

Vertrauensschadenversicherung

Category: Firmenkunden

27. Juli 2025



Unternehmen jeder Größe – vom kleinen Betrieb bis zum Mittelständler – sind auf die Ehrlichkeit ihrer Mitarbeiter und Geschäftspartner angewiesen. Doch die Realität der **Wirtschaftskriminalität** zeigt, dass dieses Vertrauen missbraucht werden kann. **Vertrauensschäden** entstehen durch vorsätzliche Handlungen wie Betrug oder **Unterschlagung**, die dem eigenen Unternehmen finanziell schaden. Umfragen zufolge waren [rund 51 % der Unternehmen bereits von derartigen Fällen betroffen](#). Eine *Vertrauensschadenversicherung* hilft, solche **existenzbedrohenden Straftaten** finanziell abzufedern.

In diesem Beitrag erklären wir Zweck und Nutzen der Vertrauensschadenversicherung, geben typische Schadenbeispiele, beschreiben zentrale Leistungen (versicherte Schäden, Ausschlüsse, Zusatzleistungen) und zeigen, wie man durch betriebliche Maßnahmen das Risiko minimieren kann. Außerdem grenzen wir sie von anderen Versicherungen wie **D&O** und **Cyber**-Policen ab.

Lesedauer: 7 Minuten

Was ist eine Vertrauensschadenversicherung?

Eine Vertrauensschadenversicherung schützt Unternehmen vor **Vermögensschäden durch vorsätzliche, vertrauensmissbräuchliche Handlungen** – sei es durch eigene Mitarbeiter (sogenannte *Vertrauenspersonen*) oder durch externe Dritte. Im Gegensatz zu einer Haftpflichtversicherung, die Schäden gegenüber Dritten abdeckt, greift die Vertrauensschadenversicherung bei **Eigenschäden** des Unternehmens. Das heißt, finanzielle Verluste des Betriebs infolge krimineller Handlungen werden vom Versicherer ersetzt. Diese Versicherung ist ausschließlich für Firmenkunden konzipiert und wird – trotz steigender Relevanz – bisher nur von wenigen Anbietern am Markt angeboten.

Zweck und Nutzen: Gerade in Branchen mit hohen Vertrauensvorschüssen (etwa Kanzleien, Beratungen, Finanzdienstleister) können einzelne kriminelle Handlungen zu erheblichen Verlusten führen. Die Vertrauensschadenversicherung ermöglicht hier einen *Risikotransfer*: das finanzielle Risiko wird vom Unternehmen auf den Versicherer verlagert. So lassen sich die Folgen von **Wirtschaftskriminalität** im Betrieb abmildern und die Handlungsfähigkeit des Unternehmens bleibt erhalten, selbst wenn intern einmal „etwas schiefgeht“.

Typische Schadenbeispiele aus der Praxis

Missbrauch von Vertrauen kann in jeder Branche vorkommen – sowohl in Büroumgebungen als auch in Produktion und Handwerk. Im Folgenden einige **Schadenbeispiele**, wie sie in der Praxis auftreten können:

- **Veruntreuung in der Buchhaltung:** Eine Buchhalterin einer Anwaltskanzlei überweist jahrelang insgesamt 150.000 € vom Kanzleikonto auf eigene Konten.

- **Diebstahl durch Insider und Komplizen:** Ein Prokurist verkauft in Absprache mit externen Komplizen firmeneigenes Altmetall privat und verursacht rund 300.000 € Schaden.
- **Betrug durch falsche Identität:** Betrüger bestellen unter dem Namen eines echten Kunden Waren im Wert von 120.000 € an eine falsche Adresse – die Lieferung ist bei der Zahlungsaufforderung längst verschwunden.
- **Fake-President-Trick:** Kriminelle geben sich per E-Mail oder Telefon als Geschäftsführer aus und weisen einen Mitarbeiter an, einen hohen Betrag auf ein Auslandskonto zu überweisen. Dabei nutzen sie Insiderwissen und sozialen Druck, um den **Täuschungsschaden** zu verursachen.

Diese Beispiele verdeutlichen die Bandbreite möglicher Vertrauensschäden – von klassischer **Unterschlagung** über **Social-Engineering**-Betrug wie Phishing bis zum komplexen **Fake-President-Fall**. Selbst kleine Unternehmen können Opfer solcher Machenschaften werden, da Täter oft gezielt dort zuschlagen, wo Kontrollen lückenhaft sind.

Versicherte Delikte und Leistungen

Versicherte Schäden: Die Vertrauensschadenversicherung deckt in der Regel eine Vielzahl von vorsätzlichen Straftaten ab, die das Firmenvermögen schädigen. Dazu zählen insbesondere **Diebstahl, Unterschlagung, Veruntreuung von Geld oder Gütern, Betrug** (z. B. gefälschte Zahlungsanweisungen oder Rechnungen) sowie **Urkundenfälschung**. Auch **Sabotage** an Maschinen oder die vorsätzliche **Zerstörung von Firmeneigentum** durch Mitarbeiter fällt unter den versicherten Eigenschaden. Wichtig: Versichert sind nicht nur Taten durch festangestellte Mitarbeiter, sondern je nach Police auch durch *vertrauensähnliche Personen* wie Auszubildende, Zeitarbeiter, Organe (Geschäftsführer, Vorstände) und in manchen Tarifen sogar durch externe Dienstleister, die für den Betrieb tätig sind.

Schäden durch Dritte: Viele Vertrauensschadenpolicen schließen explizit auch **kriminelle Handlungen Außenstehender** mit ein. Darunter fallen typische **Betrugsszenarien** oder **Social-Engineering-Angriffe**. Beispiele sind der oben erwähnte **Fake President**, **Bestellerbetrug** (gefälschte Bestellung mit abweichender Lieferadresse), **Payment Diversion** (Manipulation von Überweisungsdaten), **Phishing/Pharming** (Einschleusen gefälschter Webseiten/E-Mails zum Datendiebstahl) oder Man-in-the-Middle-Angriffe. Auch **Betriebsspionage** kann mitversichert sein, also der Diebstahl von Geschäftsgeheimnissen zu fremdem Nutzen. Selbst wenn durch einen Cyberangriff der Geschäftsbetrieb zeitweise lahmgelegt wird (z. B. Online-Shop nicht nutzbar), bieten einige Vertrauensschadenversicherer dafür Deckung in Form von Ersatz entgangener Erlöse oder Mehrkosten. Wichtig ist, dass bei Schäden durch Dritte meist ein strafrechtlicher Hintergrund (eine vorsätzliche Bereicherungsabsicht) vorliegen muss – reine technische Defekte oder Bedienfehler sind nicht abgedeckt.

Leistungsumfang: Im Schadensfall ersetzt die Versicherung den **direkten Vermögensschaden** – also den finanziellen Verlust, der dem Unternehmen entstanden ist. Darüber hinaus werden oft diverse **Folgekosten** übernommen. Dazu gehören typischerweise:

- **Schadenermittlung und -aufklärung:** Kosten für Wirtschaftsprüfer, Detektive oder Forensiker, um den Tathergang und die Schadenshöhe festzustellen.
- **Rechtskosten:** Kosten für die Strafverfolgung des Täters oder Abwehr von unberechtigten Ansprüchen Dritter.
- **Drittschäden:** Falls das Unternehmen einem Kunden oder Partner haften muss (z. B. weil ein Mitarbeiter Kundengelder veruntreute), übernimmt die Police auch diesen Fremdschaden.
- **Public-Relations-Kosten:** Honorare für PR-Agenturen, um Reputationsschäden zu begrenzen und das Vertrauen von Kunden und Öffentlichkeit zurückzugewinnen.
- **Datenwiederherstellung:** Kosten, um gelöschte oder

manipulierte Daten, Software und Dateien wiederzubeschaffen bzw. zu rekonstruieren.

- **Betriebsunterbrechungskosten:** Mehrkosten, um den Geschäftsbetrieb aufrechtzuerhalten (z. B. temporäre externe Dienstleistungen), gerade wenn IT-Systeme sabotiert wurden. Teilweise werden sogar Vertragsstrafen ersetzt, wenn sie unmittelbar durch den Versicherungsfall ausgelöst wurden.
- **Psychologische Betreuung:** Einige Tarife schließen die Kosten für eine psychologische Betreuung von betroffenen Mitarbeitern oder Führungskräften mit ein, um nach einem Vertrauensbruch die Verarbeitung des Erlebnisses zu unterstützen.

Dieser breite Leistungsumfang zeigt, dass es sich um eine **Pauschaldeckung** handelt, die über den reinen Geldverlust hinausgeht. Die Versicherung soll helfen, den Betrieb trotz Vorfalls schnell wieder auf Kurs zu bringen – finanziell wie organisatorisch. Allerdings sind je nach Versicherer Sublimits (Obergrenzen) für gewisse Kostenarten üblich. So können z. B. PR-Kosten oder psychologische Betreuung auf bestimmte Beträge pro Schaden begrenzt sein.

Typische Ausschlüsse und Einschränkungen in der Vertrauensschadenversicherung

Trotz des umfassenden Schutzes gibt es auch in der Vertrauensschadenversicherung **Grenzen des Versicherungsschutzes**. Typische Ausschlussklauseln und Einschränkungen sind:

- **Bereits bekannte Unredlichkeit:** Schäden durch Personen, die dem Unternehmen schon vor dem Versicherungsabschluss (oder vor der Tat) als unzuverlässig oder unehrlich aufgefallen waren, sind vom Schutz ausgeschlossen. Unternehmen sollen keine bekannten „schwarzen Schafe“

weiter beschäftigen in Erwartung der Versicherungsleistung.

- **Vorsatz der Unternehmensleitung:** Handelt ein Inhaber, Vorstand oder Geschäftsführer selbst kriminell gegen das eigene Unternehmen, besteht in der Regel kein Versicherungsschutz. Solche **Eigenhandlungen von Organen** fallen nicht unter den Begriff der versicherten Vertrauensperson (hier würde eher ein **D&O-Fall** vorliegen, der aber Vorsatz ebenfalls ausschließt).
- **Nicht versicherbare Risiken:** Ganz allgemein ausgeschlossen sind Schäden, die anderswo versicherbar sind (z. B. Einbruchdiebstahl durch Außenstehende – dafür ist die Sachversicherung zuständig). Ebenso wenig versichert sind Krieg, Terror, Kernenergie und ähnliche **systemische Risiken**.
- **Inventurdifferenzen und schleichende Verluste:** Verluste, die nur als Fehlbestand bei Inventuren auffallen, ohne dass ein konkreter Vertrauensbruch nachweisbar ist, werden meistens nicht ersetzt. Es muss also ein feststellbarer Delikt zugrunde liegen, kein bloßes "Schwund".
- **Indirekte Schäden:** *Mittelbare Schäden* wie **entgangener Gewinn** oder vertraglich vereinbarte **Vertragsstrafen** wegen Verzögerungen sind oft ausgeschlossen oder nur begrenzt versicherbar. Zwar bieten einige Tarife hier begrenzte Deckungen an (siehe oben), doch der Fokus liegt auf dem unmittelbar entstandenen Schaden.
- **Obliegenheitsverletzungen:** Wie bei jeder Versicherung müssen bestimmte **Sicherheitsvorschriften und Obliegenheiten** eingehalten werden. Beispielsweise können grobe Verstöße gegen interne Kontrollen oder unterlassene Sorgfaltspflichten bei der Auswahl von Mitarbeitern den Versicherungsschutz gefährden. Kommt das Unternehmen Melde- und Aufklärungspflichten im Schadenfall nicht nach, kann dies ebenfalls leistungsfrei stellen.

Unter dem Strich soll die Vertrauensschadenversicherung für **unvorhersehbare, trotz zumutbarer Vorkehrungen eintretende Vertrauensbrüche** eintreten – nicht aber für solche, die der Versicherungsnehmer durch Nachlässigkeit oder bewusste Inkaufnahme mitverursacht hat. Eine sorgfältige Vertragsgestaltung und Beratung sind wichtig, um Deckungslücken oder Überschneidungen mit anderen Policen zu vermeiden.

Risikominimierung im Betrieb

Eine wichtige Erkenntnis: Prävention im Unternehmen ist der erste Schutz vor Vertrauensschäden. Versicherer erwarten oft, dass Betriebe angemessene **Sicherheitsmaßnahmen** etabliert haben – und für die eigene Schadensbilanz ist dies ohnehin sinnvoll. Hier einige bewährte Maßnahmen, um das Risiko zu senken:

- **Vier-Augen-Prinzip:** Führen Sie bei sensiblen Vorgängen (z. B. Überweisungen, Kassenbestände) stets eine Gegenkontrolle durch eine zweite Person durch. Mindestens zwei Unterschriften bei größeren Zahlungsvorgängen sind empfehlenswert. Diese interne Kontrolle erschwert Solo-Betrügereien erheblich.
- **Aufgabentrennung:** Trennen Sie Verantwortlichkeiten, etwa zwischen Buchhaltung und Zahlungsfreigabe oder zwischen Einkauf und Rechnungsprüfung. So vermeiden Sie, dass eine Person einen kompletten Prozess allein kontrolliert – was Missbrauch erleichtern würde.
- **Sorgfältige Personalauswahl:** Prüfen Sie neue Mitarbeiter – vor allem in vertrauensvollen Positionen – genau. Holen Sie **Referenzen** früherer Arbeitgeber ein und lassen Sie sich ggf. ein polizeiliches Führungszeugnis vorlegen. Eine genaue Auswahl kann *Wiederholungstäter* filtern und ein Signal setzen, dass man genau hinschaut.
- **Klare Prozesse & Schulungen:** Sensibilisieren Sie Ihre Belegschaft regelmäßig für aktuelle Betrugsmaschen

(**Social Engineering, Phishing, Fake President**). Schaffen Sie klare Handlungsanweisungen: etwa wie sich Mitarbeiter bei dubiosen Zahlungsaufforderungen verhalten sollen und an wen sie sich wenden können. Wenn Mitarbeiter wissen, dass im Zweifel immer intern rückgefragt werden muss, lässt sich mancher Schaden im Keim ersticken.

- **Technische Schutzmaßnahmen:** Implementieren Sie aktuelle **IT-Sicherheitsmaßnahmen**. Eine starke Firewall, aktuelle Antivirensoftware und vor allem regelmäßige **Backups** sind Pflicht. Viele Attacken von außen (z. B. Schadsoftware, Datendiebstahl) können so vereitelt oder ihre Auswirkungen begrenzt werden.
- **Regelmäßige Revision und Kontrolle:** Führen Sie interne oder externe Audits in unregelmäßigen Abständen durch. Eine unabhängige Prüfung entdeckt ungewöhnliche Geldabflüsse oder Manipulationen oft, bevor der Schaden eskaliert. Wichtig ist jedoch, dass Prüfungen überraschend und vertieft stattfinden – einfache Routineprüfungen, mit denen Täter rechnen, reichen nicht aus.

All diese Maßnahmen reduzieren die Gefahr von Vertrauensschäden beträchtlich. Dennoch gilt: Einen **100%igen Schutz** gibt es nicht – gerade **innovative Betrugsmaschen** entwickeln sich ständig weiter. Die Kombination aus Prävention und Versicherungsschutz bietet den umfassendsten Schutz: Interne Kontrollen verhindern viele Delikte, und wenn doch ein gravierender Fall passiert, federt die Vertrauensschadenversicherung die finanziellen Folgen ab.

Abgrenzung zur D&O- und Cyber-Versicherung

Die Vertrauensschadenversicherung überschneidet sich in

einigen Bereichen mit anderen Versicherungen des Unternehmens. Wichtig ist zu verstehen, wofür sie gedacht ist und wofür andere Policen einspringen.

D&O-Versicherung (Managerhaftpflicht): Eine D&O (Directors and Officers)-Versicherung schützt die Organe eines Unternehmens (Geschäftsführer, Vorstände, Aufsichtsräte) vor Haftungsansprüchen, wenn ihnen bei der Geschäftsführung Fehler unterlaufen. Sie deckt **Vermögensschäden durch fahrlässige Pflichtverletzungen** der Unternehmensleitung ab – **vorsätzliche** Schädigungen hingegen sind bei D&O immer ausgeschlossen. Genau hier kommt die Vertrauensschadenversicherung ins Spiel: Sie deckt **vorsätzliche Handlungen von Mitarbeitern oder Führungskräften** ab, die das Unternehmen selbst schädigen. Damit schließt sie eine **Deckungslücke** der D&O-Versicherung. Ein Beispiel: Veruntreut ein Geschäftsführer firmeneigene Gelder („schwarze Kasse“), greift die D&O nicht, wohl aber die Vertrauensschadenversicherung. Beide Versicherungen ergänzen sich also – die eine schützt vor Managementfehlern, die andere vor krimineller Energie im Unternehmen. Wichtig: Die Vertrauensschadenversicherung schützt damit indirekt auch die Bilanz und kann verhindern, dass in solchen Fällen die Firma selbst oder die D&O-Versicherung den Schaden tragen muss. Es handelt sich jedoch um getrennte Verträge; eine gesetzliche Pflicht zum Abschluss einer Vertrauensschadenversicherung besteht (noch) nicht, doch im Rahmen des Risikomanagements sollte sie je nach Risikolage geprüft werden.

Cyber-Versicherung: Viele wirtschaftskriminelle Handlungen haben heute eine **Cyber-Komponente** – und umgekehrt können Cyberangriffe zu Vertrauensschäden führen. Grundsätzlich fokussiert die Cyber-Versicherung auf **technische IT-Risiken**, also z.B. Hackerangriffe, Datenlecks, Systemausfälle und deren Folgen. Sie übernimmt oft IT-Dienstleisterkosten, Datenwiederherstellung, Benachrichtigung von Betroffenen bei Datenpannen, Cyber-Erpressung und Betriebsunterbrechung infolge eines Cybervorfalles. Überschneidungen mit der

Vertrauensschadenversicherung gibt es bei **Angriffen, die sowohl IT- als auch Betrugselemente** enthalten. Beispiel **Fake President Fraud**: Hierbei handelt es sich um einen Cyber-gestützten Betrug (E-Mail-Fälschung plus social engineering). Eine Cyber-Versicherung würde in einem solchen Fall z.B. für die **Datenforensik und Systemwiederherstellung** nach dem Angriff und evtl. für **Betriebsunterbrechung** aufkommen, während die Vertrauensschadenversicherung den **abgeflossenen Geldbetrag** ersetzt. Ähnlich verhält es sich bei Phishing-basierten Überweisungsdiebstählen. **Social-Engineering-Schäden** waren in der Vertrauensschadenversicherung schon abgedeckt, lange bevor Cyber-Policen diese als Zusatzbaustein angeboten haben. Allerdings sind reine Cybervorfälle ohne menschliches Betrugselement (etwa ein externer Hacker stiehlt Geld direkt durch eine Sicherheitslücke) teilweise nicht vom Vertrauensschadenschutz erfasst – hier greift dann nur die Cyber-Versicherung. In der Praxis werden beide Versicherungen oft **kombiniert abgeschlossen**, um Lücken zu vermeiden und umfassend gegen sowohl **Computerkriminalität** als auch **Vertrauensdelikte** geschützt zu sein. Zudem enthalten Vertrauensschadenversicherungen häufig eine **Subsidiaritätsklausel**: Sie leisten nur, wenn keine andere Versicherung greift. Dadurch wird geregelt, dass erst eine eventuell vorhandene Cyber- oder andere Police zahlt, bevor der Vertrauensschadensversicherer eintritt – Doppelversicherungen werden vermieden. Für den Versicherten ist daher wichtig, beide Policen sauber aufeinander abzustimmen, um weder Lücken noch Überschneidungen im Schutz zu haben.

Fazit: Für wen ist die Vertrauensschadenversicherung sinnvoll?

Vertrauensschadenversicherungen bieten einen wichtigen Schutz vor den finanziellen Folgen von **Wirtschaftskriminalität im**

Unternehmen. Insbesondere **kleine und mittlere Unternehmen**, die oft weniger ausgefeilte Kontrollmechanismen als Großkonzerne haben, profitieren von dieser Deckung. Branchen wie Kanzleien, Beratungsunternehmen, Agenturen oder VC-Firmen, in denen wenige Personen Zugriff auf große Werte oder sensible Daten haben, sollten das Risiko eines Vertrauensschadens nicht unterschätzen. Aber auch produzierende Unternehmen und Handwerksbetriebe können Opfer von **Untreue, Diebstahl oder Betrug** aus den eigenen Reihen oder durch Außenstehende werden.

Die Vertrauensschadenversicherung ersetzt zwar nicht eine gute Prävention – aber sie ist eine wertvolle **Sicherheitsnetz-**Maßnahme. Unternehmerisch denkende Leser sollten im Rahmen ihres Risikomanagements prüfen, ob diese Versicherung zu ihrem Betrieb passt. Im Idealfall **kombiniert** man robuste interne Kontrollen mit einer Vertrauensschadenversicherung als Auffanglösung. So können Sie ruhig schlafen, weil Sie wissen: Sie haben *Ihr Möglichstes getan*, um sowohl vorbeugend als auch reaktiv gegen **Vertrauensmissbrauch** gewappnet zu sein. Eine individuelle Beratung durch einen spezialisierten Versicherungsmakler kann helfen, den passenden Deckungsumfang zu ermitteln und die Verträge auf Ihren Bedarf zuzuschneiden.

Benötigen Sie Versicherungsschutz für Ihr Unternehmen, [nehmen Sie gerne Kontakt mit uns auf.](#)

© Foto: Mohamed Hassan (Pixabay)