

Vertrauensschadenversicherung auf einen Blick

Tatort am Arbeitsplatz

Betrügnern, Hackern
Kunden
Lieferanten

Im Geschäftsverkehr wird in
krimineller Absicht Vertrauen
missbraucht von ...

Mitarbeitenden
Zeitarbeitskräften
Reinigungspersonal

Der Wolf im Schafspelz – interne Täter

Keine Firma stellt einen Mitarbeiter ein, dem sie nicht vertraut. Denn ohne Vertrauen ist eine Zusammenarbeit unmöglich. Nur in den seltensten Fällen hat ein Betriebsangehöriger von Anfang an die Absicht, sich zu bereichern und das Unternehmen zu schädigen. Doch die Lebensverhältnisse können sich rasch verändern und der Mitarbeitende hat plötzlich einen höheren Geldbedarf. Aber auch die Bedrohungslage durch externe Täter nimmt stark zu und die Abgrenzung zum Cyber-Betrug verschwimmt.

Mögliche Gründe für Betrugsfälle

- Wachsende Ansprüche der Familie, Habgier
- Kostspielige Scheidung
- Alkohol- / Spielsucht
- Pflegebedürftige Angehörige
- Unsichere Arbeitsbedingungen
- Vermeintlicher sozialer Zwang zu gehobenem Lebensstil
- Verändertes Werteverständnis
- Finanzieller Engpass

Risikoumfeld / Trends

- Günstiges Wirtschaftsumfeld für Wirtschaftskriminalität aufgrund Inflation, Krieg, Insolvenzrisiko
- Typische Täter aus dem Kreis der Mitarbeitenden sind:
 - lange im Unternehmen, in gehobener Position und kennen die Lücken im Kontrollsystem oder
 - jung und unerfahren und auf der Suche nach dem schnellen Geld
- Jeder dritte Betrug in Privatunternehmen wird von Hinweisgebern aufgedeckt.

So fliegen Täter auf!

Selbstanzeige aus
schlechtem Gewissen

Interne Kontrollsysteme
Routineprüfung/Revision,
Prüfung von Auffälligkeiten



„Whistleblowing“

Zufall

Hinweise – von anderen Mitarbeitern,
durch Unternehmensexterne

Typische Betrugsmaschen

Veruntreuung von
Sach- und Geldwerten

Urkundenfälschung

Diebstahl



Bestellerbetrug

Fake President

Unterschlagung

Mitarbeiterbetrug

Fingierte Rechnungen

Hinweisgeberschutzgesetz



Informationen zum Hinweisgeberschutzgesetz

Das Gesetz zur Umsetzung der EU-Whistleblowing-Richtlinie ist seit 2. Juli 2023 in Kraft.

Was wird geregelt?

Das Gesetz dient dem Schutz von Hinweisgebern vor Repressalien (z.B. Disziplinarmaßnahmen oder Diskriminierungen) und soll das Whistleblowing insgesamt vereinfachen. Es regelt die verpflichtende Einrichtung interner Meldestellen in Unternehmen und macht umfangreiche Vorgaben, welche Maßnahmen bei Hinweisen einzuleiten sind mit entsprechenden Dokumentationspflichten.

Was passiert bei Verstößen?

Es drohen hohe Bußgelder und Haftungsansprüche gegen Unternehmen bzw. Unternehmensleiter. Weiterhin steht dem Hinweisgeber unter Umständen Schadenersatzanspruch zu.

Tatsächliche Betroffenheit

In 57 % aller
Wirtschaftsdelikte
sind Innentäter
beteiligt

57 %

... der betroffenen
Unternehmen gaben
an, einen Schaden von
mehr als 1 Mio. Euro
erlitten zu haben

15 %

Nahezu jedes Zweite
Unternehmen war in den
vergangenen 24 Monaten
von Wirtschafts-
kriminalität betroffen.

40 %

So hoch waren die
Schäden von Unter-
nehmen durch
Wirtschaftskriminalität
2022 in Deutschland.

2,1 Mrd. Euro

Die Leistungsmerkmale der Vertrauensschadenversicherung



Leistungsübersicht	
 Schäden durch Vertrauenspersonen 2-fach maximierte Versicherungs- summe	 Schäden durch außenstehende Dritte (Sublimit 2,5 Mio. Euro)
 Schäden durch Eingriffe in die IT (Sublimit 2,5 Mio. Euro)	 Mitversicherte Unternehmen
 Umfangreiche Kostenübernahmen	 Rückwärtsdeckung Unbegrenzt
 Nachmeldefrist Max. 36 Monate	 Weltweiter Versicherungsschutz
 Vertragsstrafen	 Vorläufige Entschädigungsleistung 50 %, max. 2,5 Millionen
Kostenübernahmen	Auswirkungen ohne Absicherung

- Schadenermittlungskosten
 - Rechtsverfolgungskosten
 - Informationskosten
 - Aufwendungen zur Fortführung des Geschäftsbetriebs
 - Public-Relations-Kosten
 - Kosten für psychologische Betreuung
 - Spionageaufklärung
- Umfassende Vermögensschäden (Firmenvermögen, Rechts- und Schadenermittlungskosten)
 - Schäden bei Dritten, für die das Unternehmen haftet
 - Mangelnde Liquidität des Unternehmens
 - Störung des Betriebsfriedens
 - Finanzielle Belastung durch zusätzliche Kosten

Prävention	
Unternehmenskultur	Sicherheitsvorkehrungen und Kontrollen
	
• Offene, vertrauensvolle Unternehmenskultur • Möglichst flache Hierarchien • Konstruktive Fehlerkultur • Offene Kommunikation • Klare Unternehmensrichtlinien • Faire Bezahlung mit finanziellen Anreizen und Leistungsvergütung	
• Klares Vier- oder Mehr-Augen-System • Wachsamkeit und Beobachten von Auffälligkeiten, wie Anomalien bei Arbeitsstunden / -zeiten, Zugriffsversuche auf begrenzt zugängliche Daten / Gebrauch von unautorisierten Datenträgern • Einrichten von geschützten internen oder externen Whistleblowing-Kanälen (Ombudsleute) • Präventives Risikomanagement und regelmäßige Prozessoptimierung • Umgehende, transparente und objektive Untersuchung bei Verdachtsmomenten • Überprüfung von Bewerbern (Führungszeugnis, Referenzen, Schufa und Background-Check) • Regelmäßige Budgetkontrolle und Erfolgsrechnungen • Laufende Rentabilitäts- und Liquiditätsbetrachtungen • Sensibilisierung von Mitarbeitenden auf Cyber-Risiken sowie Verbesserung der IT-Sicherheit • Regelmäßige Stichproben-Kontrollen der Handlungen von Mitarbeitenden • Mitarbeiterschulungen für Betrugsfälle im Internet (z.B. durch Social Engineering)	