Allianz

Allianz Trade

MEDIENMITTEILUNG

Allianz Trade Schadensstatistik: Fake-President-Betrugsmasche weiter „en vogue" – auch dank KI

- Künstlich intelligent: Wirtschaftskriminelle professionalisieren ihre Betrugsmaschen mit KI-Tools noch weiter, Deepfakes stellen bei „Social-Engineering-Betrug" große Gefahr dar
- Unbequeme Wahrheit: Innentäter richteten 2023[1] in Deutschland weiterhin die meisten und größten Schäden an: 55 % der Fälle und 76 % des Schadenvolumens gingen auf ihr Konto, 2024 könnte sich das Blatt allerdings wenden
- Falsche Chefs weiter in Mode: Fallzahlen bei Fake President sind 2023 um knapp ein Drittel (+31 %) gestiegen, Schadenvolumen bei Unternehmen hat sich allerdings halbiert (-55 %)
- Trend 2024: Schadenvolumen bei Unternehmen durch Fake President dürfte 2024 deutlich, schätzungsweise[2] um über 50 % steigen, bei gleichbleibenden Fallzahlen

Hamburg, 12. November 2024 – Wirtschaftskriminelle schlagen immer häufiger zu und richten immer größere Schäden an. Sie werden – auch dank Künstlicher Intelligenz (KI) – immer professioneller. Insbesondere das sogenannte „Social Engineering", also Betrugsmaschen, bei denen die Täter Menschen manipulieren, erfreut sich bei Kriminellen immer größerer Beliebtheit. Allerdings richten weiterhin die Innentäter, also die eigenen Mitarbeitenden, die meisten Schäden an.

„Die unbequeme Wahrheit für Unternehmen bleibt: Die Schwachstelle ist der Mensch, und die eigenen Mitarbeitenden richten weiterhin die meisten und – zumindest bis 2023 – auch die größten Schäden an. 2024 könnte sich dieses Blatt bei der Höhe der Schäden erstmals wenden", sagt Marie-Christine Kragh, Globale Leiterin der Vertrauensschadenversicherung bei Allianz Trade.

2023 waren Innentäter für mehr als die Hälfte (55 %) aller bei Allianz Trade gemeldeten Schäden in Deutschland verantwortlich sowie – getrieben durch viele besonders große Schäden – für rund drei Viertel des gemeldeten Schadenvolumens (76 %). 2024 setzt sich bei den Fallzahlen dieser Trend bisher fort: Von Januar bis August 2024 begingen Innentäter rund 60 % der gemeldeten Fälle. Neu ist 2024 allerdings, dass die externen Täter bei der Höhe der Schäden im gleichen Zeitraum die Nase vorn hatten (61 %). Wobei sich erfahrungsgemäß für das Gesamtjahr noch deutliche Verschiebungen ergeben können, sowohl durch Großschäden als auch aufgrund der Tatsache, dass kriminelle Handlungen durch Innentäter meist erst wesentlich später entdeckt und gemeldet werden als Delikte durch externe Täter.

„Menschen-Hacker": Social Engineering boomt bei Wirtschaftskriminellen

Zu den externen Tätern zählen auch die „Social Engineers": Beim Zahlungs- und Bestellerbetrug leiten sie Zahlungs- und Warenströme um, und bei der Fake-President-Betrugsmasche geben sie sich als vermeintliche Chefs aus und weisen Mitarbeitende an, Geldsummen für vermeintliche Geschäftstransaktionen auf betrügerische Konten zu überweisen. Die Fallzahlen bei diesen Delikten stiegen 2023 um 17 % gegenüber dem Vorjahr und das Schadenvolumen um 19 %.

„Die Fake-President-Betrugsmasche ist nach dem überraschenden Revival vor zwei Jahren weiterhin in Mode", sagt Kragh, „Die Fallzahlen bei dieser Betrugsmasche sind 2023 nochmals um fast ein Drittel (+31 %) nach oben geschnellt."

Die bei den Unternehmen verursachten Schäden pro Fall sind 2023 allerdings deutlich gesunken. Im vergangenen Jahr hat sich das Schadenvolumen halbiert (-55 %). In den meisten Fällen lagen die Schadenssummen bei niedrigen bis mittleren sechsstelligen Summen.

Trend 2024: Falsche Chefs weiterhin „en vogue" mit Großschäden, KI bringt neue Evolutionsstufe

[1] Allianz Trade Schadensstatistik: Die Zahlen beziehen sich auf die bei Allianz Trade in Deutschland gemeldeten Fälle 2023
[2] Schätzung für das Gesamtjahr 2024 basierend auf der Allianz Trade Schadensstatistik von Januar-August 2024 in Deutschland

„Die falschen Chefs haben 2023 also deutlich öfter zugeschlagen, aber dabei weniger hohe Summen erbeutet", sagt Kragh. „In Sicherheit wiegen sollten sich Unternehmen allerdings nicht – im Gegenteil. In diesem Jahr rechnen wir mit einer weiterhin hohen, aber gleichbleibenden Anzahl an Fällen und vermehrt auch wieder Großschäden. Wir gehen davon aus, dass das Schadenvolumen bei Unternehmen 2024 um weit mehr als 50 % steigen wird. Das deutet darauf hin, dass die Betrüger dank KI-Tools ihre Masche weiter professionalisieren mit einer noch zielgerichteteren Ansprache von Mitarbeitenden und Unternehmen."

Die neue Technologie dürfte Wirtschaftskriminellen auch beim Zahlungsbetrug weiter in die Hände spielen. Die Höhe der Schäden durch Zahlungsbetrug ist 2023 im Vergleich zum Vorjahr um mehr als die Hälfte gestiegen (+59 %), vor allem getrieben durch Großschäden. Die gefälschten Rechnungen sind in vielen Fällen praktisch nicht von den Originalen zu unterscheiden.

Für das Gesamtjahr 2024 zeichnet sich bei den Großschäden beim Zahlungsbetrug nach Schätzungen von Allianz Trade auf Basis der Schadensstatistik von Januar bis August 2024 eine leichte Entspannung ab: Die Fallzahlen dürften zwar auf hohem Niveau bleiben, aber die durchschnittlichen Schäden dürften sich wieder etwas normalisieren und das Schadenvolumen 2024 insgesamt rückläufig sein (-25 %).

Gefahr durch Deepfakes: immer weniger Skills notwendig, Voice Cloning per Knopfdruck
Mit der rasanten Entwicklung bei KI-Tools dürften Deepfakes in Zukunft vermehrt eine Gefahr für Unternehmen darstellen.

„Vor ein paar Jahren war Voice Cloning noch etwas für absolute Spezialisten und die Qualität oft fraglich", sagt Tom Alby, Chief Digital Transformation Officer bei Allianz Trade in Deutschland, Österreich und der Schweiz. „Heute gibt es das dank KI-Tools quasi auf Knopfdruck ‚von der Stange'. 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."

Die Technologie ist bei Social Engineers allerdings nur Mittel zum Zweck: Sie soll die Echtheit des Chefs und des Auftrags unterstreichen. Die Manipulation durch Emotionen und Druck spielt eine ebenso große Rolle.

„Das Ausnutzen von künstlich erzeugten Stimmen und Bildern für die Vertrauensbildung ist ein mächtiges Werkzeug", sagt Kragh. „Eine gut formulierte E-Mail ist eine Sache, aber wenn der falsche Chef plötzlich auch noch mit der echten Stimme spricht oder auch echt aussieht und im Zweifelsfall in ‚seinem' Büro zu sehen ist, dann ist das nochmals eine ganz neue Dimension, die in vielen Fällen alle Zweifel verschwinden lässt. Mitarbeitenden kann man nicht einfach einen Sicherheits-Patch aufspielen und alles wird automatisiert abgewehrt. Die Sensibilisierung wird deshalb wichtiger denn je."

Katz- und Maus-Spiel: Wettlauf zwischen Evolutionsstufen der Kriminellen und Schutzmaßnahmen
Gut gemachte Deepfakes sind oft nur schwer zu identifizieren. Mitarbeitende sollten auf eine unnatürliche Betonung oder Sprachmelodie achten oder darauf, 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 zu Nase zu fassen.

„Ich gehe allerdings davon aus, dass wir in den kommenden Monaten Deepfakes sehen werden, bei denen das schon alles nicht mehr gilt", sagt Alby. „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."

„Wachsamkeit, kritisches Denken und eine gute, offene Unternehmenskultur sind allerdings die wichtigsten Faktoren", sagt Kragh. „Eine einzige Rückfrage kann das ganze Kartenhaus

zusammenstürzen lassen und die Täter entlarven. Auch die Verpflichtung des CEOs, keine Überweisungen in Videocalls anzuweisen oder eine Losung für gewisse Transaktionen können geeignete Schutzvorkehrungen sein."

Bei einem kürzlich bekannt gewordenen Fall hat ein Mitarbeiter eines Autokonzerns mit einer simplen Rückfrage einen Fake-President-Betrugsversuch vereitelt: Welches Buch der CEO ihm vergangene Woche empfohlen habe. Der falsche Chef hatte keine Ahnung.

Die vollständige Allianz Trade Analyse finden Sie beigefügt und hier:
https://www.allianz-trade.de/content/dam/onemarketing/aztrade/allianz-trade_de/dokumente/allianz-trade-schadensstatistik-wirtschaftskriminalitaet-ki-betrueger-de1.pdf

Die Pressemeldung von Allianz Commercial zu Cyber Risikotrends und Cyber Security Resilience finden Sie hier:
https://commercial.allianz.com/news-and-insights/news/cyber-risk-trends-2024/de.html

---

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 50 Ländern vertreten und beschäftigt mehr als 5.500 Mitarbeiter weltweit. 2023 erwirtschaftete die Allianz Trade Gruppe einen konsolidierten Umsatz von EUR 3,7 Milliarden und versicherte weltweit Geschäftstransaktionen im Wert von EUR 1.131 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

Hinweis bezüglich zukunftsgerichteter Aussagen

Die in dieser Meldung enthaltenen Informationen können Aussagen über zukünftige Erwartungen und andere zukunftsgerichtete Aussagen enthalten, die auf aktuellen Einschätzungen und Annahmen der Geschäftsführung basieren, und bekannte und unbekannte Risiken sowie Unsicherheiten beinhalten, aufgrund derer die tatsächlichen Ergebnisse, Entwicklungen oder Ereignisse von den hier gemachten Aussagen wesentlich abweichen können. Neben zukunftsgerichteten Aussagen im jeweiligen Kontext spiegelt die Verwendung von Wörtern wie „kann", „wird", „sollte", „erwartet", „plant", „beabsichtigt", „glaubt", „schätzt", „prognostiziert", „potenziell" oder „weiterhin" ebenfalls eine 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.