PwCs globale Umfrage zur Wirtschaftskriminalität

Zunehmende Bedrohung durch externe Tätergruppen

pwc

www.pwc.de/gecs

Durch den zunehmenden geopolitischen, finanziellen, ökologischen und gesellschaftlichen Druck stehen Unternehmen vor einer Risikolandschaft, die unvorhersehbarer ist als je zuvor. Gleichzeitig erschweren es ihnen die damit einhergehenden Veränderungen, sich präventiv gegen Wirtschaftskriminalität zu wappnen. Denn während die Unternehmen noch damit beschäftigt sind, schnell auf die Veränderungen zu reagieren, finden Kriminelle immer intelligentere Wege, die Mechanismen zur Betrugsabwehr zu umgehen.

Die Aufsichtsbehörden haben die Herausforderungen der komplexen Risikolandschaft bereits erkannt und bauen daher zusätzliche personelle und technische Kapazitäten auf. Neben den typischen Ermittlungsverfahren bei Wirtschaftskriminalität verstärken sie auch Überprüfungen der Arbeitsplatzkultur, der Lieferkettensorgfaltspflicht und der Nachhaltigkeitsberichterstattung.

Wie aber reagieren die Unternehmen? Gibt es ausreichend Kontrollen für die Vielzahl an neu eingeführten digitalen Technologien? Verfügen Unternehmen über ein Risikomanagement, das den Anforderungen einer zunehmend hybriden Arbeitswelt entspricht? Haben sie zum Ende der Pandemie in einer unsicheren Wirtschaftslage für angemessene Richtlinien und Anreize gesorgt? Mit welchen Betrugsrisiken und -szenarien haben es Unternehmen heute genau zu tun? Um Antworten auf diese und weitere Fragen zu finden, hat PwC dieses Jahr erneut Unternehmensvertreter:innen weltweit zur aktuellen Situation der Wirtschaftskriminalität befragt.

Jahrelange Bemühungen der Unternehmen, wirtschaftskriminelle Aktivitäten durch Richtlinien, Schulungen, interne Kontrollen und Überwachung zu bekämpfen, haben dazu beigetragen, die interne Wirtschaftskriminalität – selbst in einer volatilen Risikolandschaft – einzudämmen. Schon seit einiger Zeit entstehen jedoch neue, schwerwiegende Bedrohungsszenarien. Die diesjährige Umfrage zeigt, dass insbesondere die Schutzmaßnahmen der Unternehmen gegen externe Bedrohungen angreifbar sind und externe Tätergruppen aktuell eine größere Gefahr darstellen.

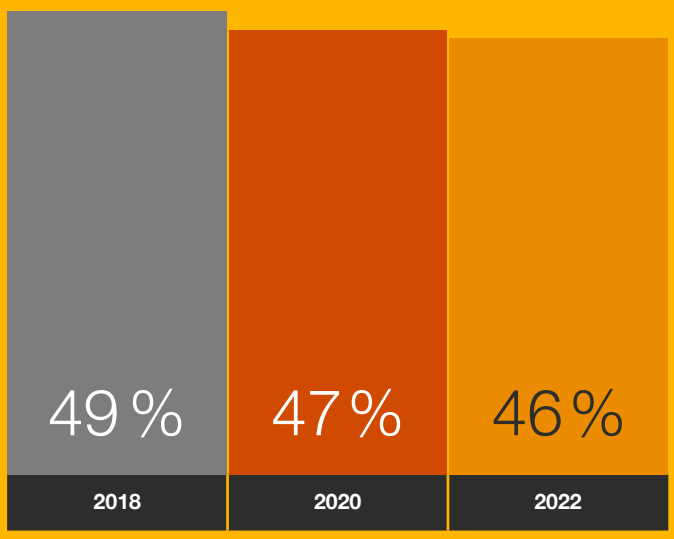
1

Maßnahmen zur Prävention von Wirtschaftskriminalität zeigen Wirkung

Es gibt aber auch gute Nachrichten. Trotz der instabilen geo- und umweltpolitischen Lage, der Lieferkettenprobleme, einer unsicheren wirtschaftlichen Entwicklung, des Fachkräftemangels und vieler neuer Risiken ist der Anteil an Unternehmen, die von wirtschaftskriminellen Handlungen betroffen sind, seit 2018 insgesamt nicht gestiegen. Nur knapp die Hälfte der weltweit befragten Unternehmen (46%) gab an, in den vergangenen 24 Monaten mit einer Form von Wirtschaftskriminalität konfrontiert gewesen zu sein. In Deutschland waren sogar lediglich 40% (2020: 48%) betroffen.

Eine Ausnahme bildet hier die Technologie-Branche, die mit einem deutlichen Anstieg wirtschaftskrimineller Aktivitäten seit 2020 in das Gesamtergebnis einfließt. Fast zwei Drittel der Unternehmen aus den Bereichen Technologie, Medien und Telekommunikation waren von Wirtschaftskriminalität betroffen. Dies entspricht der höchsten Quote aller Branchen.

Konstanter Anteil an Unternehmen, die von Wirtschaftskriminalität betroffen sind



Basis: Alle Befragten (1.296), 2020 (5.018), 2018 (7.228)

Die Wirtschaftskriminalitätsraten sind über die vergangenen vier Jahre zwar insgesamt stabil geblieben, aber die Auswirkungen sind erheblich. 52 % der Unternehmen mit einem weltweiten Jahresumsatz von mehr als 10 Mrd. US-Dollar sind in den vergangenen 24 Monaten Opfer von Wirtschaftskriminalität geworden. Innerhalb dieser Gruppe berichtete fast jedes Fünfte, dass der jeweils schwerwiegendste Vorfall einen finanziellen Schaden von mehr als 50 Mio. US-Dollar nach sich zog. Bei kleineren Unternehmen (mit einem Umsatz von weniger als 100 Mio. US-Dollar) war der Anteil geringer: 38 % hatten mit Fällen von Wirtschaftskriminalität zu kämpfen, von denen jedes Vierte einen Gesamtschaden von mehr als 1 Mio. US-Dollar verursachte.

Wo liegen die größten Risiken? Für die Unternehmen weltweit stellt die Cyberkriminalität die größte Bedrohung dar (37 %), gefolgt von Betrug durch Kunden (33 %) und Vermögensdelikte (25 %).

46 %

der befragten Organisationen berichteten, dass sie in den vergangenen 24 Monaten von Wirtschaftskriminalität betroffen waren

Kriminalitätsraten und finanzielle Auswirkungen bei großen und kleinen Unternehmen

Unternehmen mit einem Umsatz von >10 Mrd. US-Dollar

52 %

waren in den vergangenen 24 Monaten von Wirtschaftskriminalität betroffen

18 %

berichten, dass die schwerwiegendste Wirtschaftsstraftat eine finanzielle Auswirkung von mehr als 50 Mio. US-Dollar hatte

Unternehmen mit einem Umsatz von <100 Mio. US-Dollar

38 %

waren in den vergangenen 24 Monaten von Wirtschaftskriminalität betroffen

22 %

berichten, dass die schwerwiegendste Wirtschaftsstraftat eine finanzielle Auswirkung von mehr als 1 Mio. US-Dollar hatte

Quelle: PwC's Global Economic Crime and Fraud Survey 2022

Die Unternehmen arbeiten hart an besserer Technologie und strengeren internen Kontrollen.

Arten von Wirtschaftskriminalität, aufgeschlüsselt nach Unternehmen mit weltweiten Umsätzen

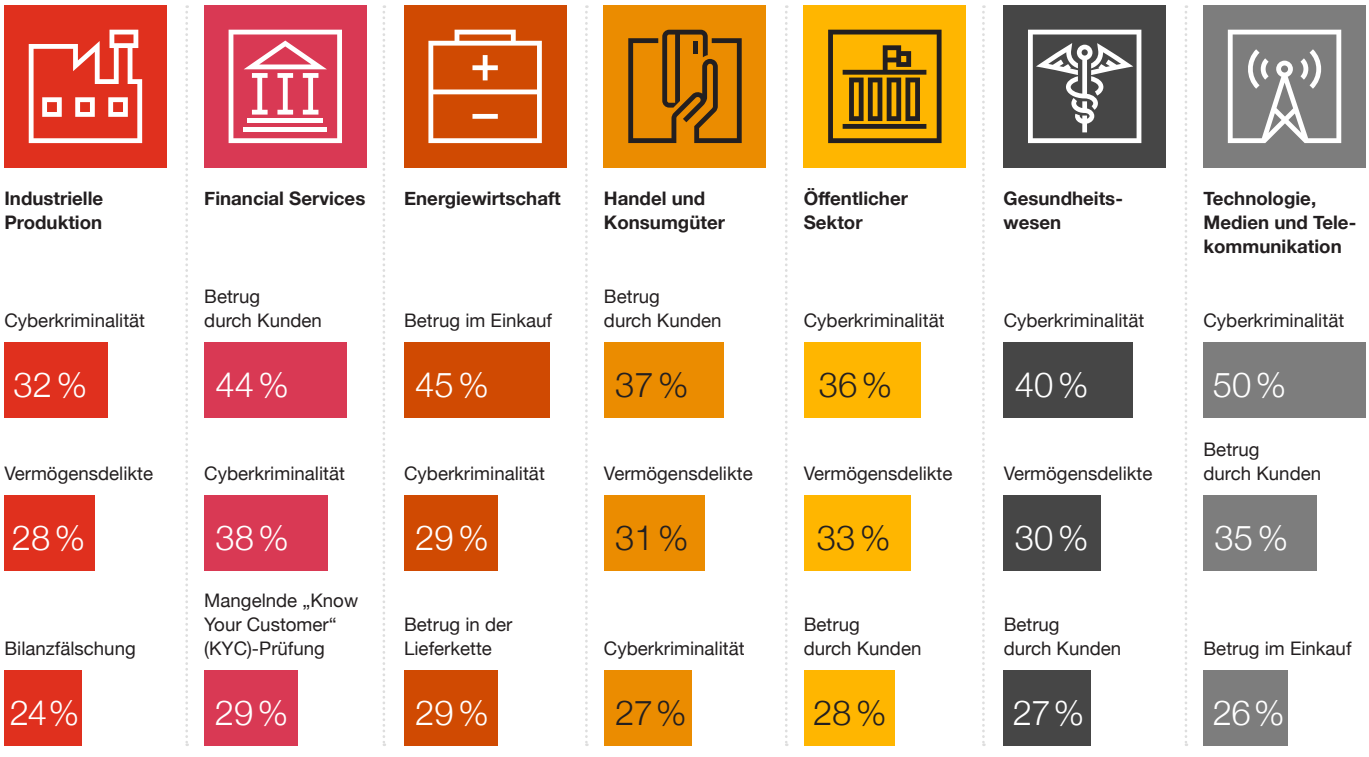
	Weniger als 100 Mio. US-Dollar	100 Mio. bis weniger als 1 Mrd. US-Dollar	1 Mrd. bis weniger als 10 Mrd. US-Dollar	Mehr als 10 Mrd. US-Dollar
1	Cyberkriminalität 32 %	Cyberkriminalität 41 %	Cyberkriminalität 42 %	Betrug durch Kunden 35 %
2	Betrug durch Kunden 27 %	Betrug durch Kunden 32 %	Betrug durch Kunden 34 %	Cyberkriminalität 32 %
3	Vermögensdelikte 23 %	Vermögensdelikte 23 %	Vermögensdelikte 24 %	Vermögensdelikte 31 %

Quelle: PwC's Global Economic Crime and Fraud Survey 2022

Eine Ausnahme bilden Unternehmen in der Energieindustrie. Hier stellt der Betrug im Einkauf die größte Bedrohung dar. Von den befragten Unternehmen in dieser Branche, die angaben von Wirtschaftskriminalität betroffen gewesen zu sein (31 %), berichtete fast die Hälfte von einem solchen Vorfall. Durch den im Vergleich mit vielen anderen Branchen kleineren digitalen Fußabdruck und die geringere Zahl an Interaktionen mit Kunden ist es nachvollziehbar, dass sich wirtschaftskriminelle Aktivitäten in dieser Branche von den anderen abheben. Dennoch zeigen aktuelle Ereignisse, dass Cyberangriffe, insbesondere auf kritische Infrastrukturen, zunehmend eine größere Gefahr darstellen könnten.

Eine weitere Erkenntnis: Die systematische Umsetzung von Maßnahmen hilft Unternehmen, sich gegen Wirtschaftskriminalität zu schützen. Besonders Richtlinien, Prozesse und Schulungen haben sich als hilfreich erwiesen, um Mitarbeiter:innen Orientierung für regelkonformes Verhalten zu bieten. Die Ergebnisse zeigen außerdem, dass Unternehmen aktuell daran arbeiten, ihre Technologien zu verbessern und stärkere Maßnahmen im Meldewesen und bei internen Kontrollen einführen. So sollen sowohl interne als auch externe Bedrohungen abgewehrt werden. Bei zwei Drittel der von Wirtschaftskriminalität betroffenen Unternehmen wurden die jeweils schwerwiegendsten Vorfälle durch unternehmensinterne Kontrollen aufgedeckt, was einem Anstieg um sieben Prozentpunkte gegenüber 2020 entspricht.

Arten von Wirtschaftskriminalität, aufgeschlüsselt nach Branchen



Quelle: PwC's Global Economic Crime and Fraud Survey 2022

IM FOKUS

Wirtschaftskriminalität in Zeiten einer Rezession

Die Pandemie hat viele Unternehmen durch die beschleunigte digitale Transformation in alarmierendem Maße verwundbar gemacht. So hat beispielsweise die Arbeit aus dem Homeoffice die Angriffsfläche für Cyberkriminelle erweitert. Gleichzeitig hatte die Pandemie jedoch auch einen weiteren Effekt: Vermögensdelikte, die zwar immer noch zu den häufigsten Wirtschaftsstraftaten gehören, sind in den vergangenen 24 Monaten zurückgegangen, was wohl zum Teil auch auf die Arbeit im Homeoffice zurückzuführen ist.

68 % der von Wirtschaftskriminalität betroffenen Unternehmen gab an, in den letzten 24 Monaten mit neuen Verhaltensvorfällen wie Betrug durch Kunden als Folge der durch die Corona-Pandemie verursachten Veränderungen konfrontiert gewesen zu sein. 72 % der Unternehmen sahen sich in dieser Situation einem erhöhten Verhaltensrisiko ausgesetzt. In Bezug auf Plattformen waren 29 % der Unternehmen von Vorfällen wie mangelnde „Know Your Customer (KYC)“-Prüfung betroffen und 40 % waren einem erhöhten Plattformrisiko ausgesetzt.

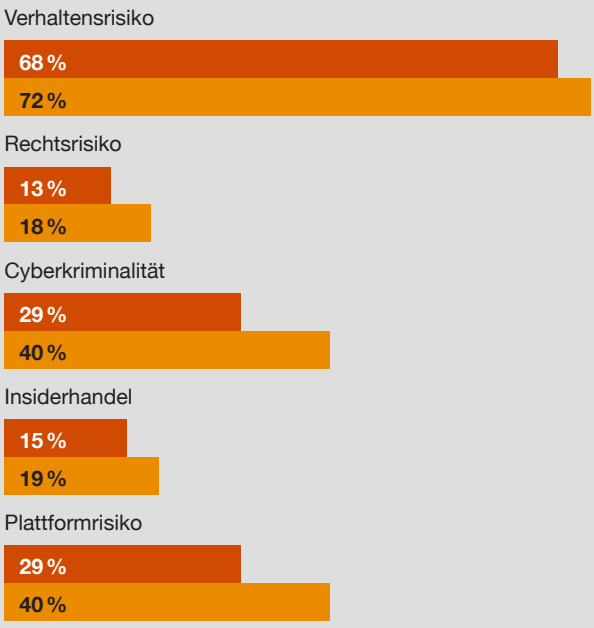
Doch wie können Unternehmen auf ein erhöhtes Risiko von Wirtschaftskriminalität in Zeiten einer Rezession reagieren? Hier lohnt sich ein Blick auf die letzten Abschwünge – etwa die Rezession von 2007 bis 2009. Dort zeigt sich, dass neue Betrugsmuster in wirtschaftlich turbulenten Zeiten nicht sofort erkannt werden. Oft dauert es 18 bis 24 Monate, bis diese Fälle sichtbar werden. In wirtschaftlichen Umbruchzeiten können jedoch interne Betrugsfälle auch leichter sichtbar werden, weil die Anpassung des betrügerischen Verhaltens der Umstellung auf ein verändertes wirtschaftliches Umfeld hinterherhinkt – z. B. korruptive Handlungen, durch die in Zeiten einer Rezession unrealistisch hohe Verkaufszahlen erreicht werden. Es gibt also allen Grund, in Zeiten einer Rezession die Aufmerksamkeit verstärkt auf wirtschaftskriminelle Aktivitäten zu richten, auch auf solche, mit denen das Unternehmen bisher vielleicht noch nicht konfrontiert war.

70 %

der von Wirtschaftskriminalität betroffenen Unternehmen verzeichneten neue Deliktarten als Folge der durch die Corona-Pandemie verursachten Veränderungen

Wirtschaftskriminelle Aktivitäten und Risiken als Folge der COVID-19-Pandemie

Aufgeschlüsselt nach Betrugs-/Risikobereichen



Quelle: PwC's Global Economic Crime and Fraud Survey 2022

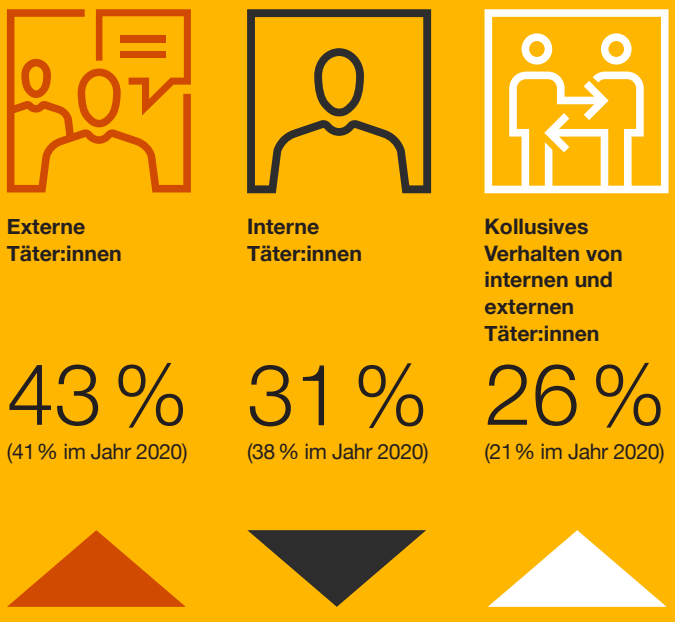
2

Neue Bedrohungen erfordern neue Schutzmaßnahmen

Die Studie zeigt, dass sich ein neues, beunruhigendes Bedrohungsprofil abzeichnet: Externe Täter:innen, deren Verhalten durch Unternehmen nicht kontrolliert und schwer beeinflusst werden kann, werden stärker und effektiver. Fast 70 % der von wirtschaftskriminellen Handlungen betroffenen Unternehmen gaben an, dass ihr gravierendster Vorfall entweder ausschließlich auf externe Täter:innen oder auf kollusives Verhalten von externen und internen Täter:innen zurückzuführen ist. Konventionelle Werkzeuge der Betrugsbekämpfung wie Verhaltensregeln, Schulungen und interne Ermittlungen sind zur Abwehr von Angriffen durch externe Täter:innen entweder nur wenig oder überhaupt nicht effektiv einsetzbar.

Hacker und Angreifer:innen aus dem Bereich der organisierten Kriminalität gehörten in der aktuellen Untersuchung zu den häufigsten externen Täter:innen und haben in den vergangenen beiden Jahren erheblich an Einfluss gewonnen. In etwa einem Drittel der Fälle mit externen Täter:innen handelte es sich bei den Angreifer:innen um Hacker und in 28 % der Fälle um Personen aus dem Bereich der organisierten Kriminalität. Im Vergleich zu unserer Untersuchung aus dem Jahr 2020 sind beide Anteile gewachsen.

Hauptverantwortlich für das schwerwiegendste Delikt



Quelle: PwC's Global Economic Crime and Fraud Survey 2022

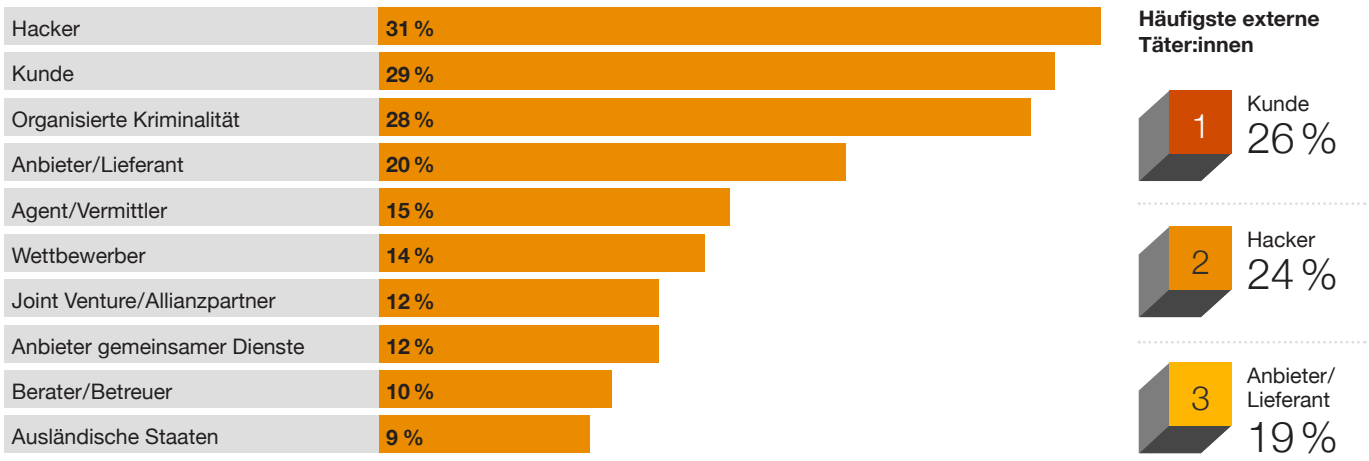
Täter:innen aus dem Bereich der organisierten Kriminalität gehen immer strukturierter und spezialisierter vor. Sie nutzen gezielt Schwachstellen aus und investieren ständig in neue Methoden, um ihre Opfer zu überlisten. Die Bekämpfung dieser Gruppe unterscheidet sich von den Bemühungen zur Eindämmung von internen wirtschaftskriminellen Aktivitäten, da Unternehmen kaum Möglichkeiten haben, Aktivitäten aus dem Bereich der organisierten Kriminalität zu beeinflussen oder zu kontrollieren.

Die Zunahme externer wirtschaftskrimineller Aktivitäten lässt sich auf eine Kombination aus verschiedenen Faktoren zurückführen. Dieser Trend wird sich in Zukunft fortsetzen. Erstens wird es, wie in den vergangenen Jahren auch, weiterhin eine hohe Zahl an Fällen von Datendiebstahl oder -missbrauch geben. Für Unternehmen wird es immer schwieriger, die personenbezogenen Daten aus dem Kundenverhältnis zu schützen. Zudem wird durch den Diebstahl der Daten die Wirksamkeit der etablierten wissensbasierten Authentifizierungsstrategien (z. B. Abfrage einer geheimen persönlichen Frage zur Änderung des Passwortes) reduziert.

Zweitens kooperieren viele Täter:innen nun auch miteinander. Dadurch sind sie in der Lage, Angriffe in größerem Umfang und auf höherem technischen Niveau durchzuführen. Dank Chatrooms, dem Dark Web und Kryptowährungen können sich Spezialist:innen zu Datendiebstählen, zur Erstellung falscher Identitäten, zu Angriffsmethoden und auf anderen Spezialgebieten in einer wachsenden kriminellen Wirtschaft vernetzen, sich koordinieren und Transaktionen durchführen.

Drittens zeichnet sich darüber hinaus der Trend ab, dass sich Personen, die bislang nicht straffällig waren, Betrugsgruppen anschließen. Dieser Trend ist in Ländern mit schlechten sozioökonomischen Bedingungen besonders ausgeprägt. Dort rechtfertigen die Menschen solche Handlungen für sich damit, dass sie weniger legitime wirtschaftliche Möglichkeiten haben.

Arten der externen Tätergruppen



Quelle: PwC's Global Economic Crime and Fraud Survey 2022

3

Plattformen bieten neue Angriffsflächen für wirtschaftskriminelle Aktivitäten

Vier von zehn der Unternehmen, die in den vergangenen beiden Jahren von Wirtschaftskriminalität betroffen waren, haben diese in verschiedenen Formen auf ihren digitalen Plattformen erlebt – zum Beispiel in Zusammenhang mit ihrer KYC-Prüfung, Desinformation, Geldwäsche und Verstößen gegen Wirtschaftssanktionen. Die zunehmende Verbreitung digitaler Plattformen etwa in den Bereichen Social Media, Dienstleistungen und E-Commerce öffnet einer Vielzahl von Risiken, die die meisten Unternehmen gerade erst zu erkennen beginnen, Tür und Tor.

Plattformrisiken beschränken sich nicht nur auf den Cyberangriff selbst, sie können Dominoeffekte auslösen. Der Angriff auf eine Plattform ist mit einem Einbruch in das Unternehmen vergleichbar. Haben sich Kriminelle erst einmal Zugang verschafft, können sie verschiedenste Arten wirtschaftskrimineller Handlungen mit Auswirkung auf das gesamte Unternehmen begehen. Plattformbetrug als unternehmensweites Problem erfordert daher eine Bekämpfung durch konzernweite und auch funktionsübergreifende Maßnahmen — und mit einer schlagkräftigen Gemeinschaft von Problemlöser:innen.

Was ist Plattformbetrug?

- Betrug auf **Handelsplattformen** (z. B. Betrug durch Kunden durch Nutzung falscher Identitäten, Diebstahl von Identitäten)
- Betrug auf **Banking-Plattformen** (z. B. Verstöße gegen die KYC-Prüfung oder gegen Vorschriften zur Vermeidung von Geldwäsche, Terrorismusfinanzierung sowie gegen Wirtschaftssanktionen)
- Betrug auf **Social-Media-Plattformen** (z. B. Verbreitung von Falschinformationen)

40 %

der von Wirtschaftskriminalität betroffenen Unternehmen waren Opfer von Plattformbetrug

IM FOKUS

Neue Bedrohungen: ESG-Betrug

Aufkommende, neue Risiken bergen die Gefahr, in den kommenden Jahren gravierende Schäden anzurichten, wenn sich Unternehmen unzureichend auf diese vorbereiten und diesen begegnen. Diese zunächst wenig wahrnehmbaren Risiken können sich rasant zu einer erheblichen Gefahr entwickeln. Im Rahmen der Befragung gaben beispielsweise nur sechs Prozent der Unternehmen an, dass sie in den vergangenen 24 Monaten Opfer eines Betruges durch Verstöße gegen Wirtschaftssanktionen wurden. Wie werden die Erfahrungen mit dieser Deliktart in den nächsten 24 Monaten aber aussehen, wenn die weltweiten Sanktionen auf das höchste Niveau der jüngeren Geschichte steigen?

Die Herausforderung beim Umgang mit neuen wirtschaftskriminellen Risiken besteht darin, nicht in die Falle zu tappen, nur auf bekannte Gefahren zu schauen und Unbekanntes auszublenden. Welches sind also die neuen Deliktarten, die am meisten Anlass zur Sorge geben könnten? PwC glaubt, dass man insbesondere zwei von ihnen im Blick behalten sollte.

Betrug in Zusammenhang mit der ESG-Berichterstattung: Gesellschaftliche Verantwortung und Vertrauen sind zu einem wichtigen Werkzeug für die Wertschöpfung geworden. Die 25. jährliche globale CEO-Umfrage von PwC hat 2022 den Zusammenhang zwischen Unternehmen, in denen ein hohes Maß an Vertrauen herrscht, und ihrer Fähigkeit, den Wandel voranzutreiben, deutlich gemacht. Aber Vertrauen ist fragil. Ein vermeintliches oder tatsächliches Fehlverhalten in Bezug auf Transparenz kann den Ruf einer Marke und das ihr zugrunde liegende Vertrauen stark beeinträchtigen. Da die Verantwortung für Umwelt, Gesellschaft und Governance (engl. Environment, Social and Governance, kurz ESG) für die Stakeholder immer wichtiger wird, sind die Genauigkeit und Richtigkeit der ESG-Berichterstattung von entscheidender Bedeutung. Während nur acht Prozent der in den vergangenen 24 Monaten von Wirtschaftskriminalität betroffenen Unternehmen Opfer von Betrug bei der ESG-Berichterstattung wurden, werden die Anreize für solche Wirtschaftsdelikte sowie deren Auswirkungen eher zunehmen.

Befragt nach den drei größten Herausforderungen bei der Bewältigung der Risiken im Zusammenhang mit ESG-Zielen und Anforderungen an die Berichterstattung geben 52 % der Unternehmen aller Branchen (mit Ausnahme von Financial Services) die Fähigkeit an, ESG-Kennzahlen innerhalb der Organisation genau zu überwachen oder zu berichten. Für 48 % sind es mangelnde ESG-Ziele in ihrem Unternehmen und für 45 % ist es die Unfähigkeit, Fehlverhalten im Zusammenhang mit ESG-Risiken zu verhindern oder aufzudecken.

8 %

aller von Wirtschaftskriminalität betroffenen Unternehmen erlebten in den letzten 24 Monaten ESG-Meldebetrug.

1 von 8

Unternehmen gaben an, in den letzten 24 Monaten von Lieferkettenbetrug betroffen zu sein.

IM FOKUS

Neue Bedrohungen: Betrug in der Lieferkette

12,5 %

der Unternehmen sind als Folge der Corona-Pandemie neuen Fällen von Lieferkettenbetrug ausgesetzt.

Jedes fünfte

Unternehmen ist in seiner Lieferkette einem erhöhten Risiko für Wirtschaftskriminalität ausgesetzt.

Nur wenige Unternehmen sind sich der Risiken von Betrug und Fehlverhalten innerhalb ihrer Lieferkette bewusst, sodass dieser Deliktsbereich heute und in Zukunft ein erhöhtes Risiko darstellt.

für

43 %

der deutschen Unternehmen aller Branchen (mit Ausnahme von Financial Services) haben effiziente Technologien und Prozesse zur Ermittlung und Verwaltung von Risiken in der Lieferkette erhebliche Auswirkungen.

Lediglich

19 %

geben an, dass ihr Unternehmen einen speziellen Verantwortlichen für das Management von Risiken in der Lieferkette eingesetzt hat, während

45 %

die Risikofunktionen unternehmensweit integrieren.

Was Sie beim Schutz Ihres Unternehmens vor externen Bedrohungen bedenken sollten

Die Befragten der diesjährigen globalen Umfrage zur Wirtschaftskriminalität geben an, zum Schutz vor kriminellen Aktivitäten sowie zu deren Aufdeckung ihre internen Kontrollen, Technologien und ihr Meldewesen zu verstärken. Zur Abwehr externer Angreifer:innen reicht dies alleine jedoch nicht aus. Angesichts der Tatsache, dass diese Art Angriffe in den Mittelpunkt rücken, finden Sie hier drei Überlegungen, die Ihnen dabei helfen, sich besser dagegen zu wappnen:

1. Betrachten Sie den gesamten Lebenszyklus von Produkten.
Finden Sie heraus, wo es Möglichkeiten für Kriminelle gibt, ein Produkt auszunutzen und damit dem Unternehmen einen finanziellen, straf- oder sanktionsrechtlichen Schaden oder einen Reputationsschaden zuzufügen. Wie könnte es zu Betrugsfällen kommen, was wäre nötig, um sie zu verhindern, und welche Art von Reaktion ist im Betrugsfall erforderlich?

2. Sorgen Sie für ein ausgewogenes Verhältnis zwischen Benutzerfreundlichkeit und Betrugskontrolle.
Um Kanäle für Kunden vor Betrug zu schützen, müssen Sie ein ausgewogenes Gleichgewicht zwischen einer positiven Nutzererfahrung und dem Erkennen und Verhindern von Betrug sicherstellen. Das Ziel, die Zahl der falsch-positiven Fälle zu verringern und gleichzeitig weiterhin echten Betrug zu erkennen, lässt sich durch eine Kombination aus Technologien, Strategien und Prozessen zur Betrugserkennung erreichen.

3. Stellen Sie eine zentralisierte Verwaltung der Daten sicher.
Oft kommen Betrugssignale aus verschiedenen, nicht miteinander verbundenen Systemen und können nur durch eine stichprobenartige, manuelle Prüfung erkannt werden. Es ist von entscheidender Bedeutung, dass Sie Betrugsindikatoren in einer zentralisierten Plattform zusammenführen, die den gesamten Lebenszyklus von Benutzer:innen (ob Betrug oder nicht) verfolgen und aussagekräftige Warnmeldungen erzeugen kann.

Fazit

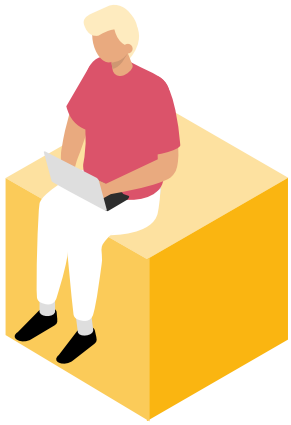
Die globale PwC-Studie zur Wirtschaftskriminalität hat gezeigt, dass die Prävention von Betrug und anderen Wirtschaftsdelikten eine komplexe Herausforderung ist. Sie erfordert eine kontinuierliche Fokussierung auf Richtlinien, Schulungen und interne Kontrollen sowie in zunehmendem Maße den Einsatz hochentwickelter Technologien. In diesem unbeständigen Umfeld ist der Schutz des Unternehmens gegen externe Bedrohungen von entscheidender Bedeutung. Denn alle Zeichen deuten darauf hin, dass Betrüger:innen die Lücken immer besser ausnutzen können – und werden. Deutsche und internationale Behörden bauen deshalb zusätzliche Ressourcen für die Ermittlung und Verfolgung von Unternehmensdelikten auf – einschließlich der Bereiche Cyberkriminalität, Kryptowährungen und insbesondere ESG.

Methodik:

Der Global Economic Crime and Fraud Survey von PwC untersucht seit über zwei Jahrzehnten die globalen Risiken von Wirtschaftskriminalität. Die diesjährige Erhebung setzt sich erstmals aus einer zweiteiligen Befragung zusammen. Der erste Teil fokussiert sich auf wirtschaftskriminelle Verhaltensrisiken. Dafür wurden weltweit ca. 1.300 Führungskräfte in 53 Ländern befragt, davon waren 58 Führungskräfte aus Deutschland.

Seit über 20 Jahren untersucht der PwC Global Economic Crime and Fraud Survey Straftaten wie:

- Bilanzfälschung
- Wettbewerbs- und kartellrechtliche Verstöße
- Vermögensdelikte
- Bestechung und Korruption
- Betrug durch Kunden
- Cyberkriminalität
- Betrügerische Geschäftspraktiken
- Betrug im Personalbereich
- Insiderhandel/unerlaubter Handel
- Geldwäsche und Sanktionen
- Betrug im Einkauf
- Steuerbetrug



61 %

der Befragten gehören der C-Suite an

39 %

der Befragten arbeiten in Unternehmen mit einem Jahresumsatz von über 1 Mrd. US-Dollar (und 65 % in Unternehmen mit einem Jahresumsatz von über 100 Mio. US-Dollar)

Die in dieser Studie aufgeführten Risiken sind dabei wie folgt klassifiziert:

Verhaltensrisiken:	Betrug durch Kunden, Betrug in der Lieferkette, Betrug im Einkauf, Betrug im Personalbereich, Vermögensdelikte, Steuerbetrug, Betrug bei staatlichen Unterstützungen, Bilanzfälschung, Korruption, Betrug bei der ESG-Berichterstattung
Rechtsrisiken:	Diebstahl geistigen Eigentums, Wettbewerbs- und kartellrechtliche Verstöße
Cyberrisiken:	Cyberkriminalität
Insiderhandel:	Betrügerische Geschäftspraktiken, Insiderhandel/unerlaubter Handel
Plattformrisiken:	Betrug auf Handelsplattformen (z. B. Nutzung falscher Identitäten), auf Banking-Plattformen (z. B. Verstöße gegen die KYC-Prüfung oder gegen Vorschriften zur Vermeidung von Geldwäsche, Terrorismusfinanzierung sowie gegen Wirtschaftssanktionen), oder Social-Media-Plattformen (z. B. Verbreitung von Falschinformationen).

Kontakte

Claudia Nestler

Partnerin
Leiterin Forensic Services
PwC Deutschland
Tel.: +49 69 9585 5552
E-Mail: claudia.nestler@pwc.com

Arndt Engelmann

Partner
Forensic Services
PwC Deutschland
Tel.: +49 89 5790 5850
E-Mail: arndt.engelmann@pwc.com

www.pwc.de/gecs