Innentäter in Unternehmen – Gefahr der Vergangenheit oder stetige Bedrohung?

Kurzfassung einer Zusammenstellung inländischer Forschungsbeiträge zum Forschungsstand und Handlungsempfehlungen bzgl. Innentäterschaft

Das Schadenspotenzial für Unternehmen durch Innentäter stellt, insbesondere im Zuge der zunehmenden Bedrohung durch das Tatmittel Internet, eine spezielle Bedrohung dar. 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 [1] innerhalb von Suchportalen, Internetseiten von Forschungsinstituten und Lehrstühlen sowie Internetpräsenzen einzelner Behörden und Unternehmen nach Veröffentlichungen externer nationaler Forschungsbeiträge recherchiert. Das Ziel des 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.

Die grundlegende Schwierigkeit bei der Darstellung des Forschungsstandes ist, dass die Informationen zu Innentätern nicht „gebündelt“ in speziellen Studien vorliegen, sondern in den vielfältigen Publikationen zur Wirtschaftskriminalität zusammengesucht werden müssen. 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. Aus den analysierten Berichten lassen sich u.a. (Motive und Charakteristika der Innentäter werden im Gesamtbericht aufgeführt) folgende wesentliche Aspekte zusammenfassen:

Welche Situationen können kritisch für einen Informationsabfluss durch Mitarbeiter sein?

- Outsourcing-Situationen

[1] 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

- 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

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[2],
- 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[3]). 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. 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.

Der Gesamtbericht zur Thematik Innentäter in Unternehmen kann auf der Kommunikationsplattform Wirtschaftsschutz unter www.wirtschaftsschutz.info eingesehen werden.

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