Prävention

Zur Vermeidung von Schäden durch Innentäter ist ein umfassendes Sicherheitskonzept erforderlich.

Dazu gehört zum Beispiel:

- Risiko- und Schwachstellenanalyse
- kontinuierliche Sensibilisierung aller Unternehmensangehörigen
- Kompetenz und Motivation der eigenen Mitarbeiter für das Sicherheitskonzept nutzen
- Benennung eines Sicherheitsverantwortlichen
- Sicherheitsregelungen für Besucher und Fremdfirmen
- modernes Personalmanagement (Personalauswahl und -betreuung)
- Monitoring
- klare Unternehmensleitlinien

Sprechen Sie uns an und vereinbaren Sie einen Termin für ein vertrauliches Sensibilisierungsgespräch.

Ihre Ansprechpartner

www.verfassungsschutz.de

www.verfassungsschutz-bw.de

www.verfassungsschutz.bayern.de

www.verfassungsschutz-berlin.de

www.verfassungsschutz-brandenburg.de

www.verfassungsschutz.bremen.de

www.hamburg.de/verfassungsschutz

www.verfassungsschutz.hessen.de

www.verfassungsschutz-mv.de

www.verfassungsschutz.niedersachsen.de

www.mik.nrw.de/verfassungsschutz

www.verfassungsschutz.rlp.de

www.saarland.de/verfassungsschutz.htm

www.verfassungsschutz.sachsen.de

www.mi.sachsen-anhalt.de/verfassungsschutz

www.verfassungsschutz.schleswig-holstein.de

www.thueringen.de/de/verfassungsschutz

Impressum: Bundesamt für Verfassungsschutz
für die Verfassungsschutzbehörden
in Bund und Ländern

Druck: INFOX GmbH&Co.
Informationslogistik KG, Troisdorf

Stand: August 2010

Verfassungsschutz

Bund
Länder

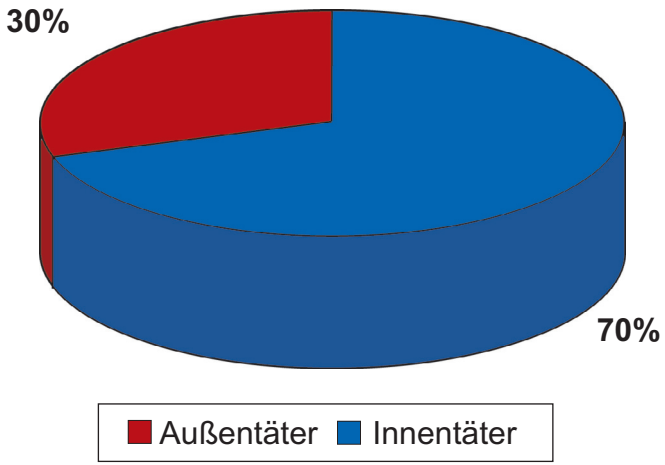
Sicherheitslücke Mensch
–
Der Innentäter als größte Bedrohung für die Unternehmen

Verfassungsschutz: **neutral** **kostenfrei** **vertraulich**

Situation

Unternehmensspezifisches Know-how entscheidet über Markt- und Zukunftschancen. Spionage, Diebstahl, Sabotage, Korruption oder IT-Kriminalität durch eigene Mitarbeiter bedroht diesen Wettbewerbsvorteil.

Das Risiko Opfer von Know-how-Abfluss durch Innentäter zu werden, wird von den meisten Unternehmen stark unterschätzt!



Gefährdungspotentiale

Umfangreiche Studien belegen, dass besonders kleine und mittelständische innovative Unternehmen gefährdet sind. In vielen Fällen ist das Sicherheitsbewusstsein nur wenig ausgeprägt. Die Möglichkeit, durch eigene Mitarbeiter ausgespäht zu werden, erscheint Unternehmern unvorstellbar.

Fallbeispiele

1. Ein gekündigter Mitarbeiter einer IT-Firma kopierte die Kundendatei für seinen neuen Arbeitgeber.
2. Ein Mitarbeiter entwendete einen Laptop mit sensiblen Firmendaten aus einem Maschinenbauunternehmen.
3. Ein Praktikant brachte brisante Daten eines technischen Projektes mittels USB-Stick in seinen Besitz.
4. Ein Wachmann fotografierte Prototypen, um die Bilder an Wettbewerber zu verkaufen.
5. Ein Mitarbeiter verkaufte noch nicht patentiertes Know-how aus dem F+E-Bereich ins Ausland.
6. Zwei führende Mitarbeiter machten sich mit einer Produktneuentwicklung ihres bisherigen Arbeitgebers selbstständig.

Täter

Innentäter sind in Anbetracht ihrer legalen Zugangsmöglichkeiten und ihres Insiderwissens über innerbetriebliche Schwachstellen in der Lage, den Unternehmen mehr Schaden zuzufügen als externe Täter es je könnten. Hierarchieebenen bilden keine Grenzen mehr - Täter kann vom Hausmeister bis zum Manager jeder sein.

Indikatoren

- Unzufriedenheit am Arbeitsplatz, fehlende Identifikation mit dem Unternehmen
- Auffällige Neugier
- Nutzung von Spionagehilfsmitteln wie z.B. Bild- und Tonaufzeichnungsgeräte, mobile Datenträger
- Auffälligkeiten im persönlichen Umfeld (aufwändiger Lebensstil, Anzeichen für Alkoholsucht, Drogenabhängigkeit, Spielsucht oder Überschuldung)
- Diskrepanzen im beruflichen Werdegang, z.B. Über- oder Unterqualifikation
- zweifelhafte Initiativbewerbung
- Verdächtige Kontakte zu Vertretungen ausländischer Staaten oder zu Konkurrenzunternehmen
- Überschreitung der Zugriffsberechtigungen