



## Spionageabwehr: Erfahrungen des Bundesamtes für Verfassungsschutz

### Kontra dem Know-how-Klau

Spionageabwehr– was geht das denn Hersteller von Bändern, Blechen und Rohren an? Sehr viel, meint bbr. Daher startet die Zeitschrift mit den Informationen eines Experten des Bundesamtes für Verfassungsschutz eine Serie zum Know-how-Schutz.

„Wir stellen ein hohes Interesse fremder Nachrichtendienste am Know-how deutscher Unternehmen fest.“  
Dr. Hans-Georg Maaßen, Präsident des Bundesamtes für Verfassungsschutz (BfV)

Es handelt sich um ein teures Interesse: Die deutsche Wirtschaft beziffert das Schadenspotenzial auf 50 Milliarden Euro jährlich. Als Gegenmaßnahme setzt das BfV auf „Prävention durch Information“ – mit Drucksachen, Schulung und Beratung. In Sachen Wirtschaftsschutz berät, sensibilisiert und schult BfV-Experte Udo Schauff deutsche Unternehmen.

„Der deutsche Maschinen- und Anlagenbau ist einer der Industriezweige, mit denen ich zuerst auf dem Gebiet Wirtschaftsspionage Kontakt hatte“, erklärt der Wirtschaftsschützer. Dabei erfuhr Schauff recht schnell, wie hoch die Begehrlichkeit von ausländischen

Geheimdiensten und Konkurrenzunternehmen am Know-how der deutschen Wirtschaft ist. Besondere Sorge bereitet den Verfassungsschützern bei der Wirtschaftsspionage beispielsweise die Volksrepublik China, ausgestattet mit den personalintensivsten Nachrichtendiensten weltweit (MSS, MID, EID). 375.000 hauptamtliche Nachrichtendienstangehörige besitzen die drei russischen Nachrichtendienste (SWR, GRU, FSB). Der SWR späht mit gesetzlichem und offiziellem Auftrag ausländische Firmen aus, um die heimische Wirtschaft zu unterstützen.

Doch grau ist auch die Geheimdienst-Theorie, mehr lernen kann ein sicherheitsbewusstes Unternehmen von der bunten Praxisvielfalt und dem erstaunlichen Einfallsreichtum der Agenten. Das belegen die folgenden Beispiele, die Schauff schildert. Beispiel eins behandelt eine der größten Gefahren: Geheimnisverrat durch einen frustrierten Mitarbeiter, der einen österreichischen Hersteller von Steuerungen für Windenergieanlagen (WEA) fast die Existenz gekostet hätte. Einem unzufriedenen Entwicklungsingenieur verspricht ein ausländischer Kunde 15.000 Euro und einen hochdotierten Arbeitsvertrag, wenn er dem WEA-Hersteller im Gegenzug den Quellcode der Steuerung beschafft. Der Mitarbeiter nimmt das Angebot an und kündigt.

Sein ehemaliger Arbeitgeber versäumt es jedoch, den Zugang zum Firmenrechner sofort zu sperren. Ein fataler Fehler, denn nun erhalten die Ausländer den Quellcode. Während in Österreich ein Gerichtsverfahren gegen den entlarvten Spion läuft, verweigert der Kunde mit einem fadenscheinigen Vorwand die Bezahlung der letzten Lieferung und kündigt den Vertrag. Das ausländische Unternehmen leugnet alles und baut seitdem eigene Windkraftanlagen mit der gestohlenen österreichischen Software. Der durch das österreichische Unternehmen geschätzte wirtschaftliche Schaden beträgt rund 60 Millionen Euro, während der geständige Ingenieur zu einem Jahr Haft und zwei Jahren Bewährungsstrafe und zur Zahlung von 200.000 Euro verurteilt wird. Schauff: „Das österreichische Unternehmen musste rund die Hälfte seiner Mitarbeiter entlassen.“

Beim Beispiel zwei geht es um die Macht der Liebe: Bei einem deutschen Metallverarbeiter bündelt eine ausländische Praktikantin mit einem dort festangestellten, einsamen Landsmann an, der selbst einmal in dem Unternehmen als Praktikant angefangen hat. Vermutlich verliebte sich der Entwickler in die Frau, die kurz Zeit später wieder in ihr Heimatland verschwindet. Der anscheinend von einer Geheimdienstagentin Angeworbene nimmt seitdem an allen Gesprächen über Entwicklungsvorhaben teil und zapft viele Datenquellen auf dem Firmenrechner an. Bevor er schließlich wegen seines auffälligen Verhaltens auffliegt und in das Heimatland der Praktikantin flieht.

Beispiel drei zeigt eine weitere Gefahrenquelle auf: den Besuch von ausländischen Firmen. Der Geschäftsführer eines ausländischen Stahlbauunternehmens besucht den Betrieb seines deutschen Geschäftspartners, der sich auf die Produktion großer gebogener Betonformflächen spezialisiert hat. Einem Mitarbeiter fällt bei dem Besuch das ungewöhnliche Verhalten des Firmenchefs auf, der bei bestimmten Stellen im Betrieb immer einen bestimmten Abstand einhält und das Anzugsjackett auf einer Seite öffnet. Der Mitarbeiter informiert seinen Vorgesetzten, der den Besucher daraufhin genau unter die Lupe nehmen lässt. Die Firma entdeckt am Gürtel eine winzige Kamera, mit der er interessante Produktionsprozesse aufgenommen hat.

Die Firma hatte dem Geschäftsführer aber vor dem Firmenbesuch eine in der Heimatsprache und in Deutsch formulierte Geheimhaltungsvereinbarung unterzeichnen lassen, die ihm Ton-, Foto- und Videoaufnahmen von Produktion und Prozessen verbietet. Ein deutsches Gericht verurteilt den Geschäftsführer schließlich wegen des Versuchs des Verrats von Geschäfts- und Betriebsgeheimnissen zu 18 Monaten Bewährungsstrafe und zu einer Geldstrafe von 80.000 Euro. Schauff: „Ein Hinweis auf das typische Schild zum Fotografier-Verbot hätte nichts gebracht, denn da hätte sich der Besucher herausgeredet, dass er das nicht verstanden oder nicht gesehen habe.“ Rechtlich verbindlich sei dagegen die in der Heimatsprache eines Besuchers verfasste und unterschriebene Geheimhaltungsvereinbarung.

Generell, so zeigen weitere beispielhafte Fälle aus der Praxis, ist bei Firmenbesuchen stets besondere Vorsicht angesagt. Teilnehmer von asiatischen Wirtschaftsdelegationen verirren sich in Räumlichkeiten der besuchten Unternehmen, finden sich anstatt in den Toiletten in der Elektronikfertigung, oder in Serverräumen mit einem USB Stick wieder. Oder mit dem Verlassen der Delegation wird der Verlust eines Firmenlaptops festgestellt.

Der Besuch mit vielen Teilnehmern, die sich nur schwer überwachen lassen, ist scheinbar geplant. Das BfV empfiehlt daher, die maximale Anzahl der Teilnehmer eines Besuches von vorneherein festzulegen und nur diese Anzahl zum Besuch zu akzeptieren. Beim Besuch sollte dann jeder Teilnehmer im Falle seiner Abwesenheit von der Gruppe einen persönlichen Begleiter erhalten, der ihn auf allen Wegen durch den Betrieb begleitet.

Vorsicht ist auch geboten bei Kontakten mit Personen von bestimmten Berufsgruppen. Dazu eine Schrift der Verfassungsschutzbehörden: „Bei ihren Beschaffungsaktivitäten verschleiern die Geheimdienste ihre wahren Absichten und versuchen, z.B. durch Tarnung ihrer Mitarbeiter als Diplomaten, Geschäftsleute oder Journalisten, an nachrichtendienstlich interessantes Material zu gelangen.“ Als Journalist der Zeitschrift Wenhui Daily hatte sich beispielsweise ein Agent des chinesischen Ministeriums für Staatssicherheit (MSS: ziviler Inlands- und Auslandsnachrichtendienst) getarnt. Bei einer Observation in Deutschland beobachtete der Verfassungsschutz, wie er von einer Chinesin einen großen Karton erhielt. Die Überprüfung ergab, dass es sich um eine Akademikerin mit Dokortitel handelte, die trotz ihrer hohen Qualifizierung für ein geringes Gehalt als Bürokraft arbeitete. Ihr Arbeitsgeber war ein Patentanwalt. Es könnte sich um eine Einschleusung durch einen Nachrichtendienst gehandelt haben. Es ist schon erstaunlich, wie phantasievoll fremde Nachrichtendienste bei der Jagd auf das Know-how deutscher Unternehmen vorgehen.

Der Artikel basiert auf einem Vortrag auf dem VDMA-Informationstag „Know-how-Schutz und Informationssicherheit“ in Frankfurt am Main im Dezember 2013.

Die nächste Folge der bbr-Serie Spionageabwehr und Know-how-Schutz gibt Tipps aus der Praxis für IT-Security und Know-how-Schutz.

Autor: Nikolaus Fecht

((Infokasten))

Die elf goldenen Regeln der Prävention

1. Nicht warten, bis der Spionagefall eingetreten ist
2. Aktuelle Informationen bei kompetenten Partnern einholen
3. Informationsschutz als wichtigen Bestandteil der Firmenphilosophie und Firmenstrategie verankern
4. Sicherheitsstandards regelmäßig analysieren
5. Ganzheitliches Sicherheitskonzept verwirklichen und permanent fortschreiben
6. Schutzmaßnahmen auf den Kernbestand zukunfts-sichernder Informationen konzentrieren
7. Einhaltung und Erfolg der Sicherheitsvorkehrungen kontrollieren, Sicherheitsverstöße sanktionieren
8. „Frühwarnsystem“ zur Erkennen von Know-how-Verlusten installieren
9. Auffälligkeiten und konkrete Hinweise konsequent verfolgen, professionelle Hilfe in Anspruch nehmen
10. Informationsschutz als strategischen Erfolgsfaktor nutzen
11. Sich durch den Verfassungsschutz kostenlos beraten lassen.

Quelle: Bundesamt für Verfassungsschutz

LINK

[www.verfassungsschutz.de](http://www.verfassungsschutz.de)