Allianz

Allianz Trade

MEDIENMITTEILUNG

Alarmstufe KI: Schäden durch Fake-President-Betrug vervielfachen sich

- Wirtschaftskriminelle dank KI-Tools immer professioneller
- Schäden bei Unternehmen durch alle Social-Engineering-Betrugsmaschen steigen um 60 %
- Weiter in Mode: Schäden durch Fake-President-Betrug verdreifachen sich 2024 (+200 %) und steigen 2025 um weitere 81 % – trotz rückläufiger Fallzahlen
- Neuer Liebling: Bestellerbetrug (+61 %) löst Zahlungsbetrug vom Spitzenplatz ab, Schäden haben sich 2025 sogar mehr als verdoppelt (+139 %)
- Unterschätzte Gefahr: „Innentäter" richten weiterhin die meisten (60 %) und größten (65 %) Schäden an

Hamburg, 20. Januar 2026 – Künstliche Intelligenz (KI) spielt Wirtschaftskriminellen in die Hände: Sie werden immer professioneller, schlagen häufiger zu – und richten bei Unternehmen immer größere finanzielle Schäden an. Insbesondere bei den sogenannten „Social-Engineering-Betrugsmaschen"[1] spielt dies eine große Rolle, bei denen „Menschen-Hacker" Mitarbeitende mit psychologischen Tricks und unter der Vorspiegelung falscher Identitäten manipulieren und sie so zur Preisgabe von sensiblen Daten oder auch Überweisungen von Firmengeldern bewegen. Diese Fälle stiegen 2025 um insgesamt 60 %.

Die aktuelle Allianz Trade Schadensstatistik zeigt, dass sich die Schäden für Unternehmen durch Fake-President-Betrugsmaschen[2] 2024 verdreifacht haben (+200 %). 2025 sind sie um weitere 81 % angestiegen – trotz rückläufiger Fallzahlen (2024: -12 %; 2025: -13 %). Ein ähnliches Bild zeigt sich beim Bestellerbetrug[3], der 2025 ein Revival erlebt: Die Schäden haben sich im vergangenen Jahr mehr als verdoppelt (+139 %) und mit einem Zuwachs bei den Fallzahlen um 61 % hat der Bestellerbetrug den Zahlungsbetrug[4] vom Spitzenplatz als häufigste Social-Engineering-Betrugsmasche abgelöst.

Katz-und-Maus-Spiel: Kriminelle verschaffen sich Vorsprung, Unternehmen ziehen nach
„Es ist ein Katz-und-Maus-Spiel: Die Kriminellen perfektionieren ihre Betrugsmaschen mittel KI und die Unternehmen versuchen, mit ihren Schutzmechanismen Schritt zu halten", sagt Marie-Christine Kragh, Globale Leiterin Vertrauensschadenversicherung bei Allianz Trade. „Das wird allerdings immer schwerer: E-Mails sind inzwischen makellos und Deepfakes täuschend echt. Das Ausnutzen von künstlich erzeugten Stimmen und Bildern für die Vertrauensbildung ist ein mächtiges Werkzeug, das in vielen Fällen auch bei geschulten Mitarbeitenden alle Zweifel verschwinden lässt. Aber auch maßgeschneiderte E-Mails mit dem richtigen Ton und internen Details schaffen eine sehr hohe Glaubwürdigkeit und steigern damit die Erfolgschancen erheblich. Das zeigt auch unsere Statistik: 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 beim ersten Aufkommen der Betrugsmasche Anfang der 2010er Jahre.

---

[1] Als Social Engineering bezeichnet man Betrugsmaschen, bei denen Kriminelle („Menschen-Hacker") ihr Gegenüber mit Hilfe von psychologischen Tricks manipulieren und unter Vortäuschung falscher Identitäten und Tatsachen dazu bewegen, bestimmte, meist sensible Informationen (z.B. Zugangsdaten) preiszugeben oder Handlungen auszuführen (z.B. Überweisungen, Abänderung von Kontodaten oder Lieferadressen).

[2] Bei der „Fake-President"-Betrugsmasche geben sich die Täter als vermeintliche Chefs aus (die Masche ist auch als „CEO Fraud" bekannt) und weisen Mitarbeitende an, Geldsummen für vermeintliche Geschäftstransaktionen auf betrügerische Konten zu überweisen.

[3] Beim Bestellerbetrug (auch als Fake Identity bekannt) geben sich Betrüger als Kunde aus und leiten nach anschließend Warenströme an manipulierte Lieferadressen um.

[4] Beim Zahlungsbetrug (Payment Diversion) werden Zahlungsströme umgeleitet durch manipulierte Rechnungen oder Nachrichten mit angeblich geänderter Bankverbindung.

Schachmatt in zwei Zügen: Per Phishing ins System, per Social Engineering ans Geld
Dank gut gefüllten Regalen im Darknet müssen die Kriminellen selbst nicht mehr über fundierte Spezialkenntnisse verfügen.

„Kriminelle brauchen in vielen Fällen keine größeren IT- oder Coding-Kenntnisse", sagt Dirk Koch, Certified Ethical Hacker und Partner bei der Rechtsanwaltskanzlei ByteLaw. „Entsprechende Tools gibt es im Darknet quasi von der Stange und zu inzwischen vergleichsweise kleinen Preisen. Oft setzen die Kriminellen die Unternehmen in zwei Zügen schachmatt: Über extrem gut gemachte Phishing- und Vishing-Angriffe mit Hilfe von KI-Tools verschaffen sie sich zunächst Zugang zu den Systemen. Das öffnet für die dann folgenden Social-Engineering-Angriffe Tür und Tor."

Gefahr vom Schreibtisch nebenan: Interne Täter richten die größten Schäden an
Doch in den Unternehmen selbst lauern nicht unerhebliche Gefahren durch die sogenannten „Innentäter", also die eigenen Mitarbeitenden.

„Es ist eine unbequeme und oft unterschätzte Wahrheit für Unternehmen: Die eigenen Mitarbeitenden richten die meisten (60 %) und 2025 auch wieder die größten Schäden (65 %) an", sagt Marie-Christine Kragh, Globale Leiterin Vertrauensschadenversicherung bei Allianz Trade.

Kriminelle Kreativität: Geklaute Designer-Kleider und veruntreute Heckenscheren
2024 lagen die externen Täter bei den erbeuteten Summen zum bisher einzigen Mal gleichauf (je 50 %). 2025 hat sich dieser Trend jedoch wieder normalisiert: Innentäter richteten mit 65 % die größten Schäden an – auf externe Täter entfielen 35 % der gemeldeten Schäden. Die Innentäter erwiesen sich erneut als sehr kreativ, schmuggelten teure Designermode in den eigenen Kleiderschrank oder etablierten erfolgreiche „Shop-im-Shop"-Konzepte mit veruntreuten Heckenscheren (siehe Beispielfälle S. 15ff).

2-stufige Schutzmaßnahmen für Unternehmen: Technik flankiert von Organisation und Prozessen
Schutz gegen Social-Engineering-Angriffe bieten Unternehmen sowohl technische als auch organisatorische Maßnahmen.

„Technisch ist eine Phishing-resistente Multi-Faktor-Authentifizierung[5] ein Must-Have, ebenso wie verifizierte E-Mail-Signatur-Verfahren", sagt Koch. „Auch die Nutzung von KI-basierten Filtern sowie eine sogenannte ‚Zero-Trust-Architektur', bei der jeder einzelne Zugriff geprüft wird, hilft, Angriffe frühzeitig zu erkennen und Schäden zu begrenzen. Organisatorisch sollten Unternehmen ihre Prozesse für Zahlungsfreigaben laufend überprüfen, das Vier-Augen-Prinzip ebenso implementieren wie sogenannte ‚Out-of-Band-Bestätigungen', also Änderungen von Zahlungsdaten nur nach telefonischer Rückfrage über die bekannte, beim Erstkontakt hinterlegte Nummer. Und im Schadensfall sind die Reaktionszeiten entscheidend, um überhaupt eine Chance zu haben, einen Teil des Geldes wiederzubeschaffen."

Schwachstelle Mensch: „Menschen-Hacker" spielen gezielt mit Emotionen
Technisch aufzurüsten ist wichtig und bietet zumindest einen Basisschutz, der durch entsprechende Arbeitsabläufe und -prozesse bestmöglich flankiert werden kann. Dennoch reicht dies oft nicht aus.

„Der Mensch bleibt hier die Schwachstelle", sagt Kragh. „Social Engineering funktioniert, weil mit Emotionen gespielt wird – etwa in Form von Wertschätzung. Aber auch Druck oder das Heraufbeschwören einer vermeintlichen Krisensituation kann eine entscheidende Rolle spielen. Bei einem Trio aus Zeitdruck, dem Triggern von Emotionen und einer Aufforderung, vom Standard abzuweichen, sollten die Alarmglocken schrillen. Eine gute Fehler- und eine offene Unternehmenskultur gehören zu den wichtigsten Hebeln gegen kriminelle Machenschaften. Denn eine einzige Rückfrage beim Chef, ob der Auftrag wirklich echt ist, lässt das ganze Betrugs-Konstrukt einstürzen wie ein Kartenhaus."

[5] z.B. durch Hardware-Token oder Passkeys statt SMS-TAN

Die vollständige Allianz Trade Schadensstatistik inklusive zahlreicher Fallbeispiele finden Sie beigefügt und hier:
https://www.allianz-trade.de/content/dam/onemarketing/aztrade/allianz-trade_de/dokumente/ratgeber-schachmatt-durch-ki-wirtschaftskriminalitaet-und-strategien-zur-abwehr.pdf

---

Allianz Trade ist weltweiter Marktführer im Kreditversicherungsgeschäft und anerkannter Spezialist für Bürgschaften und Garantien, Inkasso sowie Schutz gegen Betrug oder politische Risiken. Allianz Trade verfügt über mehr als 100 Jahre Erfahrung und bietet seinen Kunden umfassende Finanzdienstleistungen an, um sie im Liquiditäts- und Forderungsmanagement zu unterstützen.

Über das unternehmenseigene Monitoring-System verfolgt und analysiert die Allianz Trade Gruppe täglich die Insolvenzentwicklung von mehr als 83 Millionen kleiner, mittlerer und multinationaler Unternehmen. Insgesamt umfassen die Expertenanalysen Märkte, auf die 92% des globalen Bruttoinlandsprodukts (BIP) entfallen.

Mit dieser Expertise macht die Allianz Trade Gruppe den Welthandel sicherer und gibt den weltweit über 70.000 Kunden das notwendige Vertrauen in ihre Geschäfte und deren Bezahlung. Als Tochtergesellschaft der Allianz und mit einem AA-Rating von Standard & Poor's ist die Holding von Allianz Trade mit Sitz in Paris im Schadensfall der finanzstarke Partner an der Seite seiner Kunden.

Das Unternehmen ist in über 40 Ländern vertreten und beschäftigt mehr als 5.800 Mitarbeiter weltweit. 2024 erwirtschaftete die Allianz Trade Gruppe einen konsolidierten Umsatz von EUR 3,8 Milliarden und versicherte weltweit Geschäftstransaktionen im Wert von EUR 1.400 Milliarden.

Weitere Informationen auf www.allianz-trade.de

Pressekontakt
Antje Wolters
Pressesprecherin
+49 (0) 40 / 88 34 – 1033
+49 (0) 160 / 899 27 72
Antje.wolters@allianz-trade.com

Social Media

LinkedIn Allianz Trade Deutschland
XING Allianz Trade Deutschland
YouTube Allianz Trade Deutschland
Twitter Allianz Trade

---

zukunftsgerichtete Aussage wider. Die tatsächlichen Ergebnisse, Entwicklungen oder Ereignisse können aufgrund verschiedener Faktoren von solchen zukunftsgerichteten Aussagen beträchtlich abweichen. Zu solchen Faktoren gehören u.a.: (i) die allgemeine konjunkturelle Lage einschließlich der branchenspezifischen Lage für das Kerngeschäft bzw. die Kernmärkte der Allianz-Gruppe, (ii) die Entwicklung der Finanzmärkte einschließlich der „Emerging Markets" einschließlich Marktvolatilität, Liquidität und Kreditereignisse, (iii) die Häufigkeit und das Ausmaß der versicherten Schadenereignisse einschließlich solcher, die sich aus Naturkatastrophen ergeben; daneben auch die Schadenkostenentwicklung, (iv) Stornoraten, (v) Ausmaß der Kreditausfälle, (vi) Zinsniveau, (vii) Wechselkursentwicklungen einschließlich des Wechselkurses EUR-USD, (viii) Entwicklung der Wettbewerbsintensität, (ix) gesetzliche und aufsichtsrechtliche Änderungen einschließlich solcher bezüglich der Währungskonvergenz und der Europäischen Währungsunion, (x) Änderungen der Geldpolitik der Zentralbanken bzw. ausländischer Regierungen, (xi) Auswirkungen von Akquisitionen, einschließlich der damit verbundenen Integrationsthemen, (xii) Umstrukturierungsmaßnahmen, sowie (xiii) allgemeine Wettbewerbsfaktoren jeweils in einem örtlichen, regionalen, nationalen oder internationalen Rahmen. Die Eintrittswahrscheinlichkeit vieler dieser Faktoren kann durch Terroranschläge und deren Folgen noch weiter steigen. Das Unternehmen übernimmt keine Verpflichtung, zukunftsgerichtete Aussagen zu aktualisieren.