Wirtschaftskriminalität – wenn Vertrauen zum Risiko wird

25. September 2026



„So etwas kann uns nicht passieren.“ Dieser Gedanke liegt nahe, wenn man von Betrugsfällen hört, bei denen sich Kriminelle bspw. als Geschäftsführer, Vorstand oder Führungskraft ausgeben und Mitarbeitende dazu bringen, hohe Geldbeträge auf fremde Konten zu überweisen.

Doch die Realität sieht anders aus: **Kein Unternehmen ist vollständig vor Wirtschaftskriminalität geschützt.** Die Methoden der Täter werden professioneller, technischer und zunehmend schwerer zu erkennen. Gefälschte Identitäten, manipulierte Zahlungsanweisungen, Social Engineering, Cyberangriffe und inzwischen auch täuschend echte KI-generierte Stimmen und Videos eröffnen Kriminellen immer neue Möglichkeiten.

Die finanziellen Folgen können erheblich sein. Gleichzeitig kann ein Betrugsfall das Vertrauen innerhalb des Unternehmens und gegenüber Geschäftspartnern, Gesellschaftern, Kreditgebern und Kunden nachhaltig belasten.

Wirtschaftskriminalität in Zahlen

Das Risiko ist real – und die Schäden können erheblich sein.



48 %

der Unternehmen bewerten das Risiko, selbst Opfer von Wirtschaftskriminalität zu werden, als **hoch oder sehr hoch**.



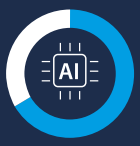
65 %

der betroffenen Unternehmen berichten von **Betrug und Untreue.**



2,76 Mrd. €

betrug der polizeilich erfasste **Schaden durch Wirtschafts-kriminalität** 2024.



71 %

sehen inzwischen ein **hohes oder sehr hohes Risiko durch KI-basierten Betrug.**

Wirtschaftskriminalität verändert sich – und mit ihr die Risiken für Unternehmen.

Quellen: KPMG, Wirtschaftskriminalität in Deutschland 2025/2026; BKA, Bundeslagebild Wirtschaftskriminalität 2024.

Wenn Vertrauen missbraucht wird, entsteht ein Vertrauensschaden

Betrug muss dabei nicht zwangsläufig von außen kommen. Ein erhebliches Risiko entsteht auch innerhalb des eigenen Unternehmens.

Mitarbeitende verfügen über Zugänge zu Kassen, Warenbeständen, Konten, IT-Systemen und vertraulichen Informationen. Werden diese Vertrauenspositionen vorsätzlich missbraucht, können erhebliche Vermögensschäden entstehen.

Eine Vertrauensschadenversicherung kann Unternehmen vor den finanziellen Folgen bestimmter vorsätzlicher und rechtswidriger Handlungen schützen – je nach vereinbartem Versicherungsschutz bspw. bei:

- vorsätzlichen und unerlaubten Handlungen durch eigene Mitarbeitende

- Betrug und Untreue
- Unterschlagung von Geld oder Waren
- Computerbetrug und bestimmten rechtswidrigen Eingriffen in IT-Systeme
- Manipulation von Zahlungsströmen
- gefälschten oder manipulierten Zahlungsanweisungen
- Fake-President- und CEO-Fraud-Angriffen
- weiteren kriminellen Handlungen Dritter, soweit diese vom Versicherungsschutz umfasst sind

Damit stellt die Vertrauensschadenversicherung einen wichtigen Baustein des betrieblichen Risikomanagements dar.

Zwei Schadenfälle aus der Praxis

Der Griff in die Kasse

Der Werkstattleiter eines Kfz-Betriebes war unter anderem dafür verantwortlich, die täglichen Bareinnahmen aus Reparaturen, Inspektionen und dem Verkauf von Ersatzteilen entgegenzunehmen und die Werkstattkasse zu führen.

Über einen längeren Zeitraum entnahm er heimlich Bargeld aus der Kasse und verwendete es für private Zwecke. Insgesamt entstand der Werkstatt dadurch ein **Fehlbetrag von 44.500 €.**

Bei einer internen Kassenprüfung stellte der Inhaber Unstimmigkeiten zwischen den gebuchten Bareinnahmen und dem tatsächlichen Kassenbestand fest. Die anschließende Prüfung ergab, dass der Werkstattleiter das Geld unberechtigt entnommen hatte.

Der Mitarbeiter wurde daraufhin gekündigt und zur Rückzahlung des entstandenen Schadens aufgefordert. Da er die Erstattung verweigerte, leitete der Inhaber rechtliche Schritte ein. Auch nach einem rechtskräftigen Gerichtsurteil blieben die anschließenden Vollstreckungsversuche erfolglos, da der ehemalige Mitarbeiter nicht über ausreichende finanzielle Mittel verfügte.

Der Versicherer ersetzte der Kfz-Werkstatt den entstandenen Vermögensschaden in Höhe von 44.500 € sowie die im Zusammenhang mit der Schadenregulierung angefallenen Rechtsanwaltskosten, soweit diese vom vereinbarten Versicherungsschutz umfasst waren.

Unterschlagung von Waren

Eine Mitarbeiterin eines Supermarktes entnahm über mehrere Monate hinweg regelmäßig Waren aus den Beständen des Marktes, ohne diese zu bezahlen.

Dabei handelte es sich unter anderem um Lebensmittel, Getränke, Drogerieartikel und weitere Produkte des täglichen Bedarfs. Die Waren verwendete sie sowohl für den eigenen Bedarf als auch für Familienangehörige und Bekannte.

Im Rahmen einer internen Bestandskontrolle stellte der Marktleiter erhebliche Differenzen zwischen dem Warenbestand und den verbuchten Verkäufen fest. Bei der anschließenden Überprüfung wurde die Mitarbeiterin mit den Unstimmigkeiten konfrontiert.

Sie gestand die unberechtigten Warenentnahmen und erklärte sich bereit, ein **notarielles Schuldanerkenntnis** über den entstandenen Schaden abzugeben.

Nach Vorlage des Schuldanerkenntnisses beim Versicherer wurde dem Supermarkt der nachgewiesene Schaden in Höhe von **6.300 €** ersetzt, soweit dieser vom Versicherungsschutz umfasst war.

Zwei Fälle, ein gemeinsames Risiko: Vertrauen ist für jedes Unternehmen unverzichtbar – und kann gleichzeitig zu einem erheblichen finanziellen Risiko werden.

Vertrauensschäden: kein Einzelfall – Tendenz steigend



205 Mio. €
Leistungen der Vertrauensschadenversicherung
2025

+20 %
gegenüber 2024

Quelle: GDV, Hochrechnung 2025 auf Basis der ersten drei Quartale

KI verändert das Betrugsrisiko grundlegend

Künstliche Intelligenz eröffnet Unternehmen enorme Chancen. Gleichzeitig entstehen dadurch neue Möglichkeiten für Kriminelle. Besonders relevant sind die Kombinationen aus **Social Engineering, Voice Cloning und Deepfakes.**

Für einen überzeugenden Betrugsversuch kann inzwischen öffentlich verfügbares Bild- und Tonmaterial ausreichen, um Stimme und Erscheinungsbild einer Führungskraft täuschend echt nachzuahmen. KI-Systeme können Gesichter, Stimmen, Mimik und Lippenbewegungen simulieren – teilweise sogar in Echtzeit.

Damit entwickelt sich der klassische **Fake-President-Betrug** weiter: Aus einer gefälschten E-

Mail oder einer manipulierten Zahlungsanweisung kann ein scheinbar echter Videoanruf der Geschäftsführung werden.

So kann ein Angriff ablaufen: Ein Mitarbeiter erhält eine Nachricht, angeblich von der Geschäftsführung. Es geht um eine **dringende und vertrauliche Zahlung.** Kurz darauf folgt ein Videoanruf. Auf dem Bildschirm erscheint vermeintlich der CFO. Gesicht, Stimme und Umgebung wirken vertraut. Weitere vermeintliche Kollegen nehmen ebenfalls an der Videokonferenz teil.

Der Mitarbeiter hat zunächst keinen offensichtlichen Grund, an der Echtheit des Gesprächs zu zweifeln – und veranlasst die Überweisung.

Das Gefährliche: Die bisherige Plausibilitätsprüfung „Ich habe gerade persönlich mit meinem Chef gesprochen" funktioniert unter Umständen nicht mehr zuverlässig.

Deepfake-Fraud ist keine Zukunftsmusik

Wie real diese Gefahr bereits ist, zeigt ein 2024 bekannt gewordener Fall aus Hongkong. Ein Mitarbeiter eines britischen Ingenieur- und Beratungsunternehmens nahm an einer Videokonferenz teil, an der vermeintlich der CFO und weitere Kollegen teilnahmen. Tatsächlich waren – mit Ausnahme des Mitarbeiters – sämtliche Teilnehmer durch Deepfake-Technologie simuliert.

In der Folge wurden in **15 Transaktionen rund 200 Millionen Hongkong-Dollar** auf Konten der Betrüger überwiesen.

Der Fall zeigt eindrucksvoll, wie sich die Methoden des Social Engineering weiterentwickeln: **gefälschte E-Mail gefälschte Identität gefälschte Stimme gefälschter Videoanruf**

Die technische Entwicklung macht es zunehmend schwieriger, allein anhand des äußeren Eindrucks zu erkennen, ob eine Zahlungsanweisung tatsächlich von einer berechtigten Person stammt.

Vertrauensschadenversicherung: Schutz, wenn Prävention nicht ausreicht

Unternehmen investieren viel in interne Kontrollen, Vier-Augen-Prinzipien, IT-Sicherheit und Mitarbeiterschulungen. Diese Maßnahmen sind unverzichtbar. **Aber keine Sicherheitsmaßnahme bietet einen hundertprozentigen Schutz.**

Eine Vertrauensschadenversicherung kann dort ansetzen, wo trotz aller Präventionsmaßnahmen ein Vermögensschaden entsteht. Sie kann – abhängig vom individuellen Vertrag – finanzielle Folgen bestimmter vorsätzlicher und rechtswidriger

Handlungen von Mitarbeitenden oder Dritten absichern.

Damit ergänzt sie bestehende Maßnahmen des Risikomanagements und kann dazu beitragen, dass ein einzelner Betrugsfall nicht zu einer existenzbedrohenden Belastung für das Unternehmen wird.

Individueller Schutz für jedes Unternehmen

Jedes Unternehmen ist anders. Größe, Branche, Geschäftsmodell, Zahlungsstrukturen und interne Organisation bestimmen maßgeblich das individuelle Betrugsrisiko. Deshalb sollte auch der Versicherungsschutz **zum Unternehmen passen.**

Mögliche Bausteine sind beispielsweise:

- individuelle Versicherungssummen
- auf das Unternehmen abgestimmte Deckungsbausteine
- Schutz vor Mitarbeiterdelikten und bestimmten Betrugshandlungen Dritter
- Absicherung moderner Betrugsformen
- optionale Erweiterungen für besondere Risiken
- individuelle Lösungen für unterschiedliche Unternehmensgrößen und Geschäftsmodelle

Schon für etwa 1.000 € pro Jahr kann ein Unternehmen seinen Versicherungsschutz sinnvoll ergänzen – bspw. eine Kfz-Werkstatt mit 15 Mitarbeitenden und einer Versicherungssumme von 100.000 €. Die tatsächliche Prämie hängt selbstverständlich von den individuellen Unternehmens- und Risikodaten sowie vom gewählten Versicherungsschutz ab.

Fazit: Vertrauen ist wertvoll. Schützen Sie es.

Betrug lässt sich nicht immer verhindern. **Seine finanziellen Folgen lassen sich jedoch gezielt begrenzen.**

Eine Vertrauensschadenversicherung kann dabei ein wichtiger Bestandteil des betrieblichen Risikomanagements sein. Sie schützt – abhängig vom vereinbarten Versicherungsschutz – vor den finanziellen Folgen bestimmter vorsätzlicher und rechtswidriger Handlungen von Mitarbeitenden oder Dritten.

Sprechen Sie mit uns über Ihren individuellen Schutz. Wir analysieren gemeinsam mit Ihnen, welchen Risiken Ihr Unternehmen ausgesetzt ist und welche Absicherung sinnvoll ist.