iX-Edition

# Computer-Forensik

Computerstraftaten erkennen, ermitteln, aufklären

Bearbeitet von
Alexander Geschonneck

6., aktualisierte und erweiterte Auflage 2014. Buch. 388 S. Kartoniert
ISBN 978 3 86490 133 1
Format (B x L): 16,5 x 24 cm

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.

*Außentäter*

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.

*Innentäter*

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.

Der Gesamtverband der deutschen Versicherungswirtschaft (GdV) geht davon aus, dass etwa 40 % der Betrugs-, Diebstahls- und Unterschlagungsdelikte[9] von den Mitarbeitern der betroffenen Unternehmen begangen werden[10]. 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 Computermissbrauch), die Alter, Geschlecht und Betriebszugehörigkeit der Täter erfasst, zeigt[11]:

- 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 2013 führte die KPMG AG Wirtschaftsprüfungsgesellschaft eine Umfrage zur »Computerkriminalität in der deutschen Wirt-

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

schaft« durch[12]. Demzufolge war jedes vierte der befragten Unternehmen bereits Opfer von Computerkriminalität.

Mehr als 80 Prozent der befragten 500 Unternehmen sehen für die Gesamtwirtschaft ein hohes bis sehr hohes Risiko, in Computerkriminalitätsvorfälle involviert zu werden. Zwei Drittel der Unternehmen erwarten sogar eine Zunahme der ernsten Bedrohungslage innerhalb der nächsten zwei Jahre.

Paradox ist hierbei jedoch, dass nur knapp ein Drittel der befragten Unternehmen das Risiko, mit dem eigenen Unternehmen von e-Crime betroffen zu sein, als hoch bis sehr hoch einschätzt. Demzufolge haben in der Risikowahrnehmung der Befragten also eher die anderen Unternehmen ein Problem. Von den betroffenen Unternehmen wurden Computerbetrug und Ausspähen oder Abfangen von Daten als häufigste Deliktstypen genannt.

Die mobile Telekommunikation und die Nutzung von mobilen Datenträgern werden als bedeutsamste Gefahrenquellen gesehen. Die zunehmende Verbreitung komplexer Technologien im Zuge der mobilen Telekommunikation bereitet somit die Angriffsmöglichkeiten für die komplexeren Deliktstypen. Die Angreifer werden dabei professioneller und führen die Angriffe zunehmend gezielt auf bestimmte Geschäftsbereiche oder Daten hin aus. Die Gefahrenquellen für e-Crime werden inzwischen vermehrt länderspezifisch gesehen, die größten Gefahren werden mit China, Russland und dem übrigen Osteuropa verbunden.

Bei den tatsächlichen Tätern besetzen die unbekannten Externen die vorderste Position. Es bleibt jedoch festzuhalten, dass die überführten Täter oft im unmittelbaren Umfeld zu finden sind.

Die Vorstudie aus dem Jahr 2010 ergab noch, dass die Personengruppe, die als besonders risikobehaftet wahrgenommen wurde – aktuelle oder ehemalige Mitarbeiter des Unternehmens – auch tatsächlich mehrheitlich dem Täterkreis bei Computerkriminalität entsprach. Inzwischen zeigt sich ein verändertes Bild. Es rangieren gemäß der aktuellen Version der KPMG-Studie die ehemaligen Mitarbeiter oder Insider, die ihr Wissen um Schwachstellen vorsätzlich missbrauchen, nach wie vor ganz oben. Bei den tatsächlichen Tätern besetzen die unbekannten Externen jedoch nun die vorderste Position, gefolgt von Mitarbeitern der betroffenen Abteilung, Kunden sowie sonstige Geschäftspartner. Beim Delikt »Verletzung von Geschäfts- und Betriebsgeheimnissen« wurden allerdings mehrheitlich die Mitarbeiter der betroffenen Abteilung als Täter identifiziert. Dies ist eigentlich auch

12. KPMG e-Crime Studie 2013, *http://www.kpmg.de/Themen/36096.htm*

nachvollziehbar, da diese oft privilegierten Zugang zu diesen Geheimnissen haben. Als Fazit kann festgehalten werden, dass auch diese Studie Computerkriminalität als Instrument im wachsenden weltweiten Konkurrenzkampf sieht, da der finanzielle Vorteil der überführten Täter bei 96 % der betroffenen Unternehmen als Motivation festgestellt wurde.

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 beschäftigten, zeichnen auch hier ein bemerkenswertes Bild.[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 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.

13. Weitere Studien von PWC, KPMG und Ernst & Young zu Themengebieten der allgemeinen Wirtschaftskriminalität