erhoben (Sekundäranalyse).

Ergebnisse:

[20] Dirk Fleischer (2016): „Wirtschaftsspionage: Phänomenologie – Erklärungsansätze – Handlungsoptionen". Springer Vieweg 2016. ISBN: 978-3-658-11988-1 (Print) 978-3-658-11989-8 (Online). Zitiert nach veko-online – Vernetzte Kompetenz im Sicherheitsmanagement, Kap. 1.3 Der Innentäter. URL: **https://www.veko-online.de/archiv-ausgabe-02-2016/687-kriminologie-wirtschaftsspionage.html**. Stand: 23.09.19.

- Die Motive des Innentäters können ideologisch oder egoistisch sein. Nach Auffassung des Autors spielt die ideologische Überzeugung von Innentätern in diesem Deliktsfeld nur in seltenen Fällen eine entscheidende Rolle. Die egoistische Vorteilsnahme sei das überwiegende Motiv. Anders ist dies bei durch staatliche Stellen eingeschleusten Praktikanten, Wissenschaftlern, Studenten oder Agenten unter sog. Legende.

- Das Phänomen der Wirtschaftsspionage zu beschreiben ist anspruchsvoll und aufgrund der lückenhaften Datenlage kaum möglich. Ernsthafte Erkenntnisse über Fallzahlen, Täter, also auch Innentäter, tatsächliche Schäden etc. fehlen. Dieser Umstand ist überwiegend anerkannt und muss geändert werden.

- Einigkeit besteht weitestgehend darüber, dass der Innentäter, sei es nun im engeren oder weiteren Sinne ein exponiertes Gefahrenpotential darstellt. Er verfügt über Insiderwissen, das der außenstehende Täter nicht oder nur schwerlich erlangen könnte.

- Vieles spricht dafür, dass es sich bei der Wirtschaftsspionage durch Innentäter um Wirtschaftskriminalität handelt. Aus dieser Grundannahme heraus sind sowohl die rechtlichen, als auch die kriminologischen Theorien für die staatliche Wirtschaftsspionage und die wirtschaftliche Wirtschaftsausspähung bei der Betrachtung des Gesamtphänomens zu berücksichtigen.

- Im Rahmen einer unternehmerischen Risikovorsorge lassen sich Indikatoren erarbeiten, nach denen ein zielorientiertes Risikomanagement zur Vermeidung von Informationsabfluss durch Innentäter etabliert werden kann. Die Unternehmen sind aufgrund der wirtschaftlichen Indikationen aufgefordert, Vorsorge zu leisten. Entscheidend ist, ein solches System im Einklang mit arbeitsrechtlichen und moralisch-ethischen Überlegungen zu konstruieren.

Bewertung: Wesentliche Aspekte zur Innentäterschaft werden fundiert und gut recherchiert in das Deliktsfeld Wirtschaftsspionage eingebettet.

5 Fazit

Die Recherche hat gezeigt, dass das Thema „Innentäter“ im wissenschaftlichen Diskurs aktuell eher wenig zur Sprache kommt. Konkrete und aktuelle Informationen zur Thematik bieten die Studien des Digitalverbandes Bitkom und der verschiedenen Unternehmensberatungen, die die aktuellen Probleme und Herausforderungen der Unternehmen zeitnah aufgreifen und in (Dunkelfeld-) Befragungen untersuchen. Daneben verfügen das Bundesamt für Verfassungsschutz und die Landesämter für Verfassungsschutz im Bereich Wirtschaftsschutz über eine fundierte Expertise. Sowohl im persönlichen Beratungskontakt, auf Fachtagungen als auch in einschlägigen Veröffentlichungen, Broschüren und Flyern findet man dort umfassende und praxisnahe Informationen.

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, Wirtschaftsspionage, Cybercrime etc. zusammengesucht werden müssen. Es besteht Forschungsbedarf bezüglich Hellfeldanalysen und einer spezifischen wissenschaftlichen Betrachtung des Phänomens.

5.1 Wer sind die Innentäter?

Ein typisches Profil des „einen“ Innentäters gibt es nicht. Die Tätertypen können sehr unterschiedlich sein und müssen im Einzelfall betrachtet werden. Dies wird besonders deutlich, wenn man aus den analysierten Berichten die herausgearbeiteten Tätermerkmale übersichtsartig zusammenfasst. Danach könnte fast jeder Mitarbeiter zum Täter werden:

- Meist männliche und im Unternehmen respektierte Personen.
- Zwischen 30 und 60 Jahren alt.
- Meist 6 - 20 Jahre im Unternehmen (mit zunehmender Unternehmenszugehörigkeit sinkt die Schadenshäufigkeit, aber die verursachten Schäden steigen).
- Meist mittleres bis Top-Management – bei bestimmten Delikten (z.B. Diebstahl) auch ohne Führungsverantwortung.
- Meist höher gebildet (z.B. bei Korruption, Geldwäsche und Wettbewerbsdelikten), je nach Delikt auch eine niedrigere Bildung (z.B. Betrug, Untreue).

5.2 Welche Situationen und Indikatoren können kritisch für einen möglichen Schadensfall durch Mitarbeiter sein?

- Outsourcing-Situationen.
- Generelle Zusammenarbeit mit Lieferanten.
- Kundengewinnung.
- Freisetzung von Mitarbeitern (erzwungen oder geplant).
- Zulassung/ Zertifizierung von Produkten (insbes. in Schwellenländern).
- Hohe Marktmacht von Kunden.
- Alleinbearbeitung von Sachverhalten durch einen Mitarbeiter, zu große Machtfülle.
- Unzufriedenheit am Arbeitsplatz.
- Auffällige Neugier.
- Versuch der Erweiterung oder Überschreitung der Zugriffsberechtigungen.
- Verdächtige Kontakte zu ausländischen Staaten oder Konkurrenzunternehmen.
- Regelwidriges Einbringen und Nutzen mobiler Endgeräte oder Datenträger.
- Ungewöhnliche Arbeitszeiten.
- Diskrepanzen im beruflichen Werdegang.

5.3 Welche Erscheinungsformen gibt es?

Die Typologie des Innentäters weist eine Bandbreite von vorsätzlichem, bewusstem Täterverhalten auf, über ein zunächst ungeplantes, unbewusstes Handeln, das später in die Vorsätzlichkeit kippen kann, bis hin zu gänzlich ungeplantem, unbewusstem Handeln.

- Unbewusstes Täterhandeln - Beispiele:
  - Der Mitarbeiter wird Opfer eines klassischen oder digitalen Social Engineering-Angriffs (z.B. CEO-Fraud).
  - Der Mitarbeiter missachtet aus Unkenntnis, Sorglosigkeit oder Fahrlässigkeit wichtige Sicherheitsregeln des Unternehmens (regelwidriges Verhalten) und löst damit einen Schadensfall aus.
- Zunächst unbewusstes Täterhandeln, das in vorsätzlichem Handeln mündet - Beispiele:
  - „Anfüttern" eines Mitarbeiters durch einen externen Täter (z.B. bei Korruption). Nachdem der Mitarbeiter seine Verstrickung in eine Straftat bemerkt, verweilt er in der kriminellen Verstrickung anstatt sich zu offenbaren.
  - Anwerben eines (zunächst ahnungslosen) Mitarbeiters in einer attraktiven Funktion als (dauerhafte) Quelle im Rahmen der klassischen Wirtschaftsspionage.
- Vorsätzliches, bewusstes Täterhandeln - Beispiele: Der Mitarbeiter „sammelt" oder verschafft sich Informationen, um z.B.:
  - seine Arbeitsziele schneller und erfolgreicher zu erreichen und damit Boni zu erhalten, sich gegen Konkurrenten abzusetzen oder schneller befördert zu werden.
  - Selbstbestimmtheit, Freiheit und Macht für den eigenen Arbeitsplatz auszubauen.
  - sie bei einem späteren Arbeitgeberwechsel zu nutzen.
  - sie in einem Konfliktfall gegen den Arbeitgeber einzusetzen.
  - sie gezielt an Mitbewerber, Nachrichtendienste oder andere Interessierte zu verkaufen oder sie aufgrund einer erlittenen Frustration weiterzugeben.
  - Sabotageakte/ Racheakte (IT-Manipulationen, physische Beschädigung oder Zerstörung von Sachmitteln) durchzuführen.

5.4 Warum wird ein Mitarbeiter zum Innentäter?

Wird ein Mitarbeiter zum Innentäter, kann dies, neben dem finanziell oder materiell erhofften Vorteil, verschiedene Beweggründe haben. Z.B. persönliche oder persönlichkeitsbezogene Motive wie:

- Streben nach Anerkennung, Respekt, Verbesserung der sozialen Stellung oder Freundschaft.
- Überzeugungen politischer, kultureller oder religiöser Art.
- Eine ich-zentrierte Persönlichkeit (z.B. Wichtigtuerei, Geltungsbedürfnis, Eitelkeit bis hin zu stark ausgeprägten Persönlichkeitsstrukturen wie Narzissmus, niedrige Sozialverträglichkeit, Rücksichtslosigkeit, Tendenzen zur Täuschung, Nicht-Einhaltung von Regeln).
- Niedrige Hemmschwelle und Mangel an Unrechtsbewusstsein.

- Psychische Ängste oder Druckaufbau durch Externe (z.B. Erpressung).
- Soziale Ängste (z.B. Arbeitsplatzverlust oder sozialer Abstieg).
- Frustration/ Wut/ fehlende Identifikation mit dem Unternehmen
- Gründung eines Konkurrenzunternehmens.

Weitere Ursachen können im Arbeitskontext verhaftet sein. So kann sich bei einem Mitarbeiter bspw. Unzufriedenheit, Neid, Missgunst, Frustration aufgrund einer Stagnation der eigenen Karriere oder aufgrund schlechter Mitarbeiterführung aufgebaut haben. Auch eine „günstige Situation" oder „günstige Gelegenheit" z.B. durch fehlende interne Kontrollen kann zur Innentäterschaft führen. Ebenfalls die Falscheinschätzung einer Situation, fehlende Schulungen am Produkt oder Unkenntnis über Arbeitsprozesse.

5.5 Welche Maßnahmen kann das Unternehmen ergreifen?

Ein ganzheitliches Konzept zur Verhinderung von Innentäterschaft erfordert eine umfassende Prävention, etablierte Sicherheitsprozesse und ausreichende Detektionsmöglichkeiten. Es umfasst als wesentliche Bausteine: Risikoanalyse, Informationsklassifizierung, materiellen Know-how-Schutz, Need2Know-Prinzip, Pre-Employment-Screening, Security-Exit-Management, Awareness und Security-Kultur durch Schulungen, Konsequenzmanagement und Vorbildfunktion der Führungskräfte. Folgende Maßnahmen wurden aus den ausgewerteten Veröffentlichungen zusammengestellt:

- Benennung eines Sicherheitsverantwortlichen.
- Bestimmung und Klassifikation essentieller Werte und Informationen auf Grundlage einer Risikoanalyse.
- Konsequente Durchführung von Risikobewertungen hinsichtlich der Aufgaben, die fremdvergeben werden können oder nicht.
- Eine auch auf Security-Kriterien gestützte Selektion der Geschäfts- und Kooperationspartner.
- Definition und Identifikation von Situationen, in denen ein ungewollter Wissenstransfer/ Verlust von Vermögenswerten stattfinden kann (z.B. Konzept zur Detektion und Unterbindung unerwünschter Aktionen der Informationssicherheit und des Datentransfers durch Mitarbeiter, Security Trainings, eingehende Prüfung der gesamten Lieferkette und eventuelle Forderungen an den Lieferanten bspw. in Bezug auf ein Compliance-Management-System).
- Erstellung eines umfassenden Sicherheitskonzeptes inklusive Berechtigungsmanagement (eventuelle Systemschwachstellen und IT-Komponenten überprüfen und verbessern, Zugangs- und Zugriffkontrollen) sowie dessen regelmäßige Fortschreibung.
- Eine durch Hintergrundprüfung abgesicherte Personalauswahl (Pre-Employment-Screening von Bewerbern auf kritische Funktionen) und sicherheitsorientierte Besetzung von Schlüsselpositionen.
- Etablieren eines Ausstiegsmanagement (z. B. Freisetzungsbelehrung, zeitnahe Sperrung aller Zugriffsberechtigungen).
- Stringente Zugangskontrollen nach dem Need-to-Know, Need-to-See und Need-to-Go Prinzip.

- Förderung der Identifikation der Mitarbeiter mit dem Unternehmen (gute Arbeitsbedingungen und eine Vertrauensbasis schaffen, den Mitarbeiter an das Unternehmen binden durch finanzielle Anreize, interessanter Aufgaben).

- Adäquates Führungsverhalten (u.a. Interesse für die Belange und Sorgen der Mitarbeiter, Wertschätzung, Entscheidungsteilhabe bzw. ausreichende Information, Unterstützung von Mitarbeitern in persönlichen Krisen/ Notlagen oder Weiterleitung an professionelle Sozialberater). Ausbildung und Erweiterung von Soft Skills.

- Kontinuierliche Sensibilisierung und Schulung der Mitarbeiter für kritische Situationen.

- Klares Artikulieren von Unternehmensrichtlinien und ethischen Werten.

- Vier-/oder Mehr-Augen-Prinzip.

- Detektion kritischer Verhaltensindikatoren von Mitarbeiter.

- Einrichtung von Meldestellen für Mitarbeiter (Hinweisgebersystem).

- Konsequente Durchführung interner Ermittlungen.

- Verhängung von wirksamen und abschreckenden Maßnahmen im Schadensfall.

- Regelmäßige Evaluation und Weiterentwicklung des Schutzkonzeptes.

Mitarbeiter sind immer Teil der Unternehmenssicherheit.

Entweder als Sicherheitsgarant oder als Sicherheitsrisiko.

Falls Sie im Rahmen des Wirtschaftsschutzes Unterstützung wünschen, wenden Sie sich an das Bundesamt für Verfassungsschutz, die Landesämter für Verfassungsschutz oder die Polizei und zeigen Sie Schadensfälle an.

Impressum

Herausgeber
Bundeskriminalamt
Kriminalistisches Institut
65173 Wiesbaden

Stand
Monat 20xx

Gestaltung & Bildnachweis
Bundeskriminalamt

Nachdruck und sonstige Vervielfältigung, auch auszugsweise,
nur mit Quellenangabe des Bundeskriminalamtes