

Wie bei jeder statistischen Annäherung an eine Thematik sind auch in diesen konkreten Beispielen immer das Gesamtbild und die zugrunde liegende Datenlage zu betrachten. Anhand einer einzelnen Statistik lässt sich nicht direkt auf andere Fragestellungen schließen. Aussagen, die in einem speziellen Kontext erfasst und ausgewertet wurden, halten deswegen in der Regel selten einer Pauschalisierung stand.

1.4 Innentäter vs. Außentäter

Angriffe können von verschiedenen Ursprungsorten kommen. Der Täter kann sich sowohl außerhalb des angegriffenen Netzwerks befinden als auch innerhalb des eigenen Verantwortungsbereichs. Beide Ursprungsorte bieten bei der Ermittlung der möglichen Täter Vor- und Nachteile. Es gibt zwar Statistiken über das Verhältnis von Innentätern zu Außentätern, diese sind aber wegen der zu erwartenden Dunkelziffer kritisch einzuschätzen.

Durch die zunehmende Vernetzung der Informationstechnik hat sich die potenzielle Gefährdung stärker in Richtung auf den ortsunabhängigen Außentäter verlagert. Recht einfache Mittel wie ein PC und ein Internetzugang und geringes Fachwissen reichen aus, um ein Computersystem empfindlich zu stören.

Außentäter

Dennoch geht aufgrund des Wissens um die internen Informationsflüsse und vorhandener Insider-Informationen weiterhin eine sehr große Gefahr von Innentätern aus. Dies wird häufig durch mangelnde interne Schutzmechanismen begünstigt. Dem Innentäter wird es oft leicht gemacht, da in den wenigsten Fällen im internen Netz verschlüsselt wird oder wichtige Systemkomponenten ausreichend gehärtet sind. Zusätzlich sind die internen Überwachungs- und Protokollierungsmöglichkeiten aus verschiedenen Gründen nicht geeignet, auffälliges Verhalten frühzeitig aufzuklären oder einen erfolgten Angriff zu erkennen.

Innentäter

Der Gesamtverband der deutschen Versicherungswirtschaft (GdV) geht davon aus, dass etwa 40 % der Betrugs-, Diebstahls- und Unterschlagungsdelikte⁹ von den Mitarbeitern der betroffenen Unternehmen begangen werden¹⁰. Im Jahr 2002 entstanden laut GdV deutschen Firmen auf diese Weise Schäden in Höhe von rund 3 Milliarden Euro. In dieser Statistik ist allerdings nicht ausschließlich die Mitarbeiterkriminalität erfasst, die durch Computermissbrauch gekennzeichnet

9. Ein Delikt (lat. = Vergehen) ist ein rechtswidriges, schuldhaftes Verhalten, das im Zivilrecht grundsätzlich mit Schadensersatzpflicht, im Strafrecht mit Straffolge verknüpft ist.

10. <http://www.gdv.de/presseservice/21725.htm>

ist, sondern auch alle anderen Formen krimineller Handlungen wie Korruption und Vorteilsnahme, Untreue, Unterschlagung, Diebstahl, Betrug, Wirtschafts- und Betriebsspionage, Verrat von Betriebsgeheimnissen, Erpressung und Insider-Geschäfte. Es ist dabei aber zu bedenken, dass höchstwahrscheinlich bei einer Vielzahl dieser Delikte Computersysteme unterstützend oder begünstigend beteiligt waren. Laut Aussage des GdV besitzen die Täter meist betriebswirtschaftliches Fachwissen sowie gute Kenntnisse der internen organisatorischen Abläufe und Gewohnheiten des geschädigten Unternehmens.

Die Betrachtung der Innentäterproblematik darf nicht nur auf die eigenen Mitarbeiter isoliert werden. Vielmehr ist dabei einzubeziehen, dass zu diesem Täterkreis alle mit erweitertem internem Know-how ausgestatteten Personengruppen gehören. Hierzu zählen dann auch Geschäftspartner, Lieferanten, externe Dienstleister und eben auch Kunden.

Eine Statistik der Euler Hermes Kreditversicherungs-AG von 9.000 versicherten Vertrauensschäden (wieder nicht nur ausschließlich Computermisbrauch), die Alter, Geschlecht und Betriebszugehörigkeit der Täter erfasst, zeigt¹¹:

- Etwa zwei Drittel der Täter waren männlich, ein Drittel weiblich.
- Mit zunehmendem Alter sinkt die Schadenshäufigkeit. 35 % der Schäden wurden von Mitarbeitern unter 30 Jahren verursacht. 30 % waren zwischen 30 und 40 Jahren alt, 23 % zwischen 40 und 50 Jahren. Nur etwa 12 % der Schäden gehen auf Mitarbeiter über 50 Jahre zurück.
- Je länger die Betriebszugehörigkeit, desto seltener die Veruntreuung: Die höchste Dichte von Veruntreuungen liegt in den ersten zwei Jahren der Betriebszugehörigkeit, während sie ab 20-jähriger Beschäftigung im gleichen Unternehmen minimal ist.
- Es war weiterhin zu erkennen, dass gerade die von langjährigen Mitarbeitern verursachten Schäden oft sehr hoch sind.

Für das Jahr 2006 geht Euler Hermes davon aus, dass ein Vermögensschaden von ca. 1,5 Milliarden Euro entstanden ist. Dies übersteigt die Schäden, die im gleichen Zeitraum durch Brandschäden verursacht wurden, um ungefähr eine halbe Milliarde Euro.

Im Jahre 2010 führte die KPMG AG Wirtschaftsprüfungsgesellschaft eine Umfrage zur »Computerkriminalität in der deutschen Wirtschaft« durch¹². Demzufolge war jedes vierte der befragten Unterneh-

11. Euler Hermes Kreditversicherungs-AG, Hamburg, 2003, »Wirtschaftskriminalität – das diskrete Risiko«
(<http://www.eulerhermes.de/imperia/md/content/ger/dt/20.pdf>)

men bereits Opfer von Computerkriminalität. Häufigstes Delikt war der Diebstahl von Kunden- oder Arbeitnehmerdaten. 61 % der von Computerkriminalität betroffenen Unternehmen waren in den vergangenen drei Jahren Opfer von Datenraub. Ein weiteres hohes Risiko ist mit dem Diebstahl von geschäftskritischem Know-how verbunden: Jedes zweite Unternehmen (52 %) war davon betroffen. Laut dieser Umfrage kamen bei fast der Hälfte der geschädigten Unternehmen die Täter aus dem eigenen Haus. In 24 % der Fälle waren es sonstige Insider. Insbesondere folgende Delikte verübten Mitarbeiter:

- Datendiebstahl bzw. Verletzung von Geschäfts- und Betriebsheimnissen (jeweils 62 %),
- Erpressung (60 %),
- Manipulation von Finanzdaten (58 %) und
- Betrug (55 %).

Unbekannte Externe sind an 47 % der Computerkriminalitätsdelikte beteiligt. Sie sind vor allem verantwortlich für Wirtschaftsspionage (70 %), für die Verletzung von Schutz- und Urheberrechten (56 %), für Computersabotage (ebenfalls 56 %) oder für das Ausspähen bzw. Abfangen von Daten (55 %).

Über diese Zahlen kann man sicherlich wie bei jeder Statistik diskutieren. Es ist aber als Tatsache anzusehen, dass die steigende Anonymität in großen Unternehmen und die zunehmende Angst der Arbeitnehmer vor Jobverlust zu einer Änderung in der Einstellung zu den Werten eines Unternehmens geführt haben. Unübersichtliche Unternehmensstrukturen – oft infolge von häufigen Umstrukturierungen oder Fusionen bzw. Firmenübernahmen – erleichtern es potenziellen Tätern zusätzlich, Lücken auszunutzen und dabei unerkannt zu bleiben.

Diverse Studien, die sich mit Wirtschaftskriminalität beschäftigen, zeichnen auch hier ein bemerkenswertes Bild^{12, 13}. Auf Basis von Betroffenenbefragungen wird darin beispielsweise davon ausgegangen, dass jedes zweite deutsche Unternehmen von Korruption oder ähnlichen Delikten betroffen ist. Wenn man sich dann noch vor Augen hält, dass für fast alle wichtigen Geschäftsprozesse (bei denen auch Geldflüsse zu verzeichnen sind) informationstechnische Systeme zum Einsatz kommen, ist es jedem Betrachter klar, dass hier mit Computerforensischen Methoden zu ermitteln ist. Sobald die Täter beispielsweise Mail- bzw. Webtechnologien einsetzen oder einfach nur mit ihrem Mobiltelefon Informationen austauschen, sind digitale Spuren

12. KPMG e-Crime Studie 2010, <http://www.kpmg.de/Themen/21481.htm>

13. Weitere Studien von PWC und KPMG zu Themengebieten der allgemeinen Wirtschaftskriminalität

zu finden, die es zu analysieren und auszuwerten gilt, auch wenn der Schaden eventuell durch einen Nicht-IT-Prozess verursacht wurde.

Ein weiterer Aspekt der Innentäterproblematik ist, dass jemand mit ausreichend Prozess- oder Firmenwissen ohne aufwendiges Hacken erheblichen Schaden anrichten kann. Auch aus technischer Sicht regelkonformes Verhalten kann eine Computer-forensische Analyse nach sich ziehen, wenn gegen interne Richtlinien verstoßen wurde. Dies kann selbst der »normale« Einsatz eines Mail- oder Webclients sein, wenn damit eine Straftat oder strafvorbereitende Handlung bzw. andere Delikte begangen werden.

1.5 Bestätigung durch die Statistik?

*Die Polizeiliche
Kriminalstatistik*

Das Bundeskriminalamt (BKA) veröffentlicht jährlich die Polizeiliche Kriminalstatistik (PKS). In der Polizeilichen Kriminalstatistik werden die von der Polizei bearbeiteten Straftaten registriert. Taten, die außerhalb der Bundesrepublik Deutschland begangen wurden, werden nicht berücksichtigt.

*Nur abgeschlossene
Verfahren*

Der Erfassung liegt ein unter teils strafrechtlichen, teils kriminologischen Aspekten aufgebauter Straftatenkatalog zugrunde. Bundeseinheitlich wird seit dem 1.1.1971 eine »Ausgangsstatistik« geführt, d.h., die bekannt gewordenen Straftaten werden erst nach Abschluss der polizeilichen Ermittlungen vor Aktenabgabe an die Staatsanwaltschaft erfasst. Seit 1993 ist es eine gesamtdeutsche Statistik. Das Zahlenmaterial wird von den Landeskriminalämtern in aggregierter Form dem Bundeskriminalamt übermittelt und dann zur Polizeilichen Kriminalstatistik zusammengefasst. Das BKA schätzt die PKS allerdings selbst kritisch ein, da ihre Aussagekraft dadurch eingeschränkt wird, dass der Polizei nicht alle Straftaten bekannt werden. Daraus können sich natürlich Abweichungen im Verhältnis zwischen erfassten und wirklich begangenen Straftaten ergeben¹⁴.

Das BKA geht bei der PKS bereits von statistikbeeinflussenden Faktoren aus. Dazu gehören

- das Anzeigeverhalten (z.B. Versicherungsaspekt),
- die polizeiliche Kontrolle,
- die statistische Erfassung,
- die Änderung des Strafrechts
- und die echte Kriminalitätsänderung.

14. BKA, PKS 2010, 3.21 »Computerkriminalität«, Seite 236
(<http://www.bka.de/pks/pks2010/>)