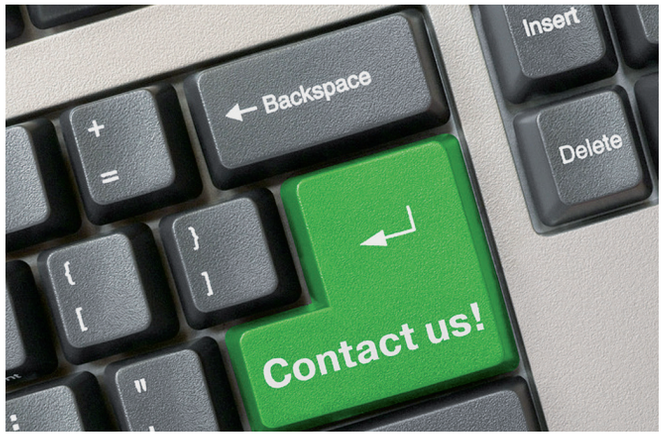
Empfehlungen

- Bestimmung essentieller Werte/Informationen
- Risiko- und Schwachstellenanalyse unter Einbeziehung aller Mitarbeiter
- Erstellung eines umfassenden Sicherheitskonzeptes inklusive Berechtigungsmanagement
- Benennung eines Sicherheitsverantwortlichen
- Kontinuierliche Sensibilisierung und Schulung aller Mitarbeiter
- Sicherheitsregelungen für Besucher und Fremdfirmen
- Konsequente Umsetzung und Fortschreibung des Sicherheitskonzeptes
- Förderung der Identifikation der Mitarbeiter mit dem Unternehmen

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



Ihre Ansprechpartner im Wirtschaftsschutz

Wirtschaftsschutz
Niedersächsisches Ministerium für Inneres und Sport - Verfassungsschutz -
Postfach 44 20
30044 Hannover
Telefon (0511) 6709 - 0
Telefax (0511) 6709 - 393
E-Mail wirtschaftsschutz@verfassungsschutz.niedersachsen.de

initiative wirtschaftsschutz

Gemeinsam. Werte. Schützen.

Dort finden Sie weitere Informationen sowie die Kontaktdaten Ihrer örtlichen Ansprechpartner.

www.wirtschaftsschutz.info

Impressum

Herausgeber:	Bundesamt für Verfassungsschutz für den Verfassungsschutzverbund
Bilder:	© Nikolai Sorokin - Fotolia.com
Stand:	März 2016

Verfassungsschutz

Bund Länder

Wirtschaftsschutz

Gefahr durch Innentäter

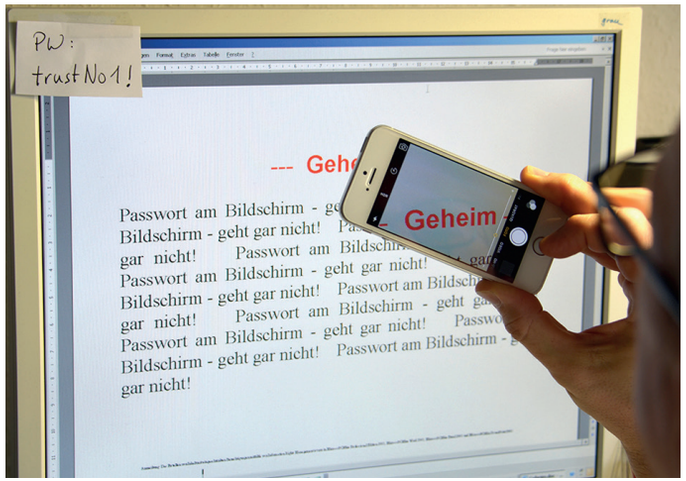
Sicherheitslücke Mensch

Prävention durch Dialog und Information

Gefährdungspotential

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

Delikte wie Spionage, Diebstahl, Sabotage oder Korruption durch eigene Mitarbeiter bedrohen Ihr Know-how und Ihren Wettbewerbsvorteil.



Für viele Unternehmen ist es unvorstellbar, Täter in den eigenen Reihen zu haben. Umfangreiche Studien belegen, dass insbesondere kleine und mittelständische innovative Unternehmen gefährdet sind. Verstärkt wird dies durch mangelndes Sicherheitsbewusstsein.

Fallbeispiele

- Ein unzufriedener Mitarbeiter zerstörte mutwillig Speichermedien mit wichtigem Know-how
- Ein gekündigter Mitarbeiter kopierte die Kundendatei für seinen neuen Arbeitgeber
- Ein Mitarbeiter entwendete einen Laptop mit sensiblen Firmendaten
- Ein Praktikant brachte brisante Daten eines technischen Projektes mittels USB-Stick in seinen Besitz
- Ein Wachmann fotografierte Prototypen, um die Bilder an Wettbewerber zu verkaufen
- Ein Mitarbeiter verkaufte noch nicht patentiertes Know-how aus dem Bereich Forschung und Entwicklung ins Ausland
- Zwei führende Mitarbeiter machten sich mit einer Produktneuentwicklung ihres bisherigen Arbeitgebers selbstständig

Täter

Innentäter sind in Anbetracht ihrer Zugangsmöglichkeiten sowie ihres Insiderwissens über innerbetriebliche Abläufe in der Lage, Unternehmen erheblichen Schaden zuzufügen.

Unabhängig vom Status im Unternehmen kann jeder zum Innentäter werden – vom Hausmeister bis zum Manager.

Indikatoren

- Unzufriedenheit am Arbeitsplatz, fehlende Identifikation mit dem Unternehmen
- Auffällige Neugier
- Regelwidriges Einbringen und Nutzen mobiler Endgeräte oder Datenträger
- Auffällige Veränderungen im persönlichen Umfeld
- Verdächtige Kontakte zu Vertretungen ausländischer Staaten oder zu Konkurrenzunternehmen
- Versuch der Erweiterung gewährter Zugriffsberechtigungen
- Ungewöhnliche Arbeitszeiten