# Der Spion, der mich nicht liebte

**Kriminalität durch Mitarbeiter im Unternehmen nimmt ständig zu.**
**Das gilt auch für Industriespionage, deren Schaden schnell zum GAU führen kann.**

Für die Geschäftsleitung einer Gold- und Silberscheideanstalt im Raum Pforzheim im Nordschwarzwald wurde im vorvergangenen Jahr ein Verdacht zur traurigen Gewissheit.
Ein Mitarbeiter des mittelständischen Unternehmens bediente sich wochenlang aus der hauseigenen „Goldgrube“ und schaffte insgesamt 54 kg Gold beiseite.
Selbst die installierte Videoüberwachung konnte den Goldjungen nicht abhalten, da diese nicht lückenlos alle Bereiche erfasste.

Mehr als einen satten Nebenverdienst hatten unbekannte Täter in einem Ingenieur-Büro innerhalb eines Schiffswerftgeländes bei Aschaffenburg im Sinn. Dort beendete man die dreijährige Entwicklungsarbeit für neuartige, luftgekühlte Dieselmotoren, indem man zwei Motoren samt Unterbau stahl. Im Gegensatz zu bisherigen wassergekühlten Einheiten hätte der neue Motor auch in Flachgewässern eingesetzt werden können, da dieser Antrieb keinen Schlamm ansaugt. Die Prototypen standen kurz vor der Patentanmeldung.

Vom Schlamm zum Schlamassel. Zum Beispiel in Form des Laptops. Klein, handlich und mit Informationen vollgestopft wie zuweilen das deutsche Schwein mit Antibiotika.
Sind sie ohnehin ein in den letzten Jahren begehrtes Stehlgut bei „normalen“ Wohnungs- und Büroeinbrüchen, mutiert die Tat schnell zum Fiasko, wenn Industriespionage Wurzel des Übels ist.
Eine Erfahrung, die zu Beginn diesen Jahres eine Firma für Zusammenbau von PC in der Nähe Dortmunds ereilte. Zwei Unbekannte fanden trotz fehlender Wegweiser und Türschilder in dem großen Gebäude zum Geschäftsführerbüro, wo sie ein betriebsbereites Laptop vom Netz trennten. Wertgegenstände im unmittelbaren Bereich ließen sie unbeachtet.
Auf der Festplatte waren höchstvertrauliche Firmendaten gespeichert, der Schaden wird auf etwa 1 Million Euro geschätzt.

Mit großem Sportsgeist wurde unlängst auch ein Vorstandsmitglied eines Pharmaunternehmens auf einem deutschen Flughafen erleichtert. Während er in einer Lounge seinen Aktenkoffer samt Firmenlaptop abgestellt hatte und in Zeitschriften blätterte, tauschten Unbekannte diesen gegen einen optisch identischen Koffer aus.
Statt seinem Laptop fand der gute Mann im Flugzeug Backsteine vor. Bad Business!

Diebstähle durch Mitarbeiter im eigenen Unternehmen nehmen ebenso zu wie Fälle von Industriespionage – sagen viele Experten. Zu trennen ist übrigens die Industrie- von der „Wirtschaftsspionage“, die eine *staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten* ausgehende Ausforschung von Unternehmen bedeutet.

Ein umfassendes Zahlenwerk hierzu existiert nicht. In dem durch das BKA veröffentlichten „Jahresbericht Wirtschaftskriminalität 2001“ sind 100 Taten des „Verrates von Geschäfts- und Betriebsgeheimnissen“ notiert. Weiter wird angeführt, dass „von einer hohen Dunkelziffer ausgegangen werden muss, die eine Quantifizierung des Schadens sehr erschwert“.
Kein Wunder, denn der von den betroffenen Unternehmen befürchtete Verlust von Image und Kunden steht meist nicht im Verhältnis zum erlittenen Schaden.

Dieses Lied kann Ansgar A. Huth sogar rückwärts singen. Als Sachverständiger für Datenschutz und Lauschabwehr ist er gefragt, gibt Seminare zum Thema. „Der Anteil der Unternehmen mit entsprechenden Schutzmaßnahmen schätze ich auf höchstens 20 %“, sagt der Experte und fügt hinzu, dass „dies auch für Großkonzerne gilt“.

Laut einem „Spiegel“-Bericht haben etwa 65-80 % aller Angestellten bereits die „innere Kündigung“ ausgesprochen. Im Rahmen der Globalisierung des Wirtschaftslebens, der zunehmenden Flexibilisierung des Arbeitsmarktes und des wachsenden Konkurrenzdrucks findet heute ein Arbeitsplatzwechsel häufiger als in früheren Zeiten statt. Die Verbundenheit zum Unternehmen schwindet. Sind zudem Betriebsklima und Mitarbeiterführung schlecht, steigt die Gefahr für kriminelle Handlungen.
Als besonders gefährdet hinsichtlich Industriespionage gelten die mittlere und höhere Führungsebene, sowie die Mitglieder von Unternehmensvorständen.

Dr. Jürgen Lieske, Risiko-Berater des Allianz-Zentrums für Technik GmbH, weiß von dem Risikopotential zu berichten. „Kriminalität im eigenen Unternehmen nimmt deutlich zu. Dies gilt besonders für die Industriespionage. Nehmen Sie nur als Beispiel in der Automobilbranche den Bereich der Kfz-Elektronik mit ihrer zunehmenden Abhängigkeit von Zulieferfirmen. Die Kontrolle des Unternehmens schwindet, ferner wird die Industrieversicherung zum Problem, weil die Haftungsfrage einem Wandel unterliegt“.

In der Automobilbranche redet man über dieses Thema genauso ungern wie eine Bundesregierung über Steuererhöhungen vor einer Wahl.
Ende des Jahres 2000 deckte die Unternehmenssicherheit von BMW eine Diebstahlserie in ihrem Forschungs- und Ingenieurszentrum auf. Mitarbeiter einer externen Firma entwendeten über einen längeren Zeitraum PC und PC-Komponenten aus dem Werk. Der Schaden betrug 800.000 DM.
Im Formel 1-Team Benetton-Renault war im vorletzten Jahr das Entsetzen groß, als Computer-Hacker Designpläne und Motorenentwürfe stahlen, die sie für mehrere Millionen Mark anderen Teams anboten.

Gesellschaften wie KPMG, PriceWaterhouse-Coopers oder die Arbeitsgemeinschaft für Sicherheit in der Wirtschaft (ASW) schätzen den Schaden durch Wirtschaftskriminalität und Spionage auf mittlerweile 20 Milliarden Euro jährlich. Sechs von zehn wirtschaftskriminellen Handlungen gehen auf das Konto von Angestellten.

**Welche Gegenmaßnahmen ergreifen?**

Schaden macht klug. Klüger ist, vorher etwas zu tun.
Dipl-Ing. Albert Blab von der Fa. Bosch Sicherheitssysteme GmbH ist mit der Thematik betraut. „Die Nachfrage von kleineren Firmen nimmt zu. Grundlage sollte immer ein durchdachtes Zutrittskontrollsystem sein. Für sensible Bereiche empfiehlt sich ein gestaffeltes Konzept, welches die Sondierung und Verifikation einzelner Bereiche oder Mitarbeiter ermöglicht“.

Während Industriespionage in die Zuständigkeit der Polizei fällt, beschäftigt Wirtschaftsspionage die Landesämter für Verfassungsschutz (LfV). Da nach einem Schadenereignis aber das Tatmotiv für die Betroffenen meist unklar ist, können die LfV im Fall des Falles durchaus konsultiert werden.

Vorbildlich aktiv ist auf diesem Sektor das LfV Baden-Württemberg (BW). Unter der Internetadresse „www.sicherheitsforum-bw.de“ kann man u.a. den Leitfaden „Schutz vor Spionage für die gewerbliche Wirtschaft“ einsehen und herunterladen. Ein Studium der Broschüre führt zu einer Sensibilisierung für mögliche Risiken.
Nach Aussage eines Experten des LfV BW empfiehlt man grundsätzlich ein „Info-Schutz-Konzept mit ganzheitlichem Ansatz“. Derzeit könne man sich „vor Nachfragen kaum retten“. Ansonsten kann auf verschiedene Institutionen wie die IHK, Deutscher Industrie- und Handelstag (DIHT), ASW, Polizei (hier die Präventionsdezernate der Landeskriminalämter) verwiesen werden.

Die einfachsten Maßnahmen könnten jedoch die folgenden sein: gutes Betriebsklima, gute Mitarbeiterführung durch Motivation, Qualitätssicherung und die Fähigkeit zur Konflikt-erkennung- und Management.

(7.146 Zeichen)