Schachmatt durch KI? Wirtschaftskriminalität und Strategien zur Abwehr

Wie Kriminelle ihre Betrugsmaschen professionalisieren und mit welchen Schachzügen sich Unternehmen schützen können.

Schachmatt durch KI?

Stellen Sie sich vor, Sie betreten ein Schachbrett, auf dem die Figuren nicht aus Holz, sondern aus Code bestehen. Und Ihre Gegner sind nicht nur Menschen, sondern auch Maschinen, die mit der Präzision und Geschwindigkeit eines Supercomputers agieren. Willkommen in der neuen Ära der KI-gestützten Wirtschaftskriminalität, wo die Grenzen zwischen Realität und Täuschung zunehmend verschwimmen.

Auf den folgenden Seiten nehmen wir Sie mit auf eine Reise durch die neuesten Entwicklungen in der kriminellen Welt, die durch KI-Tools befeuert werden. Künstliche Intelligenz bringt in vielen Bereichen enorme Effizienzsteigerungen für Unternehmen – aber sie ist ein zweischneidiges Schwert. Denn gleichzeitig ermöglicht sie es Kriminellen, mit beispielloser Raffinesse und Effizienz zuzuschlagen, ohne zwingend selbst Spezialkenntnisse zu haben. „Hacking as a service" gehört ebenso wie Deepfake-Tools zum gängigen Angebot in den gut gefüllten Darknet-Regalen.

Die Zahlen klingen alarmierend: Laut World Economic Forum (WEF)[1] ist der globale Zuwachs beim Handel mit Deepfake-Tools im Darknet von Anfang 2023 bis 2024 um sage und schreibe 223 % gestiegen. Cybersecurity-Experten verzeichneten in der Folge einen explosionsartigen Anstieg von Voice-Phishing-Versuchen[2]. Mit sogenanntem „Vishing" versuchen Kriminelle, Systeme zu infiltrieren und an Zugangsdaten von Mitarbeitenden zu gelangen, beispielsweise über gefälschte IT-Helpdesk-Anrufe.

Aber auch manipulierte Rechnungen sind dank KI kaum noch vom Original zu unterscheiden, und Schäden durch gefälschte Identitäten nehmen laut Allianz Trade Schadensstatistik ebenfalls zu, sowohl bei der „Fake-President"-Betrugsmasche als auch beim Bestellerbetrug.

Social Engineering und Deepfakes sind scharfe Waffen im Arsenal der Betrüger, die mit der Präzision eines Schachgroßmeisters ihre Züge planen. Deshalb geht es auf den folgenden Seiten nicht nur um Betrugsmaschen, sondern auch darum, wie Unternehmen die zunehmend hochprofessionellen Angriffe erkennen und abwehren können, um nicht schachmatt gesetzt zu werden.

[1] World Economic Forum Global Cybersecurity Outlook 2025
[2] CrowdStrike Global Threat Report 2025

INHALT

2,8 Mrd. Euro

So hoch waren die Schäden von Unternehmen durch Wirtschaftskriminalität 2024 in Deutschland. Insgesamt wurden 61.358 Fälle erfasst – das ist ein Plus von 58 %.

Quelle: Bundeslagebild Wirtschaftskriminalität 2024

223 %

So groß ist der globale Zuwachs beim Handel mit Deepfake-Tools im Darkweb zwischen dem 1. Quartal 2023 und dem 1. Quartal 2024

Quelle: World Economic Forum Global Cybersecurity Outlook 2025

98 %

der Organisationen in der DACH-Region berichten von steigenden Multi-Channelangriffen. E-Mail-Angriffe dominieren weiterhin.

Quelle: Sosafe Cybercrime Trends 2025

442 %

So stark war der weltweite Anstieg bei Voice-Phishing-Versuchen (Vishing) Versuchen zwischen dem ersten und zweiten Halbjahr 2024.

Quelle: CrowdStrike Global Threat Report 2025

81 %

der weltweiten Angriffe auf kompromittierte Systeme erfolgte ohne Malware.

Quelle: CrowdStrike Global Threat Report 2025

Wirtschaftskriminalität: Alarmstufe KI

Die Schäden, die durch Wirtschaftskriminalität entstehen, steigen weiter deutlich an. Künstliche Intelligenz verhilft zu Effizienzsprüngen – spielt dabei aber auch Kriminellen in die Hände: Mit generativen KI-Tools verfeinern sie ihre Social-Engineering-Angriffe und schneiden diese passgenau auf Unternehmen und einzelne Mitarbeitende zu. Die meisten Angriffe erfolgen malware-frei. Der Mensch bleibt die Schwachstelle und das Einfallstor.

62 %

der deutschen Unternehmen sehen Unachtsamkeit der Mitarbeitenden als begünstigenden Faktor beim Entstehen von E-Crime.

Quelle: KPMG e-Crime Report 2024

2,7 Mrd. USD

an Schäden entstanden 21.442 Unternehmen weltweit durch Social Engineering; Phishing/ Spoofing verdoppelten sich.

Quelle: FBI Crime Report 2024

83 %

der vom FBI erfassten Schäden im Jahr 2024 sind auf E-Crime-Maschen zurückzuführen.

Quelle: FBI Crime Report 2024 Schadensstatistik

218 %

Anstieg bei den Schäden durch Fake-President-Fälle im Jahr 2025.

Quelle: Allianz Trade Schadensstatistik

59 %

der deutschen Unternehmen sehen ihre Existenz durch Cyberattacken bedroht. Nur 50 % sehen ihr eigenes Unternehmen sehr gut vorbereitet.

Quelle: Bitkom Studie Wirtschaftsschutz 2025

57 %

aller Dokumentenfälschungen sind inzwischen digital.

Quelle: KPMG Studie Generative KI in der IT-Forensik und im Rahmen digitaler Ermittlungen 2025

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. Kriminelle oder sogenannte „Social Engineers“). Ein Blick in die Allianz Trade Schadensstatistik liefert spannende Erkenntnisse und zeigt aktuelle Trends auf.

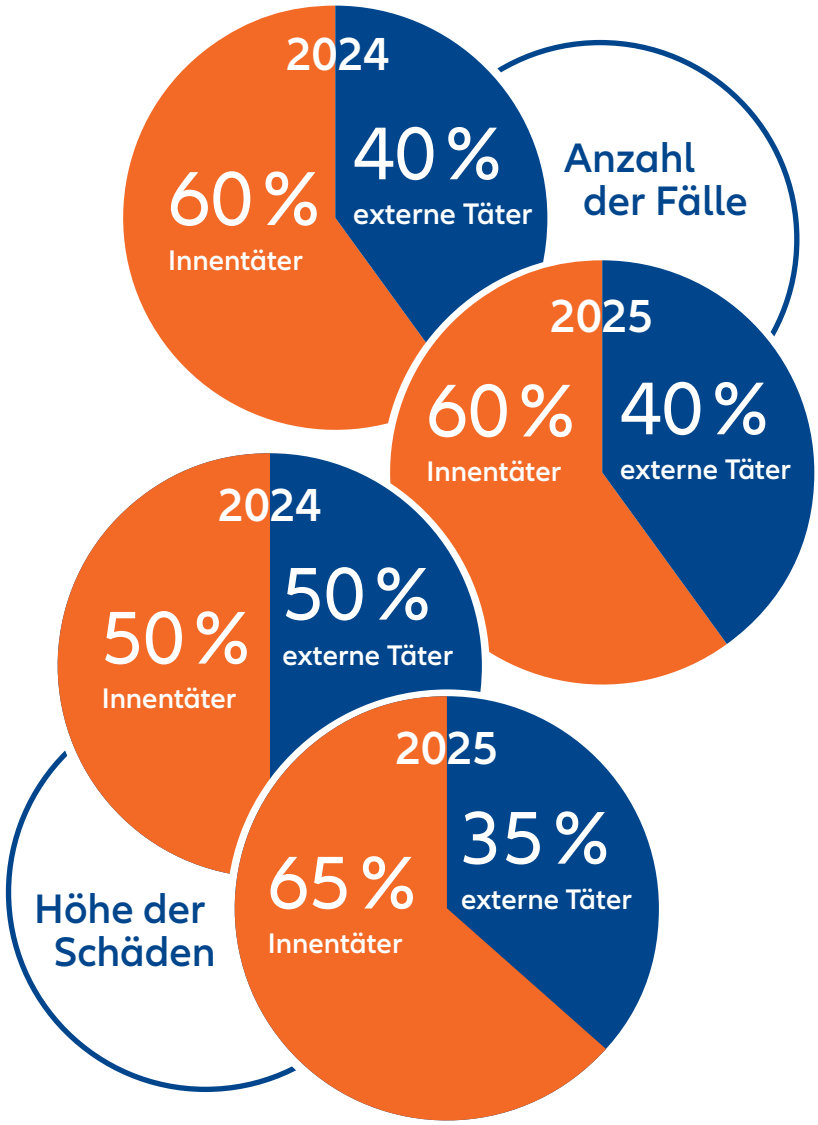
Alarmstufe KI: Wirtschaftskriminelle steigern ihre Professionalität

Künstliche Intelligenz (KI) spielt Wirtschaftskriminellen in die Hände: Sie werden immer professioneller, schlagen immer häufiger zu – und richten immer größere finanzielle Schäden an. In den vergangenen Jahren legten besonders die externen Täter deutlich zu.

Bei den Schadenssummen (Höhe der gemeldeten Schäden in Euro) lagen 2024 interne und externe Täter erstmals gleichauf (je 50%).

2025 hat sich dieser Trend jedoch wieder normalisiert und die Innentäter erbeuteten mit rund 65 % die größten Summen – auf externe Täter entfielen im vergangenen Jahr 35 % der Schäden.

Sogenannte „Innentäter“, also die eigenen Mitarbeitenden, richteten 2025 allerdings nicht nur die größten, sondern auch die meisten Schäden an. Diese unangenehme und häufig unterschätzte Wahrheit für Unternehmen bleibt also auch weiterhin Realität: Interne Täter waren sowohl 2024 als auch 2025 jeweils für rund 60 % der gemeldeten Schadensfälle verantwortlich, die externen Täter für „nur noch“ 40 %.



Quelle: Allianz Trade Schadensstatistik

Die Kunst der Manipulation: Social Engineering weiter auf dem Vormarsch

Unter Social Engineering fallen Betrugsmaschen, bei denen die Täter Menschen manipulieren. Dazu gehören insbesondere Zahlungs- und Bestellerbetrug sowie die sogenannte „Fake-President"-Betrugsmasche, bei der sich die Täter als vermeintliche Chefs ausgeben (deshalb u.a. auch als „CEO Fraud" bekannt) und Mitarbeitende anweisen, Geldsummen für vorgetäuschte Geschäftstransaktionen auf betrügerische Konten zu überweisen.

Diese Betrugsmaschen machten 2025 etwa die Hälfte (55%) der bei Allianz Trade gemeldeten externen Fälle aus und rund 78% des dazugehörigen gemeldeten Schadensvolumens. Im Durchschnitt der letzten Jahre lagen diese Anteile bei rund 50% der Fallzahlen und etwa 44% beim Schadensvolumen.

Katz- und Mausspiel zwischen Angreifern und Abwehrmechanismen

Die „Menschen-Hacker" verfeinern ihre Kunst der Manipulation zunehmend, auch mit Hilfe von KI-Tools. Der Handel mit Deepfake Tools im Darknet boomt[1]. Unternehmen versuchen, ihre Abwehrstrategien schnellstmöglich anzupassen – doch es bleibt ein Katz- und Maus-Spiel im Wettlauf von Angriffsmaschen und Abwehrmechanismen (siehe auch Interview S. 9), das sich auch in den Zahlen widerspiegelt:

2023 markierte zunächst einen Negativrekord bei der Häufigkeit von Social-Engineering-Betrugsmaschen. 2024 folgte eine kurze Verschnaufpause auf weiterhin sehr hohem Niveau: Fallzahlen gingen um 20 % zurück. Die Schadenssummen stiegen allerdings trotzdem um 15 %.

[1] World Economic Forum Global Cybersecurity Outlook 2025: Der globale Zuwachs beim Handel mit Deepfake-Tools im Darknet stieg um 223 % zwischen dem 1. Quartal 2023 und dem 1. Quartal 2024.

Schadenssummen 2025 auf neuem Rekordhoch

2025 verschafften sich die Kriminellen erneut einen Vorsprung und erreichten einen neues Rekordhoch. Die Höhe der gemeldeten Schadenssummen bei Social-Engineering-Betrugsmaschen schnellte um 60% nach oben; maßgeblich getrieben durch Großschäden bei Fake President und Bestellerbetrug (Fake Identity) – eine Masche, die in den Vorjahren zwar viele, aber eher kleinere Schäden verursacht hat.

Die Fallzahlen aller Social-Engineering-Maschen nahmen 2025 im Vergleich zum Vorjahr ebenfalls um 13 % zu. Insbesondere Bestellerbetrug (Fake Identity), bei dem Warenströme an manipulierte Lieferadressen umgeleitet werden, erlebte nach einem deutlichen Rückgang im Vorjahr 2025 wieder ein echtes Revival und löste Zahlungsbetrug als Lieblingsmasche der Social Engineers an der Spitze ab.

+ 13 %
Anstieg der Social-Engineering-Betrugsfälle 2025 vs. 2024

+ 60 %
Anstieg der der Social-Engineering-Schadenssummen 2025 vs. 2024

Quelle: Allianz Trade Schadensstatistik

Unter Allianz Trade werden verschiedene Dienstleistungen von Euler Hermes angeboten.

Perfektion durch KI führt zu Rekordschäden bei „Fake President“

Der „Fake President“ kommt trotz großer Bekanntheit der Betrugsmasche nicht aus der Mode. Sowohl 2024 (-12 %) als auch 2025 (-13 %) waren die Fallzahlen zwar rückläufig, die erbeuteten Summen verdreifachten sich jedoch im Jahr 2024 (+200 %) und schnellten auch 2025 um weiteren 81 % in die Höhe. Fazit: Wenn es knallt, dann richtig.

Im Durchschnitt liegen die Schäden aktuell im einstelligen Millionenbereich, die Großschäden bewegen sich teilweise sogar im deutlich zweistelligen Millionenbereich, wie zu Beginn der Betrugsmasche Anfang der 2010er Jahre.

Das deutet darauf hin, dass die Angriffe zwar selektiver sind, mit der Unterstützung von KI aber extrem professionell durchgeführt werden und somit häufig sehr erfolgreich sind. Kriminelle gehen dabei oft mehrstufig vor und setzen in einem ersten Schritt häufig auch auf Phishing oder Voice-Phishing, sogenanntes „Vishing“[2]. Mit diesen Techniken versuchen Kriminelle, Systeme zu infiltrieren und an Zugangsdaten von Mitarbeitenden zu gelangen, beispielsweise über gefälschte IT-Helpdesk-Anrufe. Zudem versuchen sie so an Unternehmensinterna zu gelangen, um ihre Folgeangriffe möglichst glaubwürdig zu gestalten (siehe auch Seite 7).

Neuer Liebling: Bestellerbetrug stößt Zahlungsbetrug vom Thron

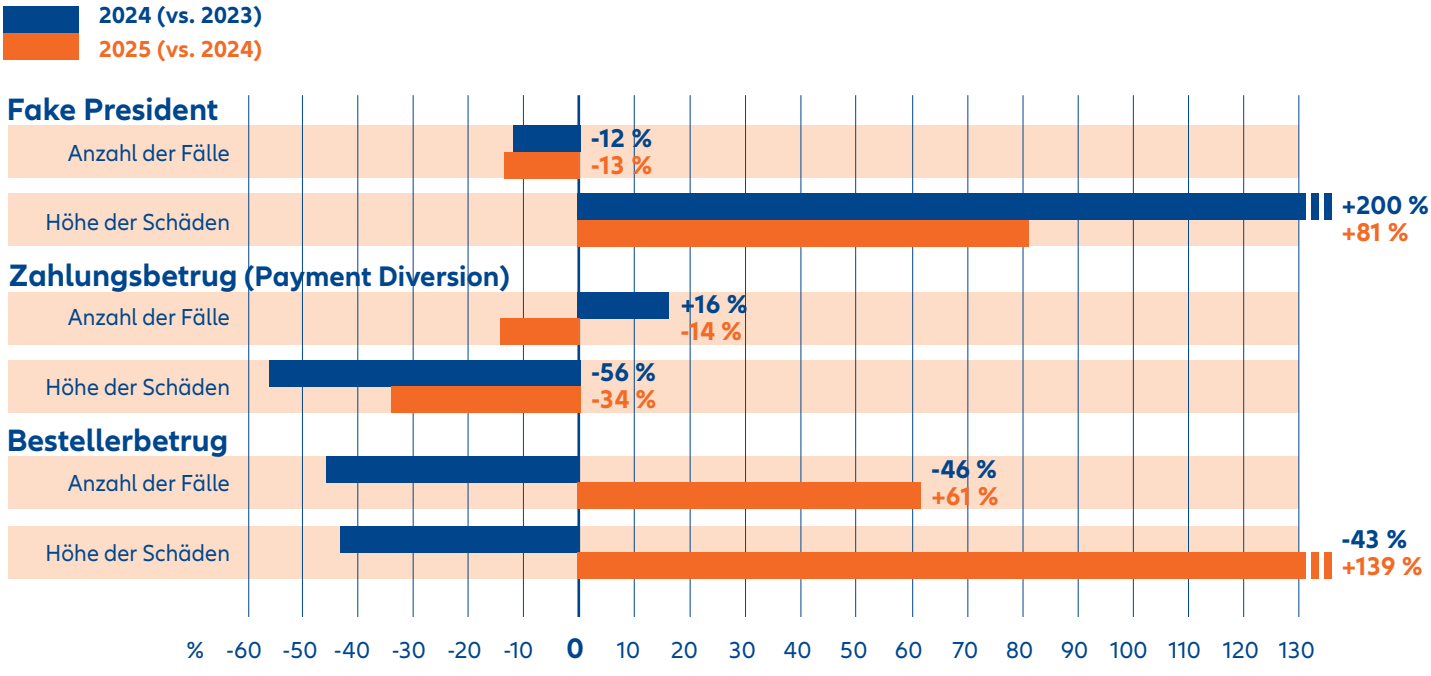
Beim Bestellerbetrug (Fake Identity) ging es nach einem Rekord 2023 bei den Fallzahlen 2024 zunächst deutlich nach unten in der Beliebtheitsskala der Angreifer (-46 %). 2025 kam allerdings das Revival mit einem Anstieg der Fallzahlen (+61 %), verbunden mit starken Anstieg der Schadenssummen (+139 %), vor allem getrieben von außergewöhnlich vielen Großschäden.

Bestellerbetrug verzeichnete 2025 die meisten Fällen bei den drei Social-Engineering-Maschen und löste damit den Zahlungsbetrug als Spitzenreiter des Vorjahres ab.

Zahlungsbetrug ging 2025 bei den Fallzahlen um 14 % zurück, das Schadenvolumen sank mangels Großschäden sogar um rund ein Drittel (-34 %).

[2] CrowdStrike Global Threat Report 2025: Der weltweite Anstieg bei Voice-Phishing (Vishing) Versuchen zwischen dem ersten und zweiten Halbjahr 2024 lag bei 442 %. Mit Vishing versuchen Kriminelle u.a. durch Social-Engineering-Techniken, Zielnetzwerke zu infiltrieren oder an Zugangsdaten zu kommen. Entsprechend erfolgte 81% der weltweiten Angriffe auf kompromittierte Systeme ohne Malware, durch gestohlene Zugangsdaten und legitime Tools, die z.B. über Vishing erlangt wurden.

Trends in Zahlen: Veränderung von Fallzahlen und Schadenhöhen



Quelle: Allianz Trade Schadensstatistik

PHISHING 2026

DIE UNTERSCHÄTZTE GEFAHR UND IHRE FATALEN ANSCHLUSSDELIKTE

Autor: Dirk Koch

Dirk Koch ist Partner in der Rechtsanwaltskanzlei ByteLaw Rechtsanwälte in Frankfurt und Certified Ethical Hacker (CEHv11). Er ist spezialisiert auf die Bereiche Cyber- und IT-Sicherheit, Cyberkriminalität, Beratung und Reaktion bei Angriffen und Sicherheitslücken sowie Investigation, IT-Forensik, Datenschutz und Datensicherheit.

Phishing ist längst nicht mehr der plumpe Betrug der frühen Internetjahre. Heute gleicht es raffinierten Schachzügen, bei dem Cyberkriminelle mit chirurgischer Präzision ihr Ziel ins Visier nehmen und versuchen, ihre Gegner in mehreren Zügen schachmatt zu setzen.

Diese Täuschungsangriffe, oft unterstützt durch künstliche Intelligenz, bedrohen Unternehmen weltweit. Doch die größte Gefahr lauert nicht nur im ersten Klick, sondern auch in den perfiden Anschlussdelikten. Nach dem erfolgreichen Phishing beginnt die zweite Phase des Angriffs. Besonders Social-Engineering-Betrugsmaschen sind dabei sehr beliebt.

Diese Maschen sind die heimtückischen Fallen, die nach einem erfolgreichen Phishing-Angriff zuschnappen und Unternehmen in den finanziellen Abgrund ziehen können. Deshalb ist es umso wichtiger, die aktuelle Bedrohungslage, technische Hintergründe und wirksame Schutzmaßnahmen zu kennen, zu verstehen und vor allem umzusetzen.

Die Falle schnappt zu: Phishing und Vishing öffnen Tür und Tor

Phishing und auch Voice-Phishing, sogenanntes „Vishing“, sind nach wie vor der häufigste Einstiegspunkt für Cyberangriffe. Moderne Phishing-Mails sind täuschend echt und gleichen einem Wolf im Schafspelz. Sie sind makellos in Rechtschreibung und Design und kommen oft von kompromittierten Absenderadressen, auf die sich die Angreifer direkten Zugang verschafft haben. Die Nutzung von KI-Tools ermöglicht zudem täuschend echte Deepfake-Anrufe und Videos, die selbst erfahrenste Mitarbeitende in die Irre führen können.

Nach einem erfolgreichen Phishing- oder Vishing-Angriff beginnt die zweite Phase: Beim sogenannten „Business Email Compromise (BEC)" übernehmen Angreifer echte Firmen-E-Mail-Konten und manipulieren laufende Kommunikation. Bei Zahlungsbetrug (Payment Diversion) ändern die Täter Bankdaten in Rechnungen oder Zahlungsanweisungen. Ohne Rückbestätigung fließen Millionen auf Täterkonten. Bei Fake President oder „CEO-Fraud 2.0" setzen sie Mitarbeitende mit Deepfake-Videoanrufen oder KI-Stimmen unter Druck, sofort Überweisungen auszuführen. Ein einziger erfolgreicher Angriff kann so zu Schäden in Millionenhöhe führen.

Verteidigungsstrategien: So kommen Unternehmen auf Augenhöhe

Um sich zu schützen, müssen Unternehmen sowohl technische als auch organisatorische Maßnahmen ergreifen.

Auf technischer Seite sind Phishing-resistente Multi-Faktor-Authentifizierung (z.B. durch Hardware-Token oder Passkeys statt SMS-TAN) sowie E-Mail-Schutz durch Sicherheitsverfahren wie SPF (Sender Policy Framework)[1], DKIM (DomainKeys Identified Mail)[2] und DMARC (Domain-based Message Authentification Reporting and Conformance)[3] essenziell. Auch die Nutzung von KI-basierten Filtern sowie eine Zero-Trust-Architektur, bei der jeder einzelne Zugriff geprüft wird, hilft, Angriffe frühzeitig zu erkennen und Schaden zu begrenzen.

Organisatorisch sollten sie die Prozesse für Zahlungsfreigaben laufend überprüfen, das Vier-Augen-Prinzip bei hohen Zahlungen ebenso implementieren (und auch leben!) wie sogenannte „Out-of-Band-Bestätigungen", also Änderungen von Zahlungsdaten nur nach telefonischer Rückfrage über die bekannte, beim Erstkontakt hinterlegte Nummer. Zudem spielen regelmäßige Sensibilisierungsprogramme zur Schulung der Mitarbeitenden eine essenzielle Rolle, insbesondere zu den neusten KI-basierten Täuschungen, zu Phishing, Social Engineering und Deepfakes. Technische Schutzmaßnahmen bieten einen grundlegenden Basisschutz, der im Rahmen organisatorischer Maßnahmen – wie gezielte Anweisungen und Schulungen – durch die Sensibilisierung der Mitarbeitenden ergänzt und präzisiert werden sollte. Fortschritte bei technischen Lösungen sind bedeutsam, dennoch bleibt die aufmerksame Wahrnehmung der Beschäftigten ein entscheidender Faktor für die Gesamtsicherheit.

Vorsicht Haftungsfalle: Fehlende Schutzmaßnahmen können fatal werden

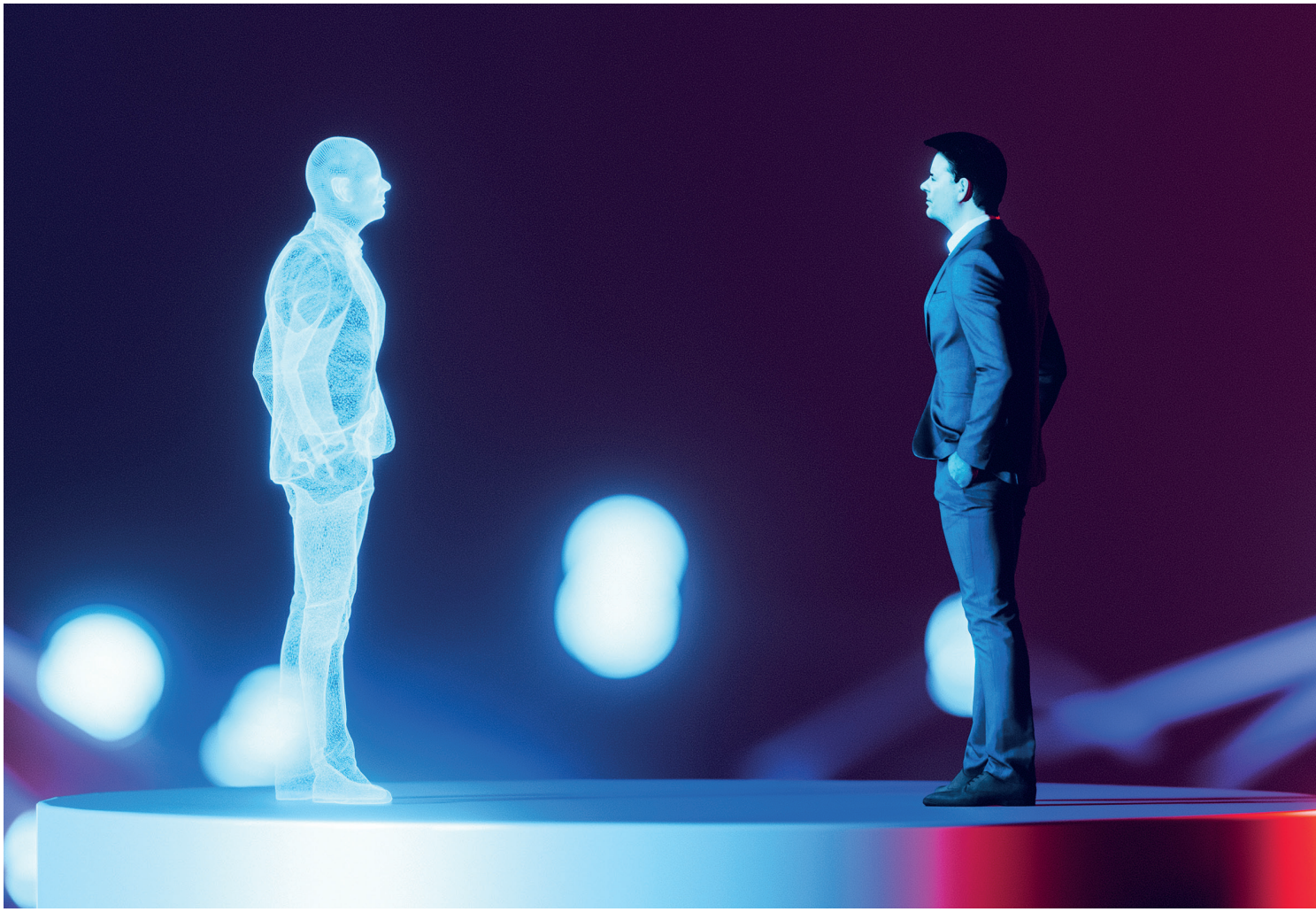
Rechtlich sind Unternehmen verpflichtet, Social-Engineering-Risiken aktiv zu managen und Vorfälle zu melden. Fehlende Schutzmaßnahmen können als Organisationsverschulden gewertet werden und zu hohen Bußgeldern sowie Haftungsansprüchen gegen das Management führen.

Phishing ist 2026 ist vielerorts eine bekannte, aber sehr unterschätzte Gefahr. Dabei ist es nicht nur ein IT-Problem, sondern ein Einfallstor und damit ein strategisches Risiko. Es ist der eine Zug, der den König ins Schach setzt. Die größte Gefahr liegt in den Folgehandlungen nach dem Klick, von manipulierten Zahlungsprozessen bis hin zu Deepfake-Betrug – und im schlimmsten Fall dem Schachmatt.

[1] SPF (Sender Policy Framework) ist ein E-Mail-Sicherheitsstandard, der Domains vor Spoofing schützt, indem er eine Liste autorisierter Server (per DNS-Eintrag) festlegt, die E-Mails im Namen der Domain versenden dürfen; empfangende Mailserver prüfen diesen Eintrag, um die Authentizität zu bestätigen und so Spam und Phishing zu reduzieren

[2] Mit DKIM (DomainKeys Identified Mail) können Domainbesitzer E-Mails von ihrer Domain automatisch signieren. Die DKIM-Signatur ist eine digitale Unterschrift. Mit Hilfe von Kryptographie verifiziert sie mathematisch, dass die E-Mail von der Domain stammt.

[3] DMARC (Domain-based Message Authentification Reporting and Conformance) sagt den Mailservern, was sie bei einem erfolglosen DKIM oder SPF tun sollen; die E-Mail als Spam markieren, die E-Mail trotzdem zustellen oder die E-Mail ganz löschen.



EXPERTENGESPRÄCH

Die Schwachstelle Mensch bleibt – und die KI findet die Lücken

Social-Engineering-Betrugsmaschen, bei denen Menschen durch Kriminelle manipuliert werden, verursachen schon seit vielen Jahren hohe finanzielle Schäden bei Unternehmen. Und ein Ende ist nicht abzusehen – im Gegenteil. ChatGPT hat die Welt verändert: Was einerseits große Effizienzsteigerungen, Arbeitserleichterungen und ganz neue Chancen eröffnet, spielt andererseits auch Betrügern in die Hände – denn ihnen wird die Arbeit nun erleichtert mit vielen neuen Möglichkeiten.

Welche das sind, erläutern die beiden Allianz Trade Experten **Marie-Christine Kragh,** Global Head of Fidelity und **Tom Alby,** Chief Digital Transformation Officer.

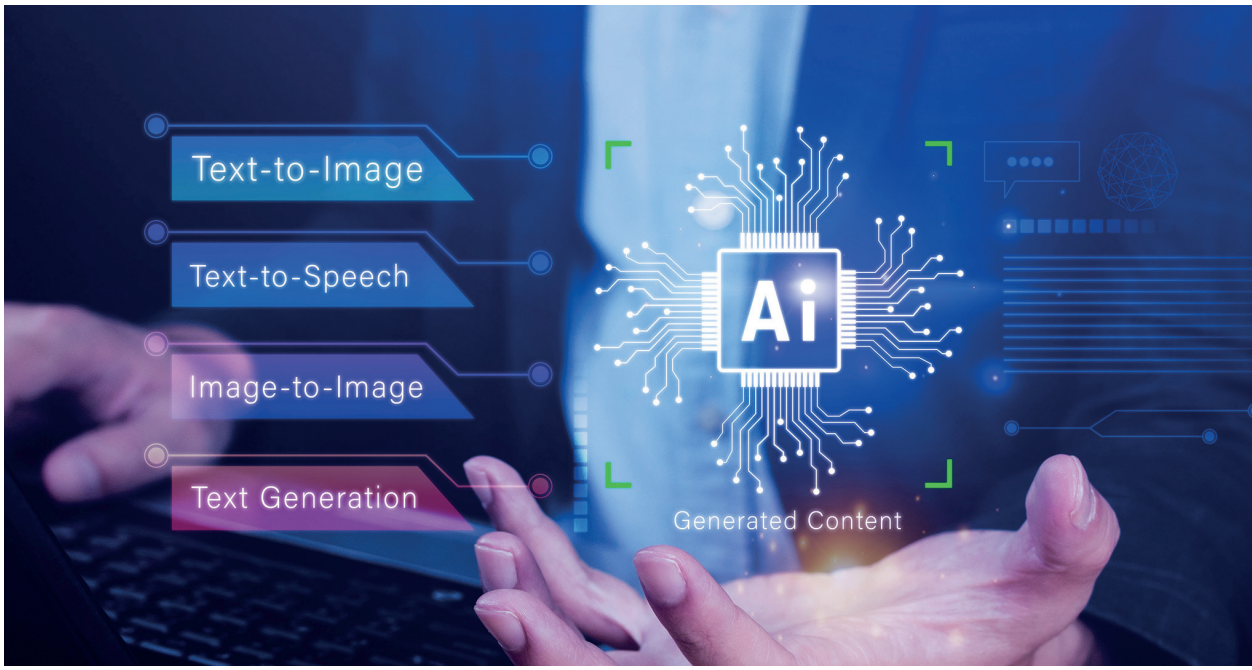
Warum kommt Social Engineering auch nach so vielen Jahren nicht aus der Mode?

Marie-Christine Kragh: Es funktioniert, weil es uns Menschen im Kern berührt, weil mit Emotionen gespielt wird. „Gut gemachtes" Social Engineering setzt genau da an, wo wir Anschlusspunkte haben – etwa in Form von Wertschätzung, nach der eigentlich jeder von uns intrinsisch sucht. Aber auch Druck kann eine entscheidende Rolle spielen oder das Heraufbeschwören einer vermeintlichen Krisensituation. Der vermeintliche Chef verweist bei der Kontaktaufnahme zum Beispiel darauf, dass man sich genau an die Person gewandt habe, weil die persönliche Zuverlässigkeit extrem wichtig sei und man genau ihr sehr vertraue. Das triggert sofort die Wertschätzung. Dann kommt der Druck, etwa mit dem Verweis auf eine vertragliche Schweigepflicht und die zeitliche Eile. Ein Unternehmen kann die beste Firewall haben, es nützt im Fall von versierten Social Engineers nur wenig: Die Schwachstelle bleibt der Mensch. Bei einem Trio aus Zeitdruck, dem Triggern von Emotionen und einer Aufforderung, vom Standard abzuweichen, sollten die Alarmglocken schrillen.

Tom Alby: Und die Künstliche Intelligenz hilft den Betrügern, genau die Lücken zu finden und die richtigen Knöpfe zu drücken. Kriminelle bekommen mit ChatGPT und anderen Large-Language-Modellen die technologische Basis auf dem Silbertablett serviert. Damit ist es ein Leichtes, Künstliche Intelligenz (KI) für ihre Zwecke zu trainieren. Nehmen wir ein ganz einfaches Beispiel: Ich füttere die KI mit ein paar E-Mails des CEO und ein paar Prompts später habe ich einen Text, der genau nach dem Chef klingt: Anrede, Tonalität und Schreibstil passen, und die Mail wirkt absolut glaubwürdig. Und genau diese vermeintliche Echtheit setzt die üblichen Prozesse und Regeln außer Kraft. Mit GPT Varianten wie FraudGPT oder WormGPT können sich Kriminelle ihre eigenen Betrugs-Assistenten schaffen.

Und was ist mit Voice Cloning & Co.?

Alby: Damit erreichen wir eine neue Evolutionsstufe. Vor ein paar Jahren war Voice Cloning noch etwas für absolute Spezialisten und die Qualität oft fraglich. Heute gibt es das quasi auf Knopfdruck und „von der Stange" mit Hilfe von KI-Tools, die entweder frei verfügbar sind oder die man für ganz kleines Geld erwerben kann – und die täuschend echt an die Realität herankommen. Large-Language-Modelle können mittlerweile problemlos auf lokalen Rechnern bedient werden. Ihr Output lässt sich dann über eine API an ein Voice-Cloning-Tool übermitteln, so dass solche Betrugsversuche skalierbar werden. Das eröffnet auch Betrügern ganz neue Horizonte – die Hürden sind so niedrig wie noch nie, sie brauchen immer weniger Skills für wirklich gut gemachte Angriffe.



Kragh: Das Ausnutzen von künstlich erzeugten Stimmen und Bildern für die Vertrauensbildung ist ein mächtiges Werkzeug. Eine gut formulierte E-Mail ist eine Sache, aber wenn der falsche Chef plötzlich mit der echten Stimme spricht oder auch echt aussieht und im Zweifelsfall in seinem authentischen Büro zu sehen ist, dann ist das nochmals eine ganz neue Dimension, die in vielen Fällen auch bei geschulten Mitarbeitenden häufig alle Zweifel verschwinden lässt.

Das heißt, wir müssen jetzt mit einer Fake-President-Welle rechnen?

Kragh: Seit unserem ersten „Fake-President"-Fall vor sechs Jahren, bei dem nach unserer Einschätzung Audio Deepfakes zum Einsatz kamen und ein Mitarbeiter auf einen „falschen Chef" hereinfiel, haben wir nur vereinzelt ähnlich gelagerte Fälle gesehen – der große Sturm blieb bisher aus. Das könnte sich jetzt aber sukzessive drehen: Das World Economic Forum geht in seinem Global Cybersecurity Outlook 2025 von einer Verdreifachung beim globalen Handel mit Deepfake-Tools im Darknet zwischen Anfang 2023 und 2024 aus.

Alby: Die eigenen Mitarbeitenden sind in mehrfacher Hinsicht attraktiv für Betrüger. Social Engineers ziehen ihre Informationen aus einer Vielzahl an Quellen. Teilweise dringen sie in Intranets ein und sammeln dort Informationen, aber auch soziale Netzwerke spielen eine immer größere Rolle. Mit sogenannten „Vishing"-Anrufen an verschiedenen Stellen des Unternehmens kommen die Kriminellen oft an vertrauliche Informationen. Bei einer großen Hotel- und Casinokette machte eine Gruppe von Kriminellen einen Mitarbeiter auf LinkedIn aus und kontaktierte anschließend das IT Help Desk. Binnen 10 Minuten hatten sie genügend Informationen gesammelt, um ins System einzudringen. Mit gut gemachten Audio Deepfakes dürfte dies in Zukunft sogar noch leichter werden, denn mit dem Manager oder der Führungskraft können Mitarbeitende ja offen über den Stand vertraulicher Projekte oder Geschäftsgeheimnisse sprechen und so unwissentlich Schützenhilfe leisten. Darüber hinaus sind sowohl bei Social Engineering als auch bei Betrugsfällen häufig auch interne (Mit-)Täter involviert. Sie können zum Beispiel gezielt Stimmmaterial, Dokumentenvorlagen für Rechnungen und E-Mails sowie Informationen zu Abläufen, Kontrollsystemen oder Ansprechpartnern liefern.

Wie können Mitarbeitende denn Deepfakes überhaupt erkennen?

Kragh: Das ist leider schon nicht mehr ganz so leicht, dennoch gibt es einige Anzeichen. Sie sollten beispielsweise auf eine eher unnatürliche Betonung achten, die Sprachmelodie, aber auch wie authentisch Bewegungen oder Blinzeln wirken. Auch schlechte Audio- oder Videoqualität, unerklärliche Nebengeräusche oder Veränderungen von Licht und Hautton könnten wichtige Hinweise sein. Ebenso eine schlechte Lippensynchronisation zum Gesagten. Sie können ihr Gegenüber auch einfach bitten, sich mit dem Finger zur Nase zu fassen.

Alby: Das ist schon mal ein guter Ansatz, aber ich würde mich nicht darauf verlassen. Ich gehe davon aus, dass wir in den kommenden Monaten Deepfakes sehen werden, bei denen das schon alles nicht mehr gilt. Deshalb ist es sinnvoll, sich intern Gedanken zu machen, wie man Kontrollmechanismen installieren kann. Denn die Kriminellen schlafen nicht, sie arbeiten quasi Tag und Nacht an den verbleibenden Defiziten und beherzigen solche „Erkennungs-Tipps" als erstes. Das ist ihr Input für die nächste Evolutionsstufe. Das wird definitiv ein Katz-und Maus-Spiel werden.

Was können Unternehmen also konkret tun, um sich zu schützen?

Kragh: Wie bei jeder Schwachstelle ist das immer eine Art Wettlauf. Erst entwickeln die Betrüger – und die sind sehr kreativ – neue Maschen und Varianten und die Unternehmen ziehen mit zeitlichem Verzug entsprechende Abwehrmechanismen nach. Unternehmen hinken also meistens einen Schritt hinterher. Umso wichtiger ist die Sensibilisierung der Mitarbeitenden durch regelmäßige Trainings und Schulungen. Oder regelmäßige simulierte Betrugs-Mails aus der eigenen IT-Sicherheit als Test. Auch die Verpflichtung des CEOs, keine Überweisungen in Videocalls anzuweisen oder eine Losung für gewisse Transaktionen kann eine geeignete Schutzvorkehrung sein. Wichtig ist nur, dass sich am Ende alle daran halten. Und der allerwichtigste Punkt ist Offenheit: Eine gute Fehler- und eine offene Unternehmenskultur sind die wichtigsten Hebel gegen kriminelle Machenschaften. Das hat ein kürzlich vereitelter „Fake-President"-Fall eindrucksvoll bewiesen, bei dem eine kluge Rückfrage des Mitarbeitenden (siehe Fallbeispiele Seite 15) das ganze Konstrukt einstürzen ließ wie ein Kartenhaus.

Marie-Christine Kragh
Global Head of Fidelity
bei Allianz Trade

Tom Alby
Chief Digital
Transformation Officer
bei Allianz Trade

Alby: Neue Technologien verändern Prozesse und Rahmenbedingungen und zwar aktuell in einem rasanten Tempo. Diese sollte man mitdenken, um zumindest einigermaßen auf Augenhöhe zu bleiben – was ehrlich gesagt schwer sein wird. Covid war für plötzliche Prozessänderungen ein gutes Beispiel: Plötzlich war die ganze Belegschaft im Homeoffice statt im Büro – wie verändern sich dadurch Prozesse und Sicherheitsrisiken? Ähnliches gilt auch für KI: Diese Tools haben viele Vorteile, aber der richtige Umgang will gelernt sen. Es ist zum Beispiel sicher keine gute Idee, interne Informationen bei ChatGPT einzugeben, um bei einer Mail an den Chef Zeit zu sparen, denn der Algorithmus nutzt auch diese Informationen, um zu lernen. Deshalb sollten Unternehmen klare Regeln und verbindliche Richtlinien definieren, was erlaubt ist und was nicht. So lassen sich schon einige Sicherheitslücken schließen. Regelmäßige Stresstests, KI-Detection-Tools, Multifaktor-Authentifizierung sind ebenfalls Optionen, Risiken zumindest zu minimieren. Für die Zukunft könnte auch Fingerprinting, also die Authentifizierung eines E-Mail-Absenders per Fingerabdruck eine Lösung sein, um eine weitere Sicherheitsstufe zu implementieren. Aber die Kriminellen werden genau diese Punkte berücksichtigen und Lösungen finden, sie zu umgehen. Und: Die Schwachstelle Mensch bleibt.

Kragh: Zumal externe Täter wie beim Social Engineering ja nur eine Seite der Medaille sind: Die Innentäter am Schreibtisch nebenan richten weiterhin die meisten Schäden an. Auch diese unbequeme Wahrheit bleibt.

> „Es wird definitiv ein Katz-und-Maus-Spiel mit den Betrügern werden."
>
> **Tom Alby**

Auffällig unauffällig: Der nette Kollege schlägt plötzlich zu

Innentäter, also Mitarbeitende, die das eigene Unternehmen schädigen, sind 2025 für die meisten und größten Schäden verantwortlich. Fazit: So gut und wichtig Vertrauen für die Unternehmenskultur ist – es sollte Grenzen haben. Mit wirksamen Kontrollsystemen und sauberen Prozessen lassen sich Tatgelegenheiten minimieren.

Es ist für Unternehmen eine unbequeme Wahrheit: Die meisten Schäden richten immer noch die eigenen Mitarbeitenden an. Sei es eine langjährige Chef-Sekretärin, die mit gefälschten Rechnungen für Event-Dienstleistungen einen Designer-Kleiderschrank finanzierte, oder der Prokurist eines Sicherheitsunternehmens, der insgesamt 26 Millionen Euro an Firmengeldern abzweigte, um sogar die Gartenwege seiner Villa zu beheizen – sie haben meist ein ähnliches Profil: Sie sind seit mindestens 10 Jahren im Unternehmen, auffällig unauffällig und beliebt, genießen das volle Vertrauen ihrer Chefs.

Laut Prof. Dr. Hendrik Schneider (siehe Interview Seite 18) sind Wirtschaftsstraftäter häufig „Latecomer to crime", also Spätzünder bei der kriminellen Karriere – auch, weil eine bis dato weiße Weste für die Weiße-Kragen-Täter eine Grundvoraussetzung ist. „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", sagt Prof. Dr. Schneider.

Zuletzt haben die externen Täter bei der Schadenshöhe merklich aufgeholt und laut Allianz Schadensstatistik 2024 sogar erstmals überholt. 2025 hatten allerdings die Täter am Schreibtisch nebenan wieder die Nase vorn bei den angerichteten Schäden.

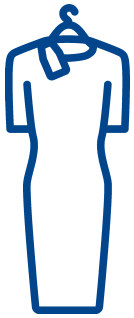
Die Innentäter dürften sich dank KI-Tools ebenfalls weiter „upskillen". Zudem bleiben ihre „Werke" häufig wesentlich länger unentdeckt und kommen teilweise erst nach vielen Jahren ans Tageslicht.

Bei Motiven und Tätertypen ist die Mischung weiterhin bunt: Vom LKW-Fahrer, der sich aufgrund von finanziellen Problemen mit Kloschüsseln und Durchlauferhitzern seines Arbeitgebers einen lukrativen Nebenverdienst verschafft hat, über die Sekretärin, die ihre 200 Katzen mit Firmengeld finanzierte, bis hin zum Buchhalter, der systematisch Gelder auf stillgelegten Konten veruntreute und sich damit Luxusimmobilie und Sportwagen leistete (alles echte Fälle!), ist alles dabei.

Mitarbeitende sind mit ihrem Insiderwissen in der besten Position, Schwachstellen zu entdecken und – je nach persönlichem Profil – wahlweise zu melden, zu schließen oder auszunutzen. Gerade deshalb sind gute Kontroll- und Compliance-Systeme sowie Whistleblowing-Kanäle enorm wichtig: Sie minimieren die Tatgelegenheiten. Die Unternehmens- und Fehlerkultur sowie der „Tone from the Top" spielen ebenfalls eine wichtige Rolle. Autokratische oder sehr hierarchische Kulturen begünstigen ein „Ausbrechen" und sind häufig wesentlich anfälliger für Wirtschaftskriminalität. Wie so oft: Die Balance macht's.

Vertraute Stimmen und kontrollsichere KI-Fälschungen

KI sorgt für Effizienzsprünge – und auch für ein Upskilling von Betrügern. Das zeigen auch die aktuellen Beispielfälle, die die ganze Bandbreite von krimineller Energie abbilden. War der richtige Ton in E-Mails vor Jahren noch eine ausgefeilte und aufwändige Kunst, spuckt die KI heute praktisch im Sekundentakt authentisch wirkende Texte und perfekt gefälschte Rechnungen aus, imitiert vertraute Stimmen – oder den Chef in der Videokonferenz. Mit jeder Evolutionsstufe steigt die Glaubwürdigkeit und damit die Erfolgsaussichten. Doch auch Innentäter sind gewieft – und bleiben viel länger unentdeckt.



Im Ballkleid meines Arbeitgebers

In einem Unternehmen, das auf den Verleih von Designerkleidern und Accessoires spezialisiert war, verschwanden Designer-Roben, passende Schuhe sowie diverse Handtaschen und Accessoires im Wert von 85.000 EUR. Bemerkt wurde das Fehlen erst, als eine Kundin ein sehr ausgefallenes Ballkleid zum Verleih bestellte, das aber trotz intensiver Suche nirgends auffindbar war. Bei der folgenden Inventur stellte sich heraus, dass es nicht das einzige Kleid war, das spurlos verschwunden war. Insgesamt fehlten 13 Kleider und 10 Paar Designer-Schuhe – allesamt von zwei bestimmten Designermarken, in Kleidergröße 38 und Schuhgröße 39. Die Manager installierten daraufhin versteckte Überwachungskameras und ertappten die Täterin so in flagranti. Die Mitarbeitende hatte eine Vorliebe für Luxuskleider – die allerdings weit über ihrem finanziellen Spielraum lagen. So hatte sie sich den Luxus-Kleiderschrank aus dem Lager des Arbeitgebers aufgestockt. Ein Teil der Beute konnte in ihrer Wohnung sichergestellt werden.

Shop im Shop-Konzept

Ein in einem Gartencenter in Thüringen für den Online-Shop zuständige Mitarbeitende implementierte ein „Shop im Shop"-Konzept: Er verkaufte Werkzeuge und Gartenzubehör des Centers – allerdings unter eigenem Namen, zu Schnäppchenpreisen und ohne sie zuvor rechtmäßig erworben zu haben. Der Shop florierte, denn er kannte alle Abläufe genau, wusste, wann er allein war und die Ware unbemerkt aus dem Lager des Gartencenters entwenden konnte. Da er die Ware direkt aus dem Büro versandte, musste er sie gar nicht erst aus dem Gebäude schmuggeln. Sein Doppel-Shop Konzept ging über ein Jahr auf – dann kam der Schock: Ein Kollege bestellte zufällig online eine der äußerst günstig angebotenen Akku-Heckenscheren und stellte fest, dass sein Kollege der Verkäufer war. Der Schaden belief sich auf insgesamt 180.000 EUR.

Die vertraute Stimme und die wiederbeschaffte Million

Ein Mitarbeitender eines Maschinenbau-Unternehmens in Süddeutschland wurde vom vermeintlichen CFO der Muttergesellschaft zunächst per „iMessage" kontaktiert. Das Vorgehen zunächst ein klassischer „CEO Fraud": Es gehe um einen vertraulichen Unternehmenskauf, bei dem er die Unterstützung des besonders vertrauensvollen Mitarbeitenden benötige. Sie unterhielten sich auch noch kurz über den Post des CFOs im Intranet, der sich aus dem Skiurlaub zurückgemeldet hatte. In den Tagen darauf folgten mehrere E-Mails von einem angeblich mit dem Erwerb betrauten Rechtsanwalt einer internationalen Kanzlei sowie mehrere Audio-Anrufe des angeblichen CFO, dessen Stimme echt klang. Innerhalb von 5 Tagen veranlasste der Mitarbeitende mehrere Zahlungen in einer Gesamthöhe von 1,9 Millionen EUR. Der CFO war so begeistert, dass er dem Mitarbeitenden sogar einen besonders gut dotierten Job in der Holding in Aussicht stellte.

Nachdem sich kurz darauf herausstellte, dass nicht der CFO, sondern Betrüger die Anweisungen veranlasst hatten, beauftragte das Unternehmen

umgehend einen Spezialisten mit der Rückholung der überwiesenen Gelder – zumindest mit einem Teilerfolg: Knapp 1 Mio. EUR konnten zurückgeholt werden, den Rest erstattete Allianz Trade.

In einem ähnlich gelagerten Fall – Erstkontakt per Whatsapp mit korrektem Profilbild des CEO und anschließender Korrespondenz mit einem Anwalt – überwies der Mitarbeitende zwei Zahlungen in Höhe von 850.000 EUR auf ausländische Konten. Bei der dritten Tranche wurde er dann doch misstrauisch und der Betrug wurde aufgedeckt. Durch das schnelle Handeln des direkt beauftragten Rückholungsspezialisten konnte immerhin die zweite Zahlung in Höhe von 400.000 EUR auf dem Empfängerbankkonto beschlagnahmt werden.

Chef-Avatare und rettende Rückfragen

Mit einem täuschen echten Video-Deepfake erbeutete eine international agierende Bande von Kriminellen im Frühjahr 2025 in den Niederlanden bei einem „CEO Fraud" rund 8,7 Mio. EUR. In dem raffinierten Täuschungsmanöver schlüpften sie in die KI-generierten Avatare des Geschäftsführers und eines Anwalts der alleinigen Gesellschafterin des niederländischen Unternehmens. Bild und Ton waren so gut gemacht, dass sowohl Aussehen als auch Stimme überzeugten: Der in der Videokonferenz mit den Zahlungen betraute Mitarbeitende führte insgesamt 17 Banktransaktionen durch. Neben Deepfake-Videos kamen gefälschte Dokumente und Sitzungsprotokolle zum Einsatz.

Die finanziellen Transfers führten zu Konten in Bulgarien, der Slowakei und Österreich. Der entstandene Schaden lag bei etwa 8,7 Millionen EUR. 1,5 Mio. EUR konnten durch die enge Zusammenarbeit von Banken und internationalen Behörden in Österreich noch sichergestellt werden – der Rest blieb verschwunden.

Schon 2024 hatte ein Video Deepfake Fall in Großbritannien für Aufsehen gesorgt: Nach einer Videokonferenz mit dem geklonten Chef überwies ein Mitarbeitender über 20 Mio. EUR in 15 Tranchen – ohne Rückfrage. Dabei hätte genau dieses gesunde Misstrauen das Kartenhaus sofort zum Einfallen gebracht. Bei den anschließenden Ermittlungen stellte sich heraus, dass es sich höchstwahrscheinlich um vorbereitete Videos gehandelt haben dürfte, die abgespielt wurden.

Wie das verhindert werden könnte, zeigt der ebenfalls 2024 gescheiterte Fake President Betrugsversuch bei einem internationalen Automobilkonzern. Geistesgegenwärtig stellt der Manager eine „goldene" Rückfrage an den vermeintlichen CEO, der ihn bittet, für eine angeblich geheime Firmenübernahme mehrere Millionen Euro zu überweisen: „Welches Buch haben Sie mir kürzlich nochmal empfohlen?" Der Betrüger ist ertappt und hat keine Ahnung von der Buchempfehlung – Schachmatt durch eine einzige Frage.

Von großen Namen geblendet – halber Solarpark verschwunden

Ein Lieferant für Solaranlagenteile in Nordrhein-Westfalen erhielt von einem sehr bekannten Energieunternehmen eine Anfrage für dessen geplanten Ausbau der Solaranlagenkapazitäten. Nach erfolgter Abgabe eines Angebotes bestellte der Energieversorger in der Folge große Mengen an Teilen für Solaranlagen, darunter Solarpaneele, Wechselrichter und Montagesysteme. Er teilte mit, das die Teile an verschiedene Lageradressen geliefert werden sollten, die angeblich zum Unternehmen gehörten.

Der Lieferant – hocherfreut über die großen Bestellungen – begann, die Ware zu versenden, ohne einen Verdacht zu schöpfen. Bei Fälligkeit der Rechnungen ist keine der bekannten Kontaktpersonen mehr erreichbar und es stellt sich heraus, dass das echte Unternehmen mit dem Auftrag gar nichts zu tun hatte. Die Lieferadressen waren lediglich kurzfristig angemietete Lagerhallen, die inzwischen längst verlassen waren. Die Betrüger hatten die Ware schnell weiterverkauft und waren anschließend spurlos verschwunden. Zurück blieb ein Schaden von 2,5 Mio. EUR.

Die perfekt gefälschte KI-Rechnung

Ein Großhändler in Hessen erhielt eine Rechnung von einem langjährigen Lieferanten für Waren im Wert von knapp 200.000 EUR. Kurz vor dem Fälligkeitsdatum erhielt die Buchhaltung des Großhändlers eine E-Mail mit der Bitte, die Zahlung auf ein geändertes Bankkonto zu leisten. Eine der Mail beigefügte Rechnung bestätigte die neue Bankverbindung. Der Großhändler leistete die Zahlung ohne weitere Rückfragen. Nach einiger Zeit flatterte allerdings eine Mahnung ins Haus. Bei der Überprüfung stellte sich heraus, dass unbekannte Dritte sich Zugang zur IT des Lieferanten verschafft hatten, die ursprüngliche Rechnung verändert und die Kommunikation im Namen des Lieferanten veranlasst hatten. Die Fälschung sah so täuschend echt aus, dass sie nicht mal bei tatsächlich erfolgten Routinekontrollen auffiel. Der Versuch, den überwiesenen Betrag zurückzuholen, blieb erfolglos. Die Betrüger hatten das Geld längst abgezogen.

Männlich, etwa 45, Chef-Finanzer sucht … Lücken im Kontrollsystem

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.

Sie schlagen zwar seltener zu, aber dann „in die Vollen" mit sehr großen Schäden: Sie kennen alle Lücken in den Kontrollsystemen und besitzen durch die langjährige Zugehörigkeit ein entsprechendes Vertrauen von Kollegen und Chefs, so dass sie oft über einen längeren Zeitraum unentdeckt agieren können.

Dabei hilft ihnen meist auch ihr freundliches und respektvolles Auftreten – sie sind oft auffällig unauffällig und geraten bei Verdachtsmomenten selten sofort in den Fokus.

Die typischen Täter

Bei den Täterinnen und Tätern, die ihr Unternehmen betrügen, sind praktisch alle Geschlechter, Altersgruppen und Hierarchieebenen vertreten. Männliche Täter dominieren weiterhin – bei Frequenz und Schadenshöhe zeigen sich in der Allianz Trade Schadensstatistik jedoch zahlreiche Unterschiede.

Jung, unerfahren, kriminell sucht … das schnelle Geld

Junge, unerfahrene Mitarbeiter:innen mit kurzer Betriebszugehörigkeit, niedrigerem Bildungsstand und einer niedrigeren Position in der Hierarchie ohne Führungsverantwortung schlagen mit wesentlich höherer Frequenz zu; die Schadenhöhe ist in den meisten Fällen allerdings geringer – auch, weil sie schneller entdeckt werden.

Im Schnitt sind die Frequenztäter zwischen 35 und Mitte 40 Jahre alt. Häufigste Delikte der Frequenztäter sind einfacher Diebstahl, Unterschlagung oder Untreue.

Quelle: Allianz Trade Schadensstatistik, Studien Wirtschaftskriminalität von KPMG, PwC, BKA Monitoringbericht Innentäter

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 Mitarbeitenden 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.

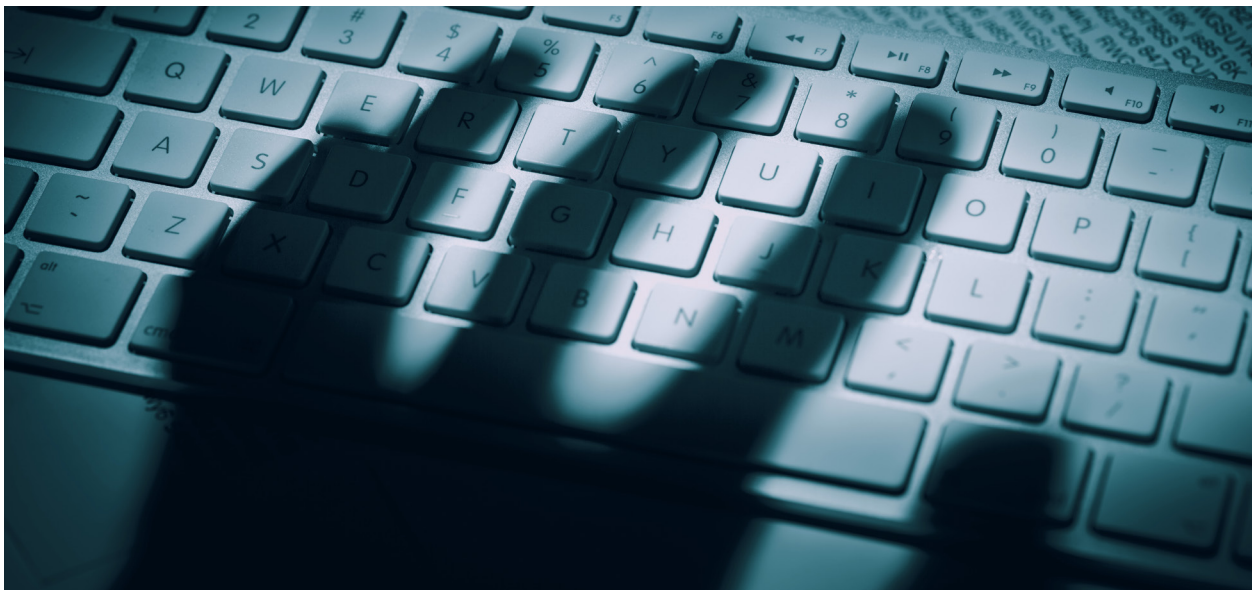
Wenn wir von „typischen Tätern" sprechen, sagen Alter, Position und Betriebszugehörigkeit nur wenig über die Täterpersönlichkeit aus. Gibt es da charakteristische Züge?

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.

Wie können sich Unternehmen vor schwarzen Schafen schützen?

Betrug und Untreue gehören weiterhin zu den „Top-Delikten" im Bereich Wirtschaftskriminalität. Die Anzahl der in der polizeilichen Kriminalstatistik[1] erfassten Fälle von Wirtschaftskriminalität bei Betrug stieg mit 116,7 % im Jahr 2024 im Vergleich zum Vorjahr deutlich - oft unter Beteiligung von Insidern. Auch in der Allianz Schadensstatistik haben Innentäter die meisten und größten Schäden angerichtet. 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.

[1] *Quelle: Bundeslagebild Wirtschaftskriminalität 2024*

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

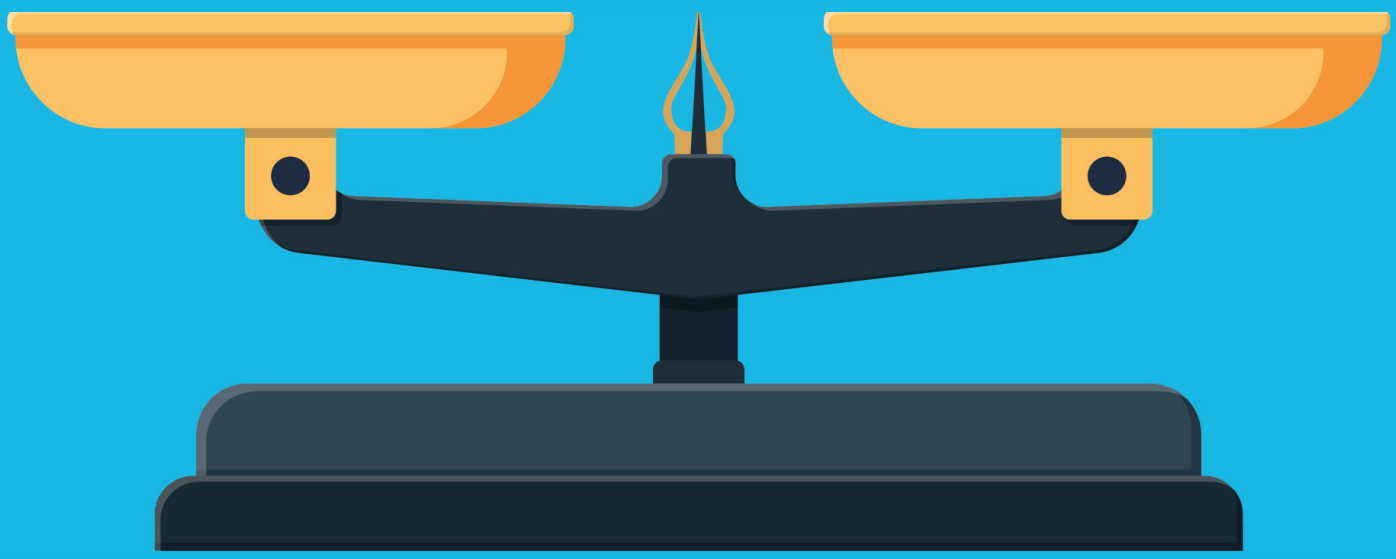
Präventives Risikomanagement und regelmäßige Prozessoptimierung: Überprüfung und Verbesserung von eventuellen Systemschwachstellen inkl. Zugangs- und Zugriffskontrollen

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. Unternehmensstruktur & Governance

- **a.** Sind die Arbeitsabläufe und -prozesse im Haus klar definiert und einsehbar?
- **b.** Gibt es ein Berichtswesen zu notwendigen und möglichen Sicherheitsvorkehrungen sowie Vorfällen und Wirksamkeit der Kontrollen?
- **c.** Gibt es definierte Eskalationswege bei Social-Engineering-Verdachtsmomenten?
- **d.** Werden Out-of-Band-Bestätigungen vorgeschrieben und dokumentiert?
- **e.** Gibt es eine offene Unternehmenskultur mit aktiver Meldung von Verdachtsmomenten?

2. Zahlungsverkehr

- **a.** Existiert ein technisch erzwungenes Vier-Augen-Prinzip für Vermögensverfügungen?
- **b.** Ist definiert, welche Zahlungen klärungsbedürftig sind?
- **c.** Werden Bankdaten nur nach Out-of-Band-Rückbestätigung geändert?
- **d.** Werden neue Bankverbindungen mit historischen Daten verglichen?
- **e.** Sind BEC-Schutzmaßnahmen implementiert?
- **f.** Gibt es Awareness-Programme zu Social Engineering und Deepfakes?

3. E-Mail-Sicherheit

- **a.** Werden E-Mail-Authentifizierungsprotokolle genutzt (SPF, DKIM, DMARC)??
- **b.** Nutzen Sie DMARC mit Policy ‚reject' und Monitoring?
- **c.** Gibt es einen Prozess zur Erkennung kompromittierter Konten (Identity-Protection)?
- **d.** Werden Schulungen zu modernen Phishing-Täuschungen angeboten (Deepfake-Audio/-Video)?

4. IT-Sicherheit

- **a.** Gibt es ein Sicherheitskonzept für das IT-System?
- **b.** Werden Phishing-resistente MFA (Passkeys, Hardware-Token) genutzt?
- **c.** Existiert ein Business-Continuity-Plan für kompromittierte Accounts?
- **d.** Erfolgt eine regelmäßige Prüfung auf Manipulationen an E-Mail-Konten?

5. Einkauf / Verkauf

- **a.** Sind Zuständigkeiten klar getrennt?
- **b.** Erfolgt eine unabhängige Prüfung der Inventarisierungsprozesse?
- **c.** Werden Managementberichte zu Retouren und Stornierungen erstellt?
- **d.** Gibt es eine Einkaufsrichtlinie und einen Code of Conduct?
- **e.** Wird Lieferantenkommunikation auf Deepfake-/ BEC-Indikatoren geprüft?

6. Personal / HR

- **a.** Werden auffällige Bewerbungsverläufe geprüft?
- **b.** Erfolgen vertiefte Checks bei Schlüsselpositionen?
- **c.** Werden alle Mitarbeitenden zur Geheimhaltung verpflichtet?
- **d.** Erfolgen Pflichtschulungen zu Phishing, Social Engineering und KI-Täuschungen?

7. Revision & Kontrollen

- **a.** Existiert eine interne Revision?
- **b.** Erfolgt eine regelmäßige Prüfungen aller Bereiche?
- **c.** Werden Remote-Office-Auswirkungen bewertet?
- **d.** Prüft die Revision Out-of-Band-Nachweise?
- **e.** Erfolgt ein Audit auf Kontoübernahme-Indikatoren?
- **f.** Werden BEC-Abwehrprozesse auf ihre Wirksamkeit geprüft?

8. Moderne Angriffsszenarien

- **a.** Gibt es Regeln für Zahlungsaufforderungen unter Zeitdruck (Fake-President / CEO-Fraud 2.0)?
- **b.** Erfolgen Zahlungsfreigaben per Video-/ Sprachanruf nur mit Rückversicherung?
- **c.** Gibt es eine Policy für Deepfake-Erkennung?
- **d.** Werden Warnsignale für ungewöhnliche Kommunikationsmuster erkannt?

Antje Wolters
Pressesprecherin

Allianz Trade Deutschland
Gasstraße 29
22761 Hamburg
Tel. +49 (0) 40 88 34-1033
Mobil +49 (0)160 899 27 72
E-Mail: Antje.Wolters@allianz-trade.com

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