Allianz Trade

Wirtschaftskriminalität – neue Technologien, neue Betrugshorizonte

Aktuelle Trends, ein kriminologischer Blick auf Täterprofile und Motive – und die Frage: Wie können Unternehmen sich schützen?

Euler Hermes Deutschland
Niederlassung der Euler Hermes SA
22746 Hamburg
Tel. +49 (0) 40 / 88 34 - 0
Fax +49 (0) 40 / 88 34 - 77 44
info.de@allianz-trade.com
www.allianz-trade.de

Die „Schwachstelle Mensch“ als Unternehmensrisiko

Es bleibt eine unbequeme Wahrheit für Unternehmen und eine unterschätzte Gefahr: Innentäter, also die eigenen Mitarbeitenden, richten weiterhin die meisten und in Summe auch die höchsten Schäden an. Aber: Die externen Täter holen sukzessive auf – nicht zuletzt aufgrund der digitalen Transformation und der technologischen Entwicklung.

Besonders interessant wird es bei sogenannten „Social Engineering“-Betrugsfällen, also beispielsweise Fake President, Zahlungs- oder Bestellerbetrug. Hier geht der Betrugsversuch zwar von externen Tätern aus – die allerdings die „Schwachstelle Mensch“ bei den Mitarbeitenden nutzen und diese manipulieren. Und obwohl diese Maschen nicht neu sind, obwohl viele Unternehmen ihre Mitarbeitenden sensibilisieren, nehmen die Fallzahlen weiterhin zu.

Doch warum können Menschen gehackt und manipuliert werden? Wie bringen die „Social Engineers“ ihre Opfer dazu, nachweislich illegale Aktivitäten durchzuführen wie zum Beispiel Überweisungen ohne das geltende 4-Augen-Prinzip? Warum werden oft ausgerechnet langjährige Mitarbeitende zu Tätern? Was motiviert sie? Welche Täterprofile gibt es – und vor allem: Wie können Unternehmen sich schützen?

In einer Analyse von Oktober 2022 haben wir bereits festgestellt: Die größten Schäden verursachen männliche Täter im Alter zwischen 40 und Mitte 50, gebildet, in gehobener oder leitender Position im Finanzwesen mit mindestens 10 Jahren Betriebszugehörigkeit.

Im vorliegenden Ratgeber wollen wir nun zusammen mit dem Rechtswissenschaftler und Kriminologen Prof. Dr. Hendrik Schneider den Versuch unternehmen, die Motive von Wirtschaftsstraftätern kriminologisch zu erklären und – darauf basierend – Unternehmen Tipps an die Hand zu geben, wie sie Wirtschaftskriminalität bekämpfen und sich vor Angriffen durch interne wie externe Täter (bestmöglich) schützen können.

Ihr Allianz Trade-Team

INHALT

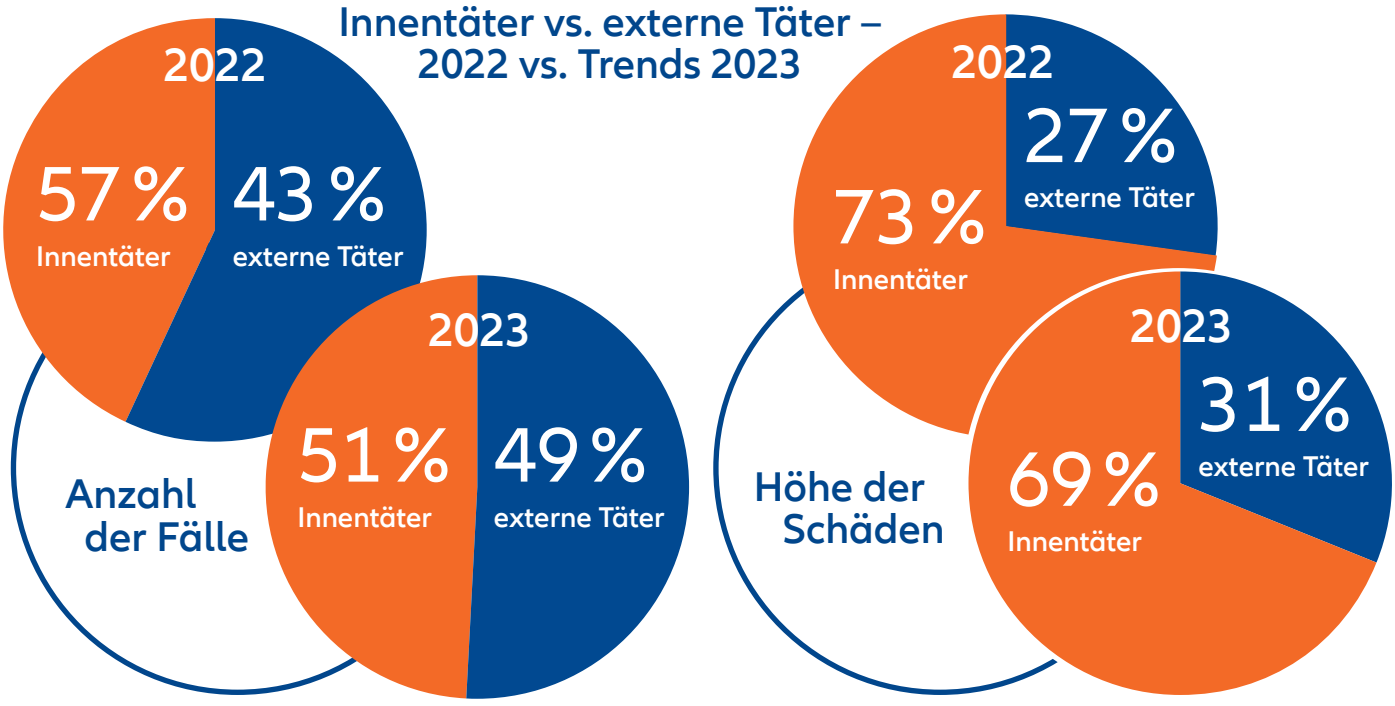
Aus der Allianz Trade Schadensstatistik

Eine Vertrauensschadenversicherung (VSV) von Allianz Trade schützt Unternehmen gegen finanzielle Schäden, die durch zielgerichtete kriminelle Handlungen entstehen – sowohl durch sogenannte „Innentäter" (z. B. Mitarbeitende, Zeitarbeitskräfte) als auch durch externe Dritte (z. B. Hacker). Ein Blick in unsere Schadensstatistik liefert spannende Erkenntnisse.

Wirtschaftskriminelle surfen auf der Homeoffice-Welle

Wirtschaftskriminelle schlagen immer häufiger zu und es sind deutlich mehr Unternehmen betroffen als in den Vorjahren. Vor allem Delikte durch externe Täter steigen zuletzt rasant an. 2022 haben Innentäter rund 57 % der Fälle verursacht.

2023 zeichnet sich ein anderes Bild: Der Anteil der internen Täter ist mit 51 % zu 49 % durch externe Täter bisher nahezu ausgeglichen. Bei der Höhe der Schäden bleibt die Wahrheit für Unternehmen allerdings weiterhin unbequem: Die eigenen Mitarbeitenden richten nach wie vor die größten Schäden an. Allerdings setzen auch hier die externen Täter zu einer Aufholjagd an und holen sukzessive auf.



Quelle: Allianz Trade Schadensstatistik

Unter Allianz Trade werden verschiedene Dienstleistungen von Euler Hermes angeboten.

Die Allianz Schadensstatistik zeigt: Von Social-Engineering-Betrugsmaschen sind Unternehmen jeglicher Größe und aus nahezu allen Branchen betroffen. Dennoch findet sich zuletzt eine Tendenz bei den Branchen, die besonders häufig Opfer von Hackern wurden.

Die „Menschen-Hacker“ erleben seit Jahren einen Boom

„Social Engineering“, also Betrugsmaschen, bei denen die Täter Menschen manipulieren, erlebt seit vielen Jahren einen Boom. Diese Betrugsmasche macht inzwischen rund ein Viertel aller bei Allianz Trade gemeldeten Schäden aus.

Social-Engineering-Betrugsfälle sind 2022 im Vergleich zum Vorjahr um etwa 18 % angestiegen. Dieser Trend setzt sich auch 2023 im bisherigen Jahresverlauf fort.

+ 400 %
Social-Engineering-Betrugsfälle haben sich seit 2014 verfünffacht

+ 18 %
Anstieg der Social-Engineering-Betrugsfälle 2022 vs. 2021

Insbesondere Zahlungsbetrug (Payment Diversion), also das Umleiten von Geldströmen, erfreut sich in den letzten Jahren immer größerer Beliebtheit im Portfolio der Wirtschaftskriminellen, die sich dabei auch den stetigen technischen Fortschritt zunutze machen.

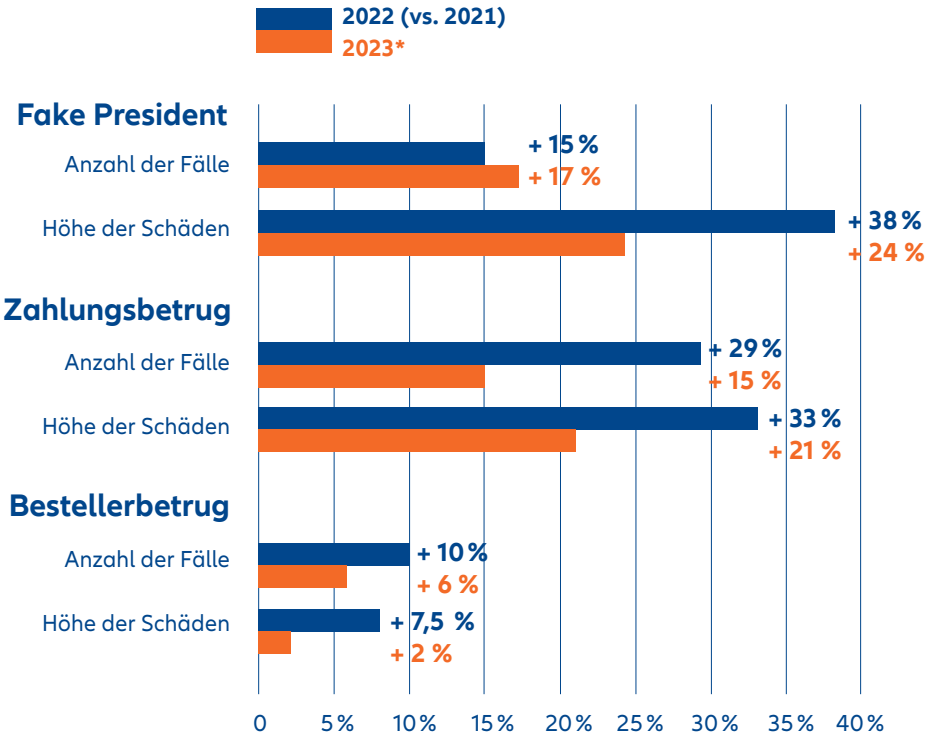
Quelle: Allianz Trade Schadensstatistik

Die falschen Chefs kommen wieder in Mode

Besonders spannend ist: Seit 2022 erlebt der „Fake-President"-Betrug ein Revival. 2022 verzeichneten Schäden durch die falschen Chefs einen Zuwachs von 38 %, bei der Anzahl der Fälle war es ein Plus von 15 %.

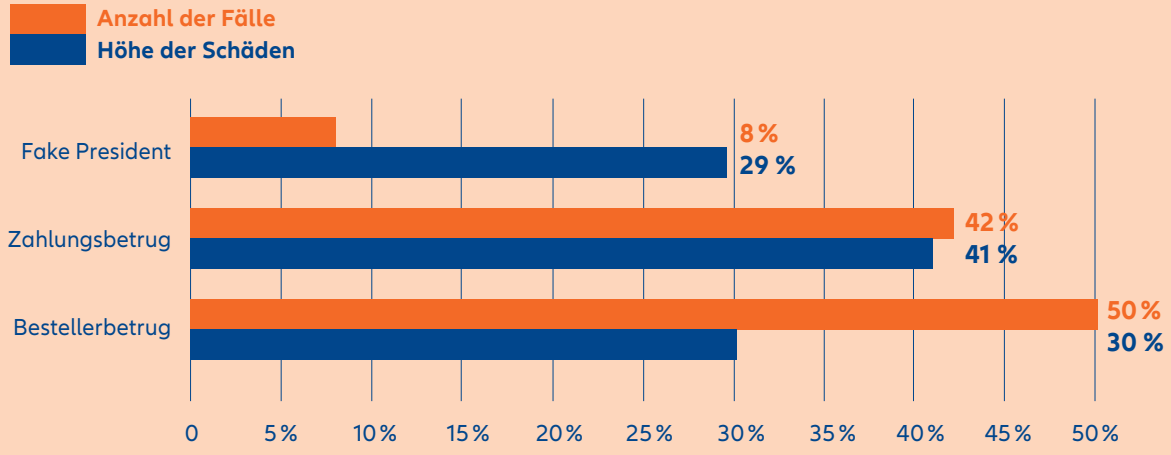
Viele Jahre stagnierten zuvor die Fallzahlen und die Höhe der Schadenssummen pro Fall ging sukzessive zurück. Die Schadenssummen liegen beim „Fake President"-Betrug inzwischen in den meisten Fällen nur noch im hohen sechsstelligen oder niedrigen einstelligen Millionen-Bereich. Zwischen 2014 und 2017 verursachten die Betrüger häufig noch Schäden zwischen 10 und 50 Mio. EUR.

Trends in Zahlen: Veränderung von Fallzahlen und Schadenhöhe



** Allianz Trade Schätzung basierend auf dem bisherigen Trend im Jahr 2023*

Zahlungsbetrug richtet 2022 insgesamt die größten Schäden an



Quelle: Allianz Trade Schadensstatistik

73.144

Wirtschaftskriminalitätsdelikte verzeichnete das BKA in Deutschland 2022 (+ 42,6 %).

Quelle: Polizeiliche Kriminalstatistik 2023

15 %

der betroffenen Unternehmen gaben an, einen Schaden von mehr als 1 Mio. Euro erlitten zu haben – ein Plus von 50 % im Vergleich zu 2020.

Quelle: KMPG, Studie Wirtschaftskriminalität in Deutschland 2023

2,1 Mrd. Euro

So hoch waren die Schäden von Unternehmen durch Wirtschaftskriminalität 2022 in Deutschland.

Quelle: Statista, Juli 2023

81 %

der deutschen Unternehmen schätzen das Risiko Wirtschaftskriminalität **für andere Unternehmen** als hoch ein.

Quelle: KMPG, Studie Wirtschaftskriminalität in Deutschland 2023

34 %

der Unternehmen schätzen das Risiko, **selbst** von Wirtschaftskriminalität betroffen zu sein, als hoch ein.

Quelle: KMPG, Studie Wirtschaftskriminalität in Deutschland 2023

Wirtschaftskriminalität: weiter steigende Fallzahlen

Die Schäden, die durch Wirtschaftskriminalität entstehen, sind hoch. Viele Unternehmen sehen zwar die Gefahr – aber mehr für andere als für sich selbst. Phishing-Delikte sind stark gestiegen. Neben Ransomware sind aber auch „Social Engineering"-Betrugsmaschen weiterhin auf dem Vormarsch – auch dank künstlicher Intelligenz wie ChatGPT.

26 %

der erfolgreichen Cyberangriffe auf deutsche Unternehmen waren „Social Engineering"-Fälle wie beispielsweise Fake President. Gemeinsam mit Phishing und Ransomware bildet Social Engineering die Top 3 der Betrugsmaschen.

Quelle: TÜV Cybersecurity Studie 2023

2,7 Mrd. USD

an Schäden entstanden rund 22.000 Unternehmen weltweit durch Social Engineering im Jahr 2022. Das ist ein Plus von 14 % im Vergleich zum Vorjahr.

Quelle: FBI Internet Crime Report 2023

38 %

Die Höhe der Schäden durch Fake President verzeichnete 2022 plötzlich wieder einen Anstieg von 38 %.

Quelle: Allianz Trade Schadensstatistik

57 %

An 57 % aller Wirtschaftsdelikte sind Innentäter beteiligt, in 31 % der Fälle begehen sie die Tat im Alleingang.

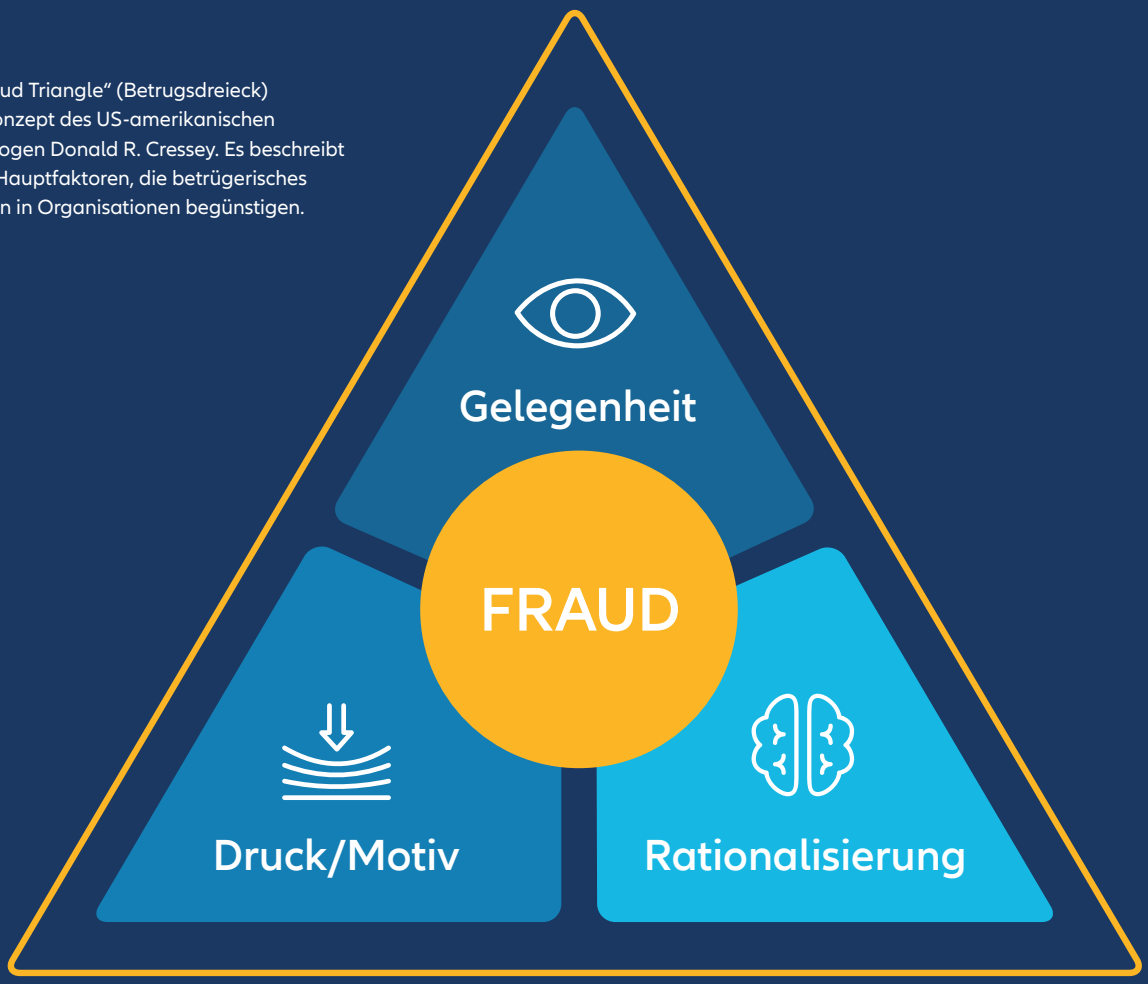
Quelle: PWC, Studie Wirschaftskriminalität 2022

46 %

der Unternehmen weltweit waren in den Jahren 2021 bis 2022 Opfer von Wirtschaftsdelikten, in Deutschland waren dies rund 40 %.

Quelle: PWC, Studie Wirtschaftskriminalität 2022

Das „Fraud Triangle“ (Betrugsdreieck) ist ein Konzept des US-amerikanischen Kriminologen Donald R. Cressey. Es beschreibt die drei Hauptfaktoren, die betrügerisches Verhalten in Organisationen begünstigen.



Warum werden Täter zu Tätern?

Ein bekanntes Sprichwort sagt: „Gelegenheit macht Diebe“. Aber das kann nur die halbe Wahrheit sein, denn nur weil es eine Tatgelegenheit gibt, begeht ja nicht automatisch jeder eine kriminelle Handlung. Was trägt also noch dazu bei, dass aus Menschen Täter werden? Und inwiefern können Unternehmen hier entgegenwirken?

Das bekannte sogenannte „Fraud Triangle“[1] des Kriminologen Donald R. Cressey liefert hierzu einige interessante Ansatzpunkte. Ihm zufolge müssen drei Faktoren gleichzeitig vorliegen: eine Tatgelegenheit, Druck (bzw. eine entsprechende Motivation) und die sogenannte „Rationalisierung“, also die Rechtfertigung der eigenen Tat. Die Gelegenheit ist sicherlich der bekannteste Aspekt – es liegt ja auch auf der Hand, dass ohne Gelegenheit eine Tat gar nicht stattfinden kann. Gleichzeitig muss ein Täter aber auch über die erforderliche Kompetenz verfügen und davon ausgehen können, dass es nur eine geringe Wahrscheinlichkeit gibt, entdeckt zu werden. Bei der Prävention von Wirtschaftskriminalität spielt dieser Aspekt bisher häufig eine Hauptrolle: Unternehmen verstärken ihre internen Kontrollmechanismen, um Tatgelegenheiten zu reduzieren.

Damit Menschen kriminell werden, bedarf es in der Regel aber noch mehr. In den meisten Fällen ist das ein erheblicher Druck. Dieser kann viele Facetten haben: Zeitdruck, Leistungsdruck, Lösungsdruck, fehlende Ressourcen, hierarchischer, gesellschaftlicher oder emotionaler Druck, Gruppenzwang, der Druck, gefallen zu wollen, Erwartungsdruck (von anderen oder an sich selbst) und natürlich finanzieller Druck können alle dafür verantwortlich sein, dass ein Mensch zum Täter wird.

Cressey beschreibt Druck auch als „non-sharable information“[2]. Das bedeutet, dass eine Person eine Lebenssituation als derart beschämend empfindet, dass sie sich nicht traut, mit dieser offen umzugehen oder sie mit ihrem Umfeld zu teilen. Das kann eine finanzielle Notlage sein, aber auch Spiel- oder Kaufsucht oder die Scham, dass wie bei der „Pig Butchering“-Masche Intimitäten an die Öffentlichkeit gelangen.

Viele Betrugsmaschen, insbesondere das „Social Engineering“, setzen genau hier an. Bei der bekannten „Fake President“-Masche zum Beispiel geben sich Kriminelle als Vorgesetzte aus und verleiten Angestellte zu größeren Geldüberweisungen: Die Masche funktioniert, weil sie Menschen im Kern berührt. Sie setzt genau dort an, wo menschliche Anschlusspunkte sind – etwa in Form von Wertschätzung, nach der jeder Mensch intrinsisch sucht. Aber auch andere Facetten von Druck, z. B. das Vorgaukeln einer vermeintlichen Krisensituation, können dabei eine entscheidende Rolle spielen.

Die dritte Seite des „Teufelsdreiecks“ ist die Rechtfertigung. Wenn Menschen etwas tun, was nicht in Ordnung ist, müssen sie das innerlich rechtfertigen, um ihr eigenes Selbstbild aufrecht zu erhalten. „Ich arbeite so viel, das habe ich verdient.“ Oder: „Ich bin das eigentliche Opfer, und das steht mir eigentlich zu.“ Oder: „Das tut dem Unternehmen jetzt nicht weh.“ Oder: „Das wurde von mir verlangt.“

Die inneren Bewältigungs- bzw. Rechtfertigungsstrategien sind vielfältig, oft aber von außen nur schwer durchschaubar. Denn nur in seltenen Fällen, wie beispielsweise bei Gerichtsprozessen, treten sie überhaupt ans Tageslicht – und auch dann nur in Ansätzen. Zudem gibt es bestimmte Täterprofile[3] und Persönlichkeitsstrukturen[4], bei denen diese Rechtfertigung nur sehr gering ausgeprägt ist.

Dennoch lohnt es sich für Unternehmen, diese beiden bisher oft eher vernachlässigten Aspekte bei ihren Präventionsbestrebungen mit zu berücksichtigen. Denn gerade die Unternehmens- und Fehlerkultur spielen hier eine große Rolle: Sehr autoritäre Führungsstile, eine absolute Ergebnisorientierung („Koste es, was es wolle“) oder eine „Mach’ es einfach, egal wie“-Kultur können Wirtschaftskriminalität erheblich fördern. Eine gesunde Fehlerkultur und eine gute Balance zwischen Kontrolle und Vertrauen (siehe auch Seite 20/21) hingegen können das Risiko krimineller Mitarbeitenden deutlich reduzieren.

[1] Cressey, D. R. (1953), Other people’s money; a study of the social psychology of embezzlement

[2] Cressey, D. R., The Criminal Violation of Financial Trust, American Sociological Review Volume: 15 (1950), Seiten 738-743

[3] Prof. Dr. Henridk Schneider/Rölfs WP Partner AG (2009), Der Wirtschaftsstraftäter in seinen sozialen Bezügen

[4] Benjamin Schorn (2022), Gier, Macht, Scham – Motive krimineller Manager psychologisch erklärt

Neue Technologien – neue (Betrugs-)Horizonte

Neue Technologien, künstliche Intelligenz und Anwendungen wie Chat GPT sind ein Quantensprung bei der Nutzung von Daten und haben viele Vorteile. Viele Prozesse können vereinfacht oder effizienter gestaltet werden. Aber es gibt eine Kehrseite der Medaille: Sie machen es auch Betrügern einfacher. Gerade beim „Social Engineering", dem Manipulieren von Menschen, birgt dies viele Gefahren.

Betrüger schlafen nicht, sie gehen mit der Zeit und nutzen alle ihnen zur Verfügung stehenden Technologien. So gab es bei Allianz Trade vor einigen Jahren den ersten Fake-President-Fall, bei dem wir davon ausgehen, dass Audio Deepfakes genutzt wurden. Seither gab es vereinzelt Fälle, bei denen eine Stimmfälschung nicht ausgeschlossen werden konnte, bei denen die Indizien aber wesentlich weniger eindeutig waren. Die Zeit und die Technologie waren – zumindest in der Breite – wohl noch nicht reif für eine große Skalierung, der Aufwand vermutlich noch zu hoch.

Audio Deepfakes: Software mit Quantensprung in den letzten Jahren

Aber: Die frei zugängliche Software zum Klonen von Stimmen hat in den letzten Jahren einen Quantensprung gemacht. Vorbei die Zeiten, in denen die Stimme vom Band blechern klang und selbst bei schlechten Handyverbindungen in den meisten Fällen keine allzu große Verwechslungsgefahr bestand. Ein aktueller Selbstversuch (probieren Sie es aus!) mit einschlägigen KI-Programmen endet allerdings mit faszinierenden und gleichzeitig erschreckenden Ergebnissen. Es dürfte also nur eine Frage der Zeit sein, bis diese Anwendungen auch in der Breite ihre Anwendung finden. Der „Break Even"-Punkt, an dem sich eine Anwendung für Betrüger lohnt, dürfte nicht mehr weit sein.

Fake President-Fälle: Wieder steigende Fallzahlen – und die Frage nach dem Warum

Es geht aber auch klassisch, ganz ohne Audio: Bei der Fake-President-Masche gibt sich ein Betrüger als vermeintlicher Vorgesetzter aus, der Angestellte z. B. zu größeren Überweisungen veranlasst. Gerade bei diesen klassischen Fake-President-Fällen verzeichnete Allianz Trade im vergangenen Jahr wieder einen Zuwachs – gegen den Trend der Vorjahre (stagnierende Fallzahlen bei dieser Betrugsmasche und niedrigere Schadenshöhen als noch zu „Hoch-Zeiten" mit Rekordschäden von über 50 Millionen Euro). Nun also wieder ein Anstieg – und die damit verbundene Frage nach dem Warum.

Chat GPT und die Betrugs-E-Mails auf Knopfdruck im „CEO Style"

Chat GPT ist neu, die gemeldeten Schäden stehen also (noch) nicht im Zusammenhang mit dieser KI-Anwendung, auch wenn diese den Betrügern ganz neue Horizonte eröffnet: Mussten sie zuvor noch relativ mühsam die notwendigen Informationen zusammensuchen, etwa durch Ausspähen des Intranets, öffentlich zugänglichen Informationen in sozialen Netzwerken oder Vishing-Anrufen an unterschiedlichsten Stellen im Unternehmen, findet mit ChatGPT eine deutliche „Optimierung" statt: Die Software wird einfach mit Daten gefüttert (beispielsweise Mitarbeiterbriefe, Intranet-Inhalte oder E-Mail-Korrespondenzen) und spuckt anschließend eine E-Mail mit einer gefälschten Zahlungsaufforderung im „CEO Style" aus. Das hebt die Authentizität der Korrespondenz auf ein ganz neues Level und damit auch die Chancen, dass die „Social Engineers" erfolgreich sind.

Faktor Druck: „Jetzt bloß nichts falsch machen“

Aber mal ganz weg von den technischen Neuerungen, die auch an Betrügern nicht vorbei gehen: Warum funktioniert diese Masche überhaupt? Weil sie dort ansetzt, wo wir Menschen im Kern berührt werden, wo wir Schnittstellen und (emotionale) Anknüpfungspunkte haben: Wertschätzung ist ein gutes Beispiel – oder eben auch Druck. Dieser kann ganz viele Facetten haben, zeitlicher Druck etwa, finanzieller Druck, Erfolgsdruck, aber auch Scham. Mehrere „persönliche Baustellen“ gleichzeitig, wie beispielsweise Doppelbelastung im Homeoffice mit Kindern zu Hause, führen ebenfalls schnell zu Überlastung und Zerstreutheit und unter anderen Umständen möglicherweise vermeidbaren Fehlern. Auch der Druck, den Vorgesetzten gefallen zu wollen, kann eine Rolle spielen. Bloß nicht den Job verlieren in diesen schwierigen Zeiten, in denen die Inflation durch die Decke geht und mein Kredit plötzlich doppelt so teuer ist. In Analogie zum „Fraud Triangle“ ist bei der Fake-President-Masche der Druck sicherlich die dominierende Komponente – siehe auch Artikel ab Seite 8 und Interview Prof. Dr. Schneider ab Seite 14.

Kein Sicherheits-Patch: Der Mensch mit seinen Emotionen bleibt die Schwachstelle

Der Faktor Mensch bleibt also die Schwachstelle – und mit jedem weiteren Fortschritt bei der Technologie entsteht hier eine noch größere Sicherheitslücke. Es gibt nicht einfach ein Sicherheits-Patch, das man den Menschen aufspielen kann.

Offenheit bleibt der wichtigste Hebel gegen kriminelle Machenschaften

Kontrollen und Compliance-Systeme spielen bei „Social Engineering“-Fällen eine eher untergeordnete Rolle – ganz anders als bei den klassischen Innentätern. Trotzdem gibt es Mittel und Wege, mit denen man „Social Engineers“ ganz leicht das Handwerk legen kann: Offenheit, eine gute Kommunikation und Fehlerkultur sowie flache Hierarchien. Ein Anruf beim echten Chef oder bei der echten Chefin genügt, und der Betrug fliegt sofort auf.

Ein kritisches Hinterfragen von Mitarbeitenden auch bei eiligen Zahlungsanweisungen ist essenziell, das Handeln „auf Autopilot“ hingegen gefährlich. Doch auch Führungskräfte selbst haben wichtige Aufgaben bei der Prävention: Das reicht von einem vernünftigen „Tone from the Top“ und Führungsqualitäten bis zur klar kommunizierten Selbstverpflichtung, keine Überweisungsaufträge per Telefon oder Video-Calls zu erteilen – und sich vor allem daran zu halten.

> Trotz regelmäßiger Sensibilisierung – der Mensch mit seinen Emotionen bleibt die Schwachstelle.

Rüdiger Kirsch, Betrugsexperte Allianz Trade und Autor dieses Beitrags

So fliegen Täter auf

Vertrauen ist gut – Kontrolle ist besser: Durch interne Kontrollsysteme fliegen Täter am häufigsten auf, gefolgt von „Whistleblowing". Deshalb spielen diese beiden Komponenten bei der Prävention die Hauptrolle. Die meisten Betrugsfälle in Unternehmen werden bei der Revision, bei sonstigen Routineprüfungen oder bei der Überprüfung von Auffälligkeiten aufgedeckt. Aber auch Hinweise von anderen Mitarbeitenden führen oft zur Überführung der internen Täter. Gerade deswegen gewinnt **das Hinweisgeberschutzgesetz** immer mehr Bedeutung: Unternehmen müssen entsprechende interne Kanäle einrichten, die jene schützen, die Auffälligkeiten melden. Zufallsfunde gibt es ebenfalls, und in ganz seltenen Fällen plagt die Betrüger im Nachgang ein schlechtes Gewissen, so dass sie sich selbst anzeigen.

1. Kontrollsysteme

- **Routineprüfung/ Revision**
- **Prüfung von Auffälligkeiten**

2. „Whistleblowing"

- **Hinweise von anderen Mitarbeitenden**
- **Hinweise durch Unternehmensexterne**

3. Zufall

4. Selbstanzeige aus schlechtem Gewissen

Quelle:
Allianz Trade Schadensstatistik

Hinweisgeberschutzgesetz: Was ist das und was bedeutet es für Unternehmen?

Das Hinweisgeberschutzgesetz (HinSchG) ist die deutsche Umsetzung der EU-Whistleblower-Richtlinie. Das Gesetz, das im Juli 2023 in Kraft getreten ist, soll Hinweisgeber vor allen denkbaren Benachteiligungen schützen. Für einen Großteil der Unternehmen, Behörden und Gemeinden bedeutet das: Sie sind verpflichtet, ein internes Hinweisgebersystem zu implementieren. Hinweise von Mitarbeitern werden so durch die sich daraus entwickelnde Gesetzgebung und Rechtsprechung gefördert.

Laut einer Studie der heutigen Fachhochschule Graubünden (FHGR/früher HTW Chur) verfügten 2019 lediglich 55 % der befragten Unternehmen über eingerichtete Meldestellen. Mit der gesetzlichen Verpflichtung und den in der Folge neu eingerichteten Hinweisgebersystemen dürften deshalb insgesamt deutlich mehr Auffälligkeiten gemeldet und Verfehlungen von internen Tätern aufgedeckt werden.

Rechtsanwalt Prof. Dr. jur. Hendrik Schneider
ist Rechtswissenschaftler und Kriminologe. In seiner Forschung hat er sich eingehend mit unterschiedlichen Täterprofilen sowie deren Beweggründen beschäftigt.

INTERVIEW

„Das erste Mal ist oft ein Schrittmacher in die Kriminalität."

Welche verschiedenen Tätertypen gibt es, wie unterscheiden sich diese und warum werden sie eigentlich zu Tätern? Prof. Dr. Hendrik Schneider berichtet über die Unterschiede und Beweggründe von Wirtschaftskriminellen – und was Unternehmen tun können, um sich vor Wirtschaftskriminellen zu schützen; heute, vor allem aber auch in der Zukunft.

Die „typischen Täter", die die größten Schäden anrichten, sind nach der Allianz Trade Schadensstatistik hochgebildete Männer, etwa Mitte 40, Führungskraft und seit mindestens 10 Jahren im Unternehmen; Kolleg:innen beschreiben sie bis dato als auffällig unauffällig. Warum?

Wirtschaftsstraftäter sind „Latecomer to crime", also Spätzünder bei der kriminellen Karriere. Das hat mehrere Gründe. Ein Uni-Absolvent hätte zum Beispiel gar nicht die Befugnisse, Transaktionen mit hohen Geldbeträgen anzuweisen. Ein Manager mit langer Betriebszugehörigkeit weiß hingegen, wie der Hase läuft, wo Nischen und Kontrolldefizite sind und hat die notwendigen Befugnisse. Da ist bei dem einen oder anderen die Verlockung groß, eine günstige Gelegenheit auszunutzen. Man sieht dies beispielsweise an dem extremen Anstieg der Verfahren wegen Subventionsbetruges in der Corona-Krise im Jahr 2020 um sagenhafte 2285 % mit einem Schaden von rund 95 Mio. EUR. In eine entsprechende Position, z. B. Wirtschaftssubventionen überhaupt beantragen zu können, kommt aber niemand, dessen polizeiliches Führungszeugnis Eintragungen aufweist. Das heißt: Eine weiße Weste ist für die Weiße-Kragen-Täter die Grundvoraussetzung.

Warum sind es eigentlich vor allem Männer?

Das ist schwer zu sagen – einer der Gründe ist sicherlich, dass noch immer mehr Männer in entsprechenden Führungspositionen tätig sind.

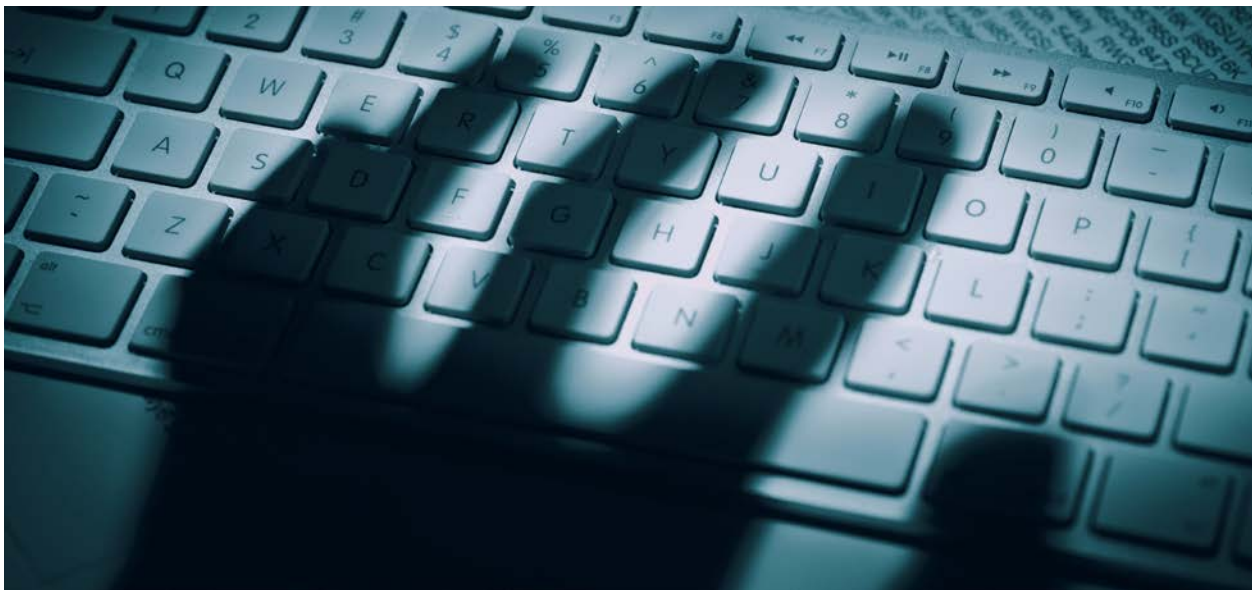
Wenn wir von „typischen Tätern" sprechen, sagen Alter, Position und Betriebszugehörigkeit nur wenig über die Täterpersönlichkeit aus. Gibt es da charakteristische Züge?

Zum einen unterscheiden wir zwischen Gelegenheitssuchern und Gelegenheitsergreifern. Wie die Bezeichnung schon nahelegt, suchen die einen proaktiv nach Schwachstellen, und die anderen reagieren auf eine Gelegenheit, die sich ergibt. Zudem gibt es personale Risikofaktoren. Wir unterscheiden vier Tätertypen: Der Täter mit einem wirtschaftskriminologischen Belastungssyndrom, der Krisentäter, der Abhängige und der Unauffällige.

Was macht diese aus?

Der Abhängige ist – wie der Name sagt – in der Regel ein Mittäter und Handlanger eines dominanten Haupttäters, von dem er wirtschaftlich oder hierarchisch abhängig ist.

Der Täter mit wirtschaftskriminologischen Belastungssyndrom hingegen lebt ein ungebremstes Leben im Augenblick nach der Devise „earning and burning money" und ist Teil einer „arbeitsplatzbezogenen Subkultur". Vielfach ereignen sich die Taten in einer biografischen Umbruchphase, die mit Kontrolldefiziten und mangelnder Einbindung einhergeht, z. B. der Job im Ausland, Scheidung etc. Er ist ein Gelegenheitssucher, der jede sich bietende Gelegenheit sofort ergreift.



Macht Gelegenheit tatsächlich Diebe?

Manchmal ist das tatsächlich der einzige Auslöser. Beim „Unauffälligen" ist das genau so. Dieser Tätertyp weist tatsächlich keine oder nur sehr geringe personale Risikofaktoren auf. Die Verlockung der günstigen Gelegenheit war einfach zu groß. Kommt die Tat an Licht, überrascht das sein gesamtes Umfeld, weil er zuvor unauffällig und angepasst war und bei einem Risiko-Screening durchs Raster fallen würde.

Nachzahlungen bei Strom- oder Heizkosten, hohe Inflation und steigende Zinsen stellen viele Menschen aktuell vor große Probleme. Müssen sich Unternehmen jetzt vor Krisentätern fürchten und was macht diese aus?

Wir sprechen insofern von ökonomischen Drucksituationen, die unter den heutigen wirtschaftlichen Bedingungen verstärkt auftreten. Die Straftat kann aus Sicht des Täters den einzigen Ausweg aus der finanziellen Krise darstellen. Weil die Tat mit seinem Selbstbild, im Konflikt steht, helfen ihm Neutralisierungstechniken, um die inneren Wogen zu glätten, z. B. „ich borge mir das Geld nur"; „den Schaden gleicht ja ohnehin die Versicherung aus".

Aber es werden ja nicht alle kriminell?

Nein. Krisentäter stehen massiv unter Druck, aber es gibt natürlich Auswege, die keine Straftaten beinhalten – im Extremfall die Beantragung des Insolvenzverfahrens. Aber nicht jeder ist bereit, diese Schritte zu gehen oder den Lebensstandard in der Krise nach unten anzupassen.

Sie haben Neutralisierungsstrategien erwähnt. Wie muss man sich solche Strategien vorstellen?

Wirtschaftskriminelle sind nicht per se unmoralisch. Gerade Krisentäter haben oft hohe Wertvorstellungen und dadurch Schwierigkeiten, kriminelle Taten vor sich selbst zu rechtfertigen. „Es ist ja nur dieses eine Mal", „ich mache nur, was die anderen auch machen", „es trifft keinen anderen persönlich, die können sich das schon leisten" können solche Rechtfertigungen sein.

Wenn Täter noch die Notwendigkeit sehen, etwas zu rationalisieren, ist dies eigentlich ein gutes Zeichen, dann ist noch nicht Hopfen und Malz verloren. Das bedeutet, dass noch eine Werteorientierung da ist und innere Wogen hochschlagen, die Alarm schlagen. Aber es kann eben auch der Anfang vom Ende sein.

Dann werden sie zu Wiederholungstätern?

Das erste Mal ist entweder tatsächlich eine einmalige Sache – oder aber ein Schrittmacher in die Kriminalität. Beim ersten Mal ist die Hemmschwelle oft hoch. Aber es gibt ein Erfolgslernen und einen Gewöhnungseffekt. Je öfter man lügt oder betrügt, desto geringer ist das Unwohlsein. Irgendwann läuten die Alarmglocken nicht mehr und es läuft dann quasi von selbst. Solange die Fassade und die Tarnung intakt sind, merken Täter oft gar nicht, wie kriminell sie sind, weil es sich durch dieses schrittweise Abrutschen gar nicht so kriminell anfühlt – das kommt oft erst beim Gerichtsprozess. Man nennt das ein „Abdriften in die verfestigte Kriminalität", und es können wirtschaftskriminelle Karrieren entstehen.

In arbeitsplatzbezogenen Subkulturen ist das übrigens auch so. In diesen Parallelwelten ist man unter Gleichgesinnten und es fehlt ein objektives Korrektiv. Wenn man abends beim Bier Revue passieren lässt, wie schlitzohrig man heute agiert hat, entstehen ganz neue Werteräume und man ist im Einklang mit seinem Umfeld. Durch die Gruppendynamik brauchen sie keine Neutralisierungstechniken. Es führt allerdings auch dazu,

dass sie noch schneller in den Abgrund gerissen werden. Dann kommt irgendwann das böse Erwachen.

Apropos böses Erwachen: Haben die Täter gar keine Angst, entdeckt zu werden und dann den Job auch noch zu verlieren?

Tatsächlich haben die Täter – entgegen vieler Annahmen – meist sehr viel zu verlieren. Das Entdeckungsrisiko spielt bei ihrer Abwägung, ob sie nun der Verlockung der Tatgelegenheit erliegen, durchaus eine Rolle.

Nur gibt es häufig einen großen Unterschied zwischen dem objektiven und dem subjektiven Entdeckungsrisiko. Risiken in der Zukunft, die weit weg erscheinen, werden oft weniger stark gewichtet.

Wenn ich als Täter weiß, dass die Taten beim nächsten Audit auffliegen könnten, macht es für das subjektive Entdeckungsrisiko einen Unterschied, ob das nächste Audit in drei Wochen oder in drei Jahren stattfindet.

Stichwort Kontrollsysteme – wie können Unternehmen sich schützen?

Gute Kontroll- und Compliance-Systeme und saubere Prozesse sind das A und O, denn sie minimieren die Tatgelegenheiten. Dabei ist es wichtig, hier auch permanent mitzudenken, welche neuen Risiken in Zukunft entstehen könnten, durch die Digitalisierung, zunehmende Cyberangriffe, neue Technologien, künstliche Intelligenz wie beispielsweise Chat GPT. Betrugsmaschen dürften sich ebenso rasant beschleunigen wie der technologische Fortschritt. Wenn ein falscher Chef auf Knopfdruck eine E-Mail im „CEO Style" ausspucken kann, schnellen Professionalität und Skalierbarkeit in neue Sphären.

Das ist tatsächlich auch ein Generationen-Thema. Deshalb ist es wichtig, auch junge, technologieaffine Mitarbeitende im Boot zu haben, die sich der damit verbundenen Risiken bewusst sind. Das gilt im Übrigen sowohl für Compliance als auch für Aufsichtsräte.

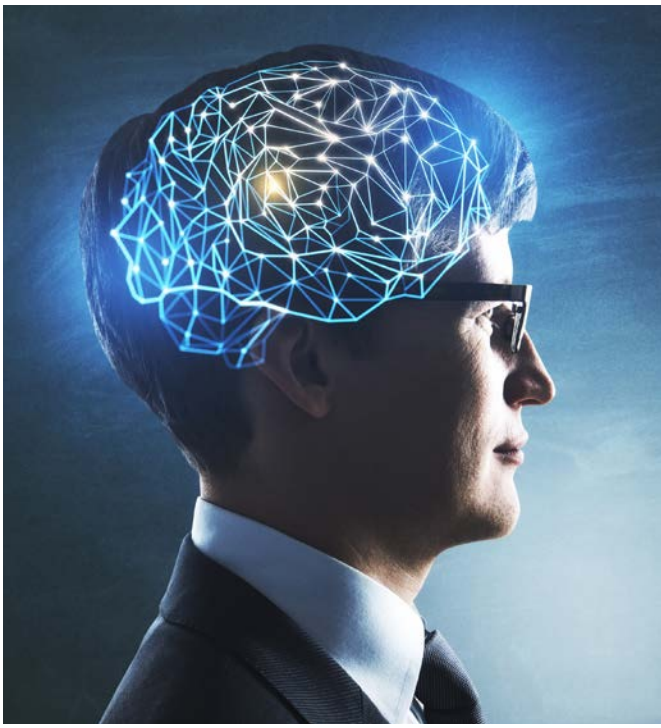
Man kann auch einfach einen Selbsttest machen und es ausprobieren. Schicken sie doch mal eine Chat GPT Mail in die eigene Organisation. Damit identifizieren sie gnadenlos die eigenen Schwachstellen bei Prozessen und Kontrollmechanismen. Sie können dann nachjustieren, bevor es zu finanziellen Schäden kommt.

Zur Prävention sind Sensibilisierungs- und Trainingsmaßnahmen sehr effektiv. Und seit Juli 2023 müssen bestimmte Unternehmen mit dem Hinweisgeberschutzgesetz zudem anonymisierte Meldekanäle für Unregelmäßigkeiten implementieren.

Welche Rolle spielt die Unternehmenskultur?

Die Unternehmens- und Fehlerkultur sowie der „Tone from the Top" spielen eine wichtige Rolle. Autokratische oder sehr hierarchische Kulturen begünstigen ein „Ausbrechen" und sind häufig wesentlich anfälliger für Wirtschaftskriminalität. Wie so oft: Die Balance macht es.

In einigen Unternehmen können komplementäre Doppelspitzen gut funktionieren, und tatsächlich sind diverse Teams hilfreich für sowohl die Unternehmenskultur als auch den Unternehmenserfolg. Wenn unterschiedliche Blickwinkel, Perspektiven und Werteorientierungen aufeinandertreffen, werden Dinge ganz anders hinterfragt und überlegt. Das führt oft zu einem wesentlich differenzierteren Vorgehen und hilft bei wichtigen Entscheidungen und bei der Kultur.



So unterscheiden sich die vier Tätertypen

DER TÄTER MIT WIRTSCHAFTSKRIMINOLOGISCHEM BELASTUNGSSYNDROM

Das Bedürfnis nach „hemmungsloser Geldverbrennung" war nach dem Votum des zuständigen Strafrichters die Triebfeder für einen Fall aus dem Bereich des Top-Management-Fraud mit einem Gesamtschaden im zweistelligen Millionenbereich. Sich einen Lebensstil nach dem Muster des „earning and burning money" mit einem ungebremsten Leben im Augenblick leisten zu können, ist vielfach die Triebfeder der Täter mit wirtschaftskriminologischem Belastungssyndrom.

Im Beispielsfall leistete sich der Täter unter anderem eine Yacht, maßgefertigte Möbel aus Tropenholz und konsumierte nur besonders erlesene Weine. Die Aufklärung des Falles zeigt eindrucksvoll auf, dass fehlende Kontrollen, mangelnde Vier-Augen-Prinzipien, defizitäre Compliance-Systeme und ein Überschuss an Kontrolle des Täters über Vorgänge und Untergebene einen Nährboden darstellen, der eine langfristige Viktimisierung des Unternehmens mit erheblichen Vermögensschäden hervorrufen. Treffen diese situativen Bedingungen auf einen Täter mit, wie der Richter im Beispielsfall ausführte, „erheblicher krimineller Energie", können erhebliche Vermögensschäden entstehen bis hin zur Insolvenzreife eines mittelständischen Unternehmens.

Auch nach dem Bekanntwerden der Untreuetaten hatte der Täter, der sich als regelmäßiger Kirchgänger und Mitglied einer „streng christlichen traditionalistischen Brüderbewegung" einen entsprechenden Tarnmantel zugelegt hatte, alles getan, um die betrügerisch erlangten Geldmittel zu behalten. So hat er zum Beispiel durch Schenkungen an Dritte versucht, Schadensersatzforderungen seines früheren Arbeitgebers zu vereiteln.

DER UNAUFFÄLLIGE

In einer quantitativ bedeutsamen Anzahl von Konstellationen können keine personalen Risikofaktoren identifiziert werden, sondern die Tat erklärt sich allein aus dem Vorliegen der günstigen Gelegenheit. Lange Unternehmenszugehörigkeit und defizitäre Kontrollen sind kennzeichnend für entsprechende situative Bedingungen. Es kann sich ein Lerneffekt des erfolgreichen Täters einstellen.

In einem der analysierten Beispielsfälle von Allianz Trade war der Täter seit 1991 Alleingeschäftsführer eines Großhandelsunternehmens. Nach 20 Jahren Unternehmenszugehörigkeit in einer unangefochtenen Führungsposition entschloss er sich, Untreuedelikte zum Nachteil des Arbeitgebers zu begehen. Die Taten wurden über einen Zeitraum von drei Jahren begangen, bis sie aufflogen und aufgrund identifizierter Unregelmäßigkeiten eine Wirtschaftsprüfer-Gesellschaft mit der Durchführung eines internen Audits beauftragt wurde. Bei den Taten handelte es sich um Untreuedelikte. Es ging dem Täter darum, private Luxusreisen, die zum Teil mit befreundeten Paaren durchgeführt wurden sowie Geburtstagsfeiern im Ausland auf Firmenkosten durchzuführen.

Der nicht wirtschaftlich unter Druck stehende Täter hätte die Reisen auch privat finanzieren können. Möglicherweise dienen die im Prozess von ihm geltenden Argumente, es habe sich um eine „Kontaktpflege" zu künftigen oder aktuellen Geschäftspartnern und Kollegen gehandelt, auch zur Rechtfertigung in Gestalt von Neutralisierungsstrategien, um die hochschlagenden inneren Wogen zu glätten.

DER KRISENTÄTER

Krisen können wirtschaftliche Krisen oder allgemeine Lebenskrisen sein. In einem Beispielsfall mit Verurteilung des Täters im Jahr 2023 stand der Täter, ein kaufmännischer Angestellter, unter wirtschaftlichem Druck, weil er einer Online-Spielsucht verfallen war.

Als die Möglichkeit, Geldmittel für die Online-Glücksspiele durch legale Mittel, wie beispielsweise Kredite zu erlangen, ausgeschöpft war, nutzte er Tatgelegenheiten, um Straftaten zum Nachteil des Arbeitgebers zu begehen. Über einen Zeitraum von zwei Jahren erstellte er falsche Rechnungen für nichterbrachte Werkleistungen. Hierdurch veranlasste er seinen Arbeitgeber, der von der Erbringung der Werkleistungen durch die in der Rechnung ausgewiesene Firma ausging, insgesamt rund 500.000 EUR auf ein Konto zu überweisen, das alleine dem Zugriff des Täters unterlag. Bei den Taten handelte es sich um Urkundenfälschung und gewerbsmäßigen Betrug.

DER ABHÄNGIGE

Sind an den Taten mehrere beteiligt, bilden sich die beruflichen Hierarchien in aller Regel auch bei der Tatbegehung und der Beuteverteilung ab.

In einem Beispielsfall aus dem Jahr 2019 war der Täter in leitender Position bei einem Unternehmen beschäftigt, das bestimmte Produkte aus Stahl im Auftrag verschiedener Kunden entweder instand setzte oder verschrottete. Dem Täter gelang es durch bestimmte Manipulationen, Stahl abzuzweigen und in Containern zwischenzulagern. Dieses Material wurde gegen Barzahlung weiterverkauft. Der männliche Haupttäter erhielt hierbei Unterstützung von einer Niederlassungsleiterin, die im Rahmen polizeilicher Ermittlungen schließlich ein Geständnis ablegte. Die Niederlassungsleiterin war insbesondere für die Vereinnahmung des Bargelds zuständig und erhielt hierbei einen Anteil von 10 %. Die Differenz musste sie an den Haupttäter auszahlen, der das Geld im Wesentlichen für den Erwerb von Fahrzeugen der Luxusklasse und eine „Stadtvilla mit zwei Garagen und Nebenräumen" verwendete.

Wie können sich Unternehmen vor schwarzen Schafen schützen?

Betrug und Untreue sind weiterhin in den Top 3 der Delikte im Bereich Wirtschaftskriminalität. 36 % der betroffenen Unternehmen in Deutschland verzeichneten 2022 Schäden durch Betrug. Nur Datendiebstahl und Datenmissbrauch (38 %) sowie Diebstahl und Unterschlagung (39 %) kamen noch häufiger vor*. Es gibt mehr schwarze Schafe, als viele Unternehmen glauben, und sie richten jedes Jahr große finanzielle Schäden an.

Sie zu identifizieren ist allerdings in vielen Fällen schwer. Denn oft sind sie auffällig unauffällig, freundlich, gut angepasst und integriert. Viele durchaus gewünschte Eigenschaften von Leistungsträgern decken sich zudem mit denen von Betrügern – wie beispielsweise Durchsetzungswillen, Risikobereitschaft, Ehrgeiz oder Aufstiegsorientierung.

Für die Unternehmen ist es deshalb wichtig, dass sie eine Balance zwischen Vertrauen und Unternehmenskultur auf der einen Seite und Vorsorge und Kontrolle auf der anderen Seite finden.

Zufriedene Mitarbeitende, die sich wohl fühlen, denen Kollegen und Vorgesetzte mit Respekt und Wertschätzung begegnen und die mit Aufgaben und Bezahlung sowie Aufstiegs- und Weiterbildungsmöglichkeiten zufrieden sind, identifizieren sich mit dem Unternehmen und sind in der Regel wesentlich loyaler als Mitarbeitende, die kein gutes Betriebsklima vorfinden. Mobbing, Frustration und Rache sind häufige Motive, die interne Täter antreiben.

Die Unternehmens- und Fehlerkultur sowie die offene und transparente Kommunikation spielen also eine entscheidende Rolle. Wenn Mitarbeitende sich trauen, Missstände anzusprechen, können Schwachstellen identifiziert, Sicherheitslücken geschlossen und Täter schneller identifiziert werden.

Kontrollmechanismen, Richtlinien sowie regelmäßige Routine-Überprüfungen sind für Unternehmen allerdings genauso wichtig, um sich zu schützen – denn Gelegenheit macht Diebe.

Dennoch: Der Faktor Mensch ist flexibel und die schwarzen Schafe finden immer Mittel und Wege. Viele Innentäter haben ein hohes Maß an krimineller Energie, sie nutzen Gelegenheiten umgehend und können auch die besten Kontrollsysteme aushebeln. Deshalb sollten sich Unternehmen nicht auf ihren Kontrollsystemen ausruhen oder in falscher Sicherheit wiegen.

**Quelle:*
KPMG Studie Wirtschaftskriminalität in Deutschland 2023

Vertrauen & Kultur

Offene, vertrauensvolle **Unternehmenskultur** mit möglichst flachen Hierarchien

Gute, konstruktive **Fehlerkultur** und offene Kommunikation

Klare Formulierung von **Unternehmensrichtlinien und ethischen Werten** sowie Integration in den Unternehmensalltag

Kollegialer, demokratischer **Führungsstil**, Wertschätzung, Vertrauen und Respekt

Gute **Arbeitsbedingungen:** Faire Bezahlung, finanzielle Anreize, Leistungsvergütung, interessante Aufgaben

Gleichberechtigung, Diversität, faire Aufstiegschancen nach klar festgelegten, objektiven und für alle nachvollziehbaren Kriterien

Talententwicklung und -förderung; Weiterbildung von Hard und Soft Skills; Nachwuchsförderung

Zufriedenheitsbefragungen von Mitarbeitenden; Implementierung von Maßnahmen zur Steigerung der Zufriedenheit

Unterstützung von Beschäftigten in (persönlichen oder finanziellen) Notlagen durch entsprechende Hilfs- oder Beratungsangebote

Vorsorge & Kontrolle

Implementierung von **Kontroll- und Compliance-Systemen;** insbesondere Vier- oder Mehr-Augen-Prinzip

Sensibilisierung und Schulung der Mitarbeitenden für **interne Richtlinien** sowie kritische Situationen und **Detektion von Auffälligkeiten**

Regelmäßige **Routine-Kontrollen**, Audits, Revisionen, ggf. Prüfung durch externe Dritte

Implementierung von geschützten internen (und ggf. externen) **Whistleblowing-Kanälen** (z. B. Ombudsleute) und regelmäßige Information der Mitarbeitenden

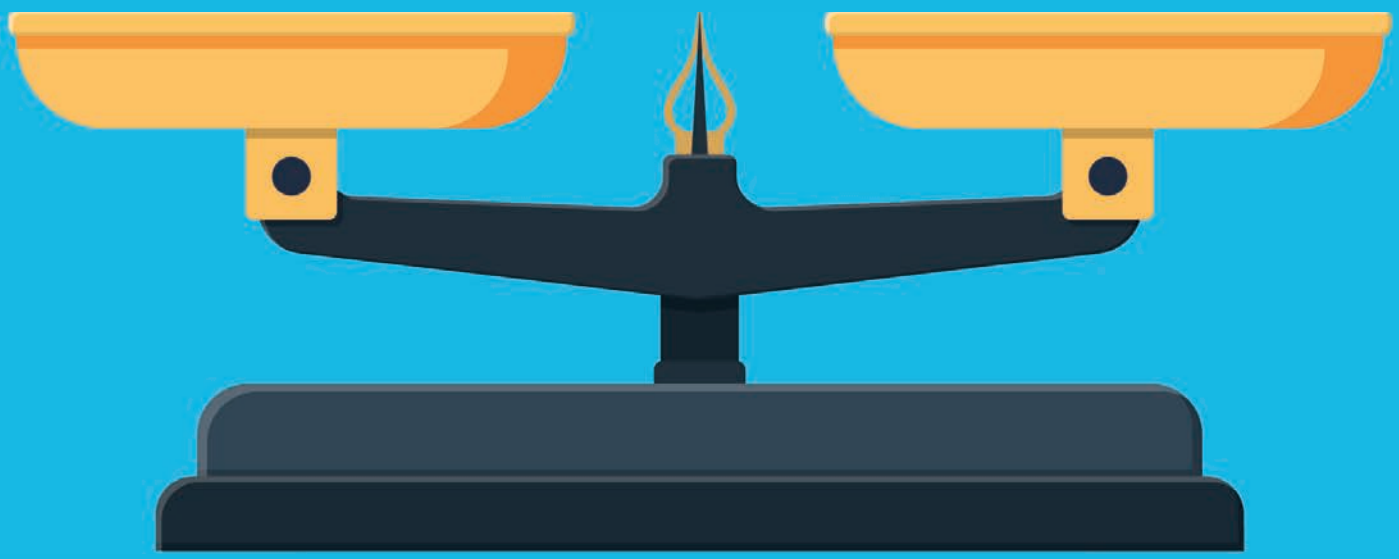
Präventives Risikomanagement und regelmäßige Prozessoptimierung: Überprüfung und Verbesserung von eventuellen Systemschwachstellen inkl. Zugangs- und Zugriffskontrollen

Wachsamkeit und **Beobachten von Auffälligkeiten,** z. B. Anomalien in den Arbeitsstunden, Versuche, auf begrenzt zugängliche Daten zuzugreifen oder der Gebrauch von unautorisierten Datenträgern

Umgehende, transparente und objektive **Untersuchung bei Verdachtsmomenten**

Überprüfung von Bewerbern, z. B. Abgleich mit Sanktionslisten, Führungszeugnis, Schufa, Plausibilitäts- bzw. Background-Check, Referenzen

Für besonders sicherheitsrelevante Positionen ggf. **Bestimmung von Personenfaktoren,** z. B. Hannoversche Korruptionsskala



Sicherheitslücken schließen

Trotz aller Vorsichtsmaßnahmen lassen sich Betrug und Veruntreuung nicht immer vermeiden. Bei Eintritt eines Schadens ist es für Unternehmen wichtig, schnell und richtig zu handeln und die Sicherheitslücken konsequent zu schließen. Zudem sollten Unternehmen **die häufigsten Risikofaktoren** am besten regelmäßig überprüfen.

1. Risikofaktor Unternehmensstruktur

- **a.** Sind die Arbeitsabläufe und -prozesse im Haus klar definiert?
- **b.** Gibt es im Hause Verantwortliche, die sich über notwendige und mögliche Sicherheitsvorkehrungen auf dem Laufenden halten?
- **c.** Gibt es Katastrophenpläne im Unternehmen?

2. Risikofaktor Personalbeschaffung

- **a.** Wird bei Bewerbern mit ungewöhnlichen Kündigungsterminen oder häufigem Stellenwechsel die Ursache ergründet?
- **b.** Werden bei Bewerbern für Schlüsselpositionen weitergehende Prüfungen (Referenzen) vorgenommen?
- **c.** Sind sämtliche Mitarbeitende schriftlich zur Geheimhaltung der Firmeninterna verpflichtet?
- **d.** Hat das Management ein Krisenszenario für Vertrauensschadenfälle?

3. Risikofaktor EDV

- **a.** Gibt es für das IT-System ein Sicherheitskonzept?
- **b.** Werden sämtliche Daten nach ihrer Schutzwürdigkeit klassifiziert und entsprechende Schutzmaßnahmen getroffen?
- **c.** Ist die IT gegen Angriffe von außen geschützt?
- **d.** Ist ein periodischer Passwortwechsel vorgesehen?
- **e.** Gibt es im Unternehmen ungesicherte Internetanschlüsse?
- **f.** Sind Online-Verbindungen zur Hausbank ausreichend geschützt?

4. Risikofaktor Zahlungsverkehr

- **a.** Sind Buchhaltung und Kasse streng getrennt?
- **b.** Werden Scheckvordrucke unter Verschluss gehalten, und werden Nummernkreise kontrolliert?
- **c.** Gibt es im Unternehmen Unterschriftenfaksimiles?
- **d.** Sind dabei vorgelagerte Kontrollen vorgesehen?

5. Risikofaktor Post

- **a.** Wird die eingehende Post mit einem Eingangsstempel versehen?
- **b.** Werden eingehende Schecks in einem Eingangsbuch notiert?

6. Risikofaktor Einkauf/Verkauf

- **a.** Sind verschiedene Personen jeweils verantwortlich für
  - die Auftragserteilung,
  - die Registrierung eingehender Waren,
  - die Genehmigung der Bezahlung von Waren?
- **b.** Werden regelmäßige Inventuren des Warenbestandes durchgeführt?
- **c.** Werden Retouren gesondert erfasst?
- **d.** Hat das Unternehmen einen Verhaltenskodex für Einkäufer?

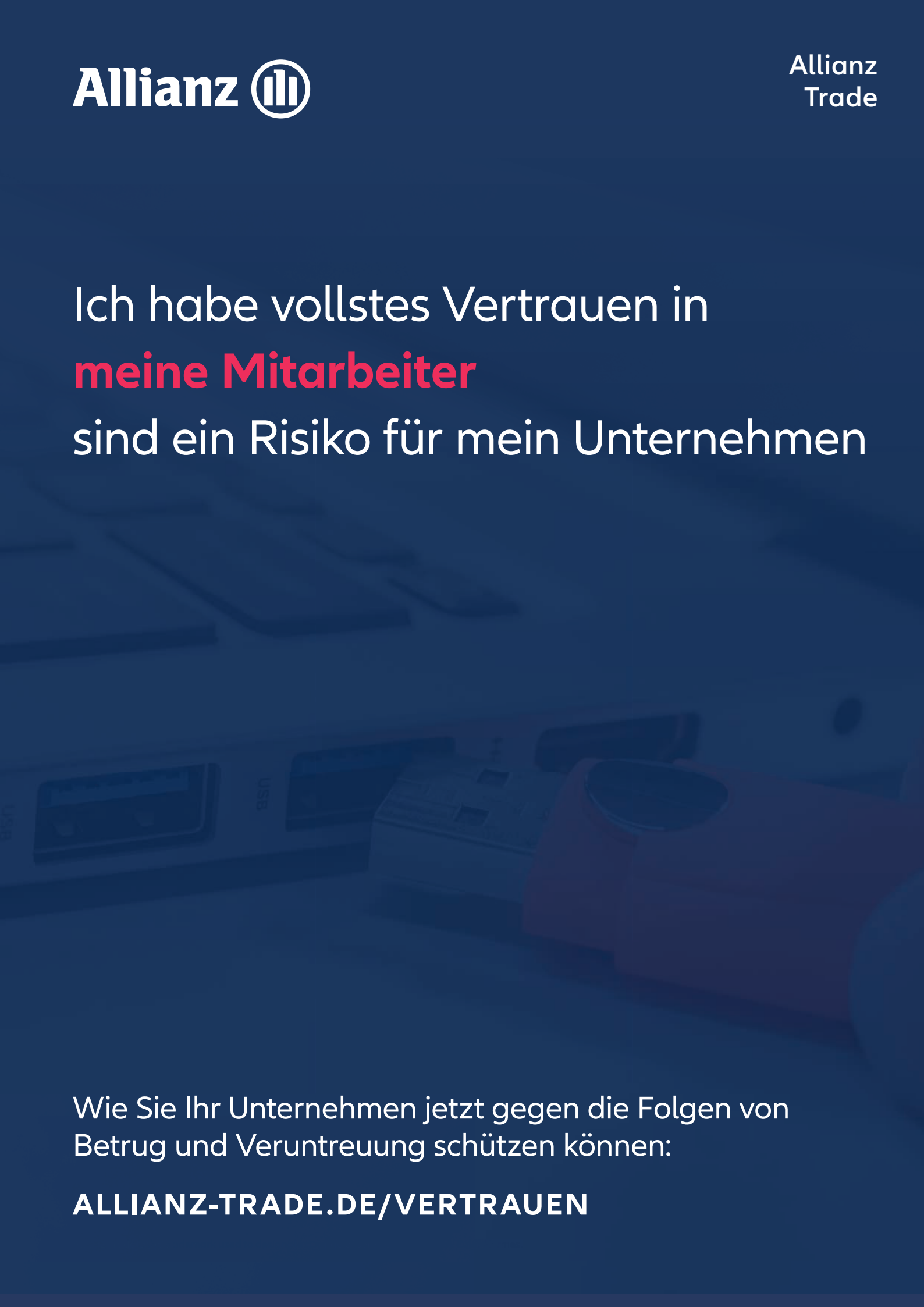
7. Risikofaktor Revision/Kontrollen

- **a.** Gibt es eine eigene Revisionsabteilung?
- **b.** Prüft diese bzw. ein Wirtschaftsprüfer regelmäßig alle Bereiche des Unternehmens?
- **c.** Ist das 4-Augen-Prinzip durchgehend im Unternehmen implementiert? Und wie wird es ggf. im Homeoffice umgesetzt?

Allianz

Allianz
Trade

Ich habe vollstes Vertrauen in **meine Mitarbeiter** sind ein Risiko für mein Unternehmen



Wie Sie Ihr Unternehmen jetzt gegen die Folgen von Betrug und Veruntreuung schützen können:

ALLIANZ-TRADE.DE/VERTRAUEN

Gut gerüstet gegen Risiken

Sichern Sie Ihr Unternehmen ab gegen Vermögensschäden durch vorsätzlich unerlaubte Handlungen von sogenannten „Vertrauenspersonen" und externen Dritten. Wir haben die richtige Lösung für Ihren Bedarf:

Schutz vor Veruntreuung PremiumPlus

Für größere Unternehmen: Weitreichende Absicherung gegen Schäden durch eigene Mitarbeitende, zielgerichtete Hackerschäden sowie Schäden durch bestimmte Straftaten Dritter.

Schutz vor Veruntreuung VSV Smart

Für kleinere Unternehmen: Weitreichende Absicherung gegen Schäden durch eigene Mitarbeitende, zielgerichtete Hackerschäden sowie Schäden durch bestimmte Straftaten Dritter.

Schutz vor Bestellerbetrug

Schutz vor Schäden durch Dritte, die an Ihre Daten gelangen und diese für betrügerische Bestellungen nutzen.

Stellen Sie Ihr Unternehmen jetzt zukunftssicher auf!
Wir unterstützen und informieren Sie gern:

Tel. + 49 (0) 40 / 88 34 - 35 36
service.de@allianz-trade.com
www.allianz-trade.de/vertrauen

Euler Hermes Deutschland
Niederlassung der Euler Hermes SA
22746 Hamburg
Tel. +49 (0) 40 / 88 34 - 0
Fax +49 (0) 40 / 88 34 - 77 44
info.de@allianz-trade.com
www.allianz-trade.de