

## Ungewollter Informationsabfluss durch „Innentäter“



Bernd Elsenhans ist Geschäftsführer der EOS Sicherheitsdienstes in Steinheim, Fachautor, Referent und Experte für Sicherheit.

Mit diesem Beitrag setzen wir die Aufbereitung von Schwerpunktthemen aus der im Oktober und Dezember 2006 erstellten Berichte zum Thema „Mitarbeiterkriminalität“ fort. Zu den herausragenden Risikofaktoren beim Know-how-Schutz zählt das eigene Personal. Dies wurde von geschädigten Unternehmen im Nachhinein eine im Zusammenhang mit abgewanderten Mitarbeitern registriert. Beide Personengruppen waren bei den befragten Unternehmen zu rund 24 Prozent die Ursache für ungewollten Informationsabfluss. Das steht bei unserer Rechercheuntersuchung in einem auffälligen Zusammenhang mit einer signifikanten Unzufriedenheit mit den betrieblichen Bedingungen.

Andere empirische Untersuchungen zeigen, dass den eingeschleusten oder angeworbenen Innentätern beim illegalen Informationsabfluss eine erhebliche Bedeutung zukommt. Zur Kategorie der Innentäter sind Stamm-Mitarbeiter aus allen Hierarchieebenen sowie nicht zur Belegschaft gehörende Personen mit Zugangs-/Aufenthaltsberechtigung im Unternehmen zu rechnen. Hierzu zählen Leiharbeitskräfte, Dienstleister aller Art, insbesondere Reinigungsfirmen und Unternehmen aus der Sicherheitsbranche, Studenten, Praktikanten, Diplomanden. Sie sind aufgrund ihrer direkten und legalen Zugangsmöglichkeiten zu sensiblen Informationen und ihrer Kenntnis innerbetrieblicher Schwachstellen wertvolle Quellen für einen fremden Nachrichtendienst.

### Mögliche Motivlagen

Außer mangelnder Sensibilität für die betriebliche Sicherheit – insbesondere den Informationsschutz – gibt es zahlreiche, teilweise im persönlichen Bereich der Mitarbeiter liegende Umstände, die der Anlass für illegales Handeln sein können. Hierzu zählen:

- allgemeiner Wertewandel
- fehlendes Unrechtsbewusstsein
- schlechtes Betriebsklima
- mangelnder Informationsfluss
- empfundene Unterbezahlung
- Überschuldung
- Karriereprobleme (Nichtbeförderung, Perspektivlosigkeit)
- Rachegedanken
- Lebenskrisen

Bei der Gewinnung von Informationen im Ausspähungsobjekt gehören persönliche Unzufriedenheit und persönliche Zwangssituationen zu den vorrangigen Ansatzpunkten für eine Anwerbung.

### Einsatz menschlicher Quellen durch Nachrichtendienste

Gerade im Bereich der Wirtschaftsspionage sind trotz technischer Möglichkeiten menschliche Informationsquellen weiterhin unverzichtbar. Ihr besonderer Wert besteht darin, nicht nur kontinuierlich zu berichten, sondern zugleich auch die beschafften Informationen fachlich bewerten zu können. Die vielfältigen Möglichkeiten beim Einsatz menschlicher Quellen soll folgender Vorgang verdeutlichen:



### Das Sicherheitsunternehmen

Ein baden-württembergisches Unternehmen der High-Tech-Branche übernahm eine Mitarbeiterin ihrer Niederlassung in China zur befristeten Einarbeitung ins Stammhaus. Die Chinesin sollte nach der Rückkehr ins Heimatland eine anspruchsvolle Tätigkeit übernehmen. Sie wurde in die Zentrale mit qualifizierten Aufgaben betraut und erhielt die dafür notwendigen Datenzugangsberechtigungen. Sie dehnte ihre Anwesenheit im Betrieb in auffälliger Weise auf das Wochenende aus. Firmendaten speicherte sie auf privaten Datenträgern mit der Begründung, sich zu Hause mit den Informationsinhalten zum Zwecke der Einarbeitung ver-

traut machen zu wollen. Trotz des Hinweises von Vorgesetzten auf die Unzulässigkeit dieser Praxis änderte sie ihr Verhalten nicht.

Die ungewöhnlichen Handlungsweisen veranlasste die eingeschaltete Polizei zu einer Hausdurchsuchung. Dabei wurden 170 CDs gefunden, auf denen sich unrechtmäßig gespeicherte sensible Firmeninformationen befanden. Beachtenswert ist, dass bei der Betroffenen festgestellte erhebliche Defizite an Unrechtsbewusstsein. Die Bearbeitung des Falls ist noch nicht abgeschlossen.

Auch betriebsfremde Personen können zu „Innentätern“ werden. Zumindest größere Firmen sind heute auf externe Spezialisten (Unternehmensberater, Finanzexperten, Headhunting-Agenturen, Übersetzungsbüros, Wirtschaftsdetektiven, Zulieferfirmen, Service- und Sicherheitsunternehmen) angewiesen. Diesen Dienstleistern müssen zur Erfüllung ihrer Aufgaben Betriebsinterna zugänglich gemacht werden. Der Risikoaspekt besteht im Handling der notwendigerweise bereitzustellenden Informationen. Arglosigkeit beziehungsweise Unachtsamkeit im Um-

gang mit sensiblen Informationen, unterentwickelte Sicherheitskultur, fehlendes Unrechtsbewusstsein, Identifikationsdefizite oder mangelhafte Kontrolle können Gesichtspunkte sein, den betrieblichen Informationsschutz zu verbessern. Ihre Berücksichtigung in einem systematisch aufgebauten Sicherheitskonzept ist die Basis für strategisches Risikomanagement.

### Effiziente Prävention setzt voraus, dass:

- betriebliche Sicherheit nach Überzeugung der Führungskräfte nicht nur ein Bestandteil der Unternehmensphilosophie ist, sondern einen wesentlichen Beitrag zum ökonomischen Erfolg leisten kann und sie an dieser Erkenntnis ihr Handeln ausrichten,
- Sicherheitsaufgaben durch einen Sicherheitsverantwortlichen koordiniert werden,
- Sicherheitsvorkehrungen von der Belegschaft verantwortlich mitgetragen werden und
- vertrauensbildende und Akzeptanz fördernde Maßnahmen ergriffen werden, die geeignet sind, die Identifikation der Mitarbeiter mit dem Unternehmen zu fördern.

Wir helfen gerne mit praktikablen Lösungen die nachhaltigen und sicher einen großen Teil der unentdeckten Straftaten durch eigenen Mitarbeiter verhindern oder aufklären. Fragen Sie uns – Wir helfen Ihnen mit Sicherheit

Bernd Elsenhans