So steckt generative KI neue Fronten in der Cybersicherheit ab

Veröffentlicht am 25. März 2024

Mobeen Tahir
Director, Macroeconomics and Thematic Research

Die wichtigsten Erkenntnisse

- Generative KI verschafft Angreifern neue Möglichkeiten und senkt die Hürde, als böswilliger Akteur aufzutreten
- Generative KI kann und muss auch zur Stärkung der Cyberabwehr eingesetzt werden
- Der Bedarf an Cybersicherheit ist größer als je zuvor – das eröffnet weiterhin Anlagechancen

2024 werden die Menschen in 55 Ländern – die 42 % der Weltbevölkerung repräsentieren – ihre politischen Vertreter wählen, darunter auch hochkarätige Wahlen für die US-Präsidentschaft und das Parlament der Europäischen Union[1]. Diese Ereignisse locken nicht nur Milliarden von Menschen zur Stimmabgabe, sondern auch böswillige Akteure an. Mit den Tools der generativen künstlichen Intelligenz (KI), die ihnen zur Verfügung stehen, versuchen sie, den Wahlprozess direkt zu sabotieren, indem sie Systeme hacken oder die öffentliche Meinung durch Fehlinformationen oder Deepfakes beeinflussen – ihre Möglichkeiten sind größer als je zuvor.

So kann generative KI Angreifern helfen

In der Vergangenheit reichte eine grundlegende Schulung in Cybersicherheit aus, um Phishing-Angriffe zu erkennen und abzuwehren. Schlechte Grammatik, verdächtige Domains und fragwürdige Links waren im Allgemeinen leicht zu entdecken. Allerdings können generative KI-Tools wie WormGPT[2], die auf Malware-bezogene Daten trainiert und speziell für kriminelle Aktivitäten entwickelt wurden, nicht nur die leicht zu entdeckenden verräterischen Elemente in Phishing-E-Mails beseitigen, sondern auch die Hürde für das Handeln als böswilliger Akteur senken.

Generative KI kann auch polymorphen Malware-Code unterstützen, eine Art von Programm, das lernt und sich weiterentwickelt und nach einem Fehlversuch automatisch intelligenter wird. Das heißt, wenn das Ziel seine Sicherheitssoftware nicht aktualisiert, kommt der Malware-Code stärker zurück, um jegliche Sicherheitslücken im System auszunutzen[3].

Durch generative KI verbessert sich auch die Qualität von Deepfakes. Nach Angaben des Weltwirtschaftsforums wurden zwischen dem 9. Dezember 2023 und dem 8. Januar 2024 mehr als 100 Deepfake-Videoanzeigen des britischen Premierministers Rishi Sunak auf Meta identifiziert, von denen viele emotionale Reaktionen wie „die Menschen sind empört“ hervorriefen[4].

Generative KI kann auch zum Identitätsdiebstahl genutzt werden. Wenn ein Opfer tatsächlich getäuscht wird und seine sensiblen personenbezogenen Daten preisgibt, können Dokumente wie Pässe und Führerscheine gefälscht werden.

So kann generative KI Verteidigern helfen

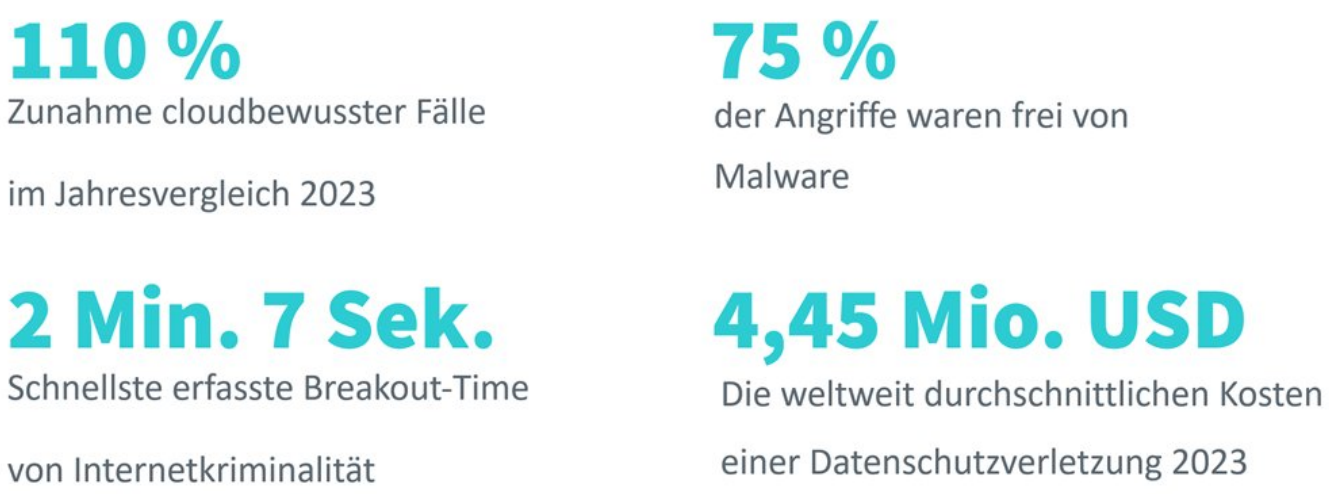
Es ist unerlässlich, dass generative KI auch zur Abwehr von immer ausgeklügelteren Angriffen eingesetzt wird. Beispielsweise kann generative KI dazu beitragen, fortschrittlichere Trainingsmodule zu entwickeln, mit denen sich Nutzer besser vor raffinierten Phishing-Angriffen schützen können.

Generative KI kann auch dazu verwendet werden, große Datenmengen zu analysieren, um Muster, Trends und Anomalien zu erkennen, die auf Schwachstellen im System hinweisen und Cybersecurity-Teams dabei helfen, die Lücken zu schließen, bevor ein polymorpher Malware-Code zurückkehrt.

Außerdem kann generative KI zur Automatisierung sich wiederholender Prozesse eingesetzt werden, um Aufgaben zu rationalisieren, die nicht nur mühsam, sondern auch anfällig für menschliche Fehler sind, wie etwa die Reaktion auf Vorfälle, die Suche nach Bedrohungen und die Malware-Analyse.

Cybersicherheit ist wichtiger denn je

Die nachstehenden Zahlen sind eine alarmierende Erinnerung daran, dass die Bedeutung der Cybersicherheit nicht hoch genug eingeschätzt werden kann.



Quellen: CrowdStrike, „2024 Global Threat Report“, IBM, Cost of a Data Breach Report 2023

Die meisten Menschen, die ein Smartphone oder einen Laptop besitzen, nutzen in der Regel Dutzende von cloudbasierten Softwareanwendungen. Kriminelle wissen um diese breitere Angriffsfläche und attackieren ihre Opfer zunehmend über die Cloud. Außerdem ist eine alarmierende Zunahme ausgeklügelter Angriffe ohne Malware zu verzeichnen: 75 % im Jahr 2023 nach noch 40 % im Jahr 2019[5]. Das deutet darauf hin, dass Angreifer zu schnelleren und effektiveren Methoden übergehen, um ihre Zielorganisationen zu infiltrieren. Dazu nutzen sie Mittel wie Social Engineering, anstatt immer darauf zu setzen, Malware in das System ihrer Opfer einzuschleusen. Das erinnert uns daran, dass bei Schulungen zur Cybersicherheit

nicht nur die Abwehr von Phishing-Angriffen vermittelt werden muss, sondern dass auch der Schutz vor physischen Täuschungen gewährleistet sein muss.

Die Breakout-Time ist der Zeitraum, den Cyberangreifer benötigen, um sich lateral innerhalb eines Unternehmens zu bewegen. Das bedeutet, dass sie Zugang zu anderen Nutzern erhalten, nachdem sie zunächst das erste Opfer kompromittiert haben. Die durchschnittliche Breakout-Time von Internetkriminalität fiel von 84 Minuten im Jahr 2022 auf 62 Minuten im Jahr 2023, wobei die schnellste erfasste Zeit gut 2 Minuten betrug[6]. Schließlich beliefen sich die durchschnittlichen Kosten von Datenschutzverletzungen für Unternehmen im Jahr 2023 auf 4,45 Millionen US-Dollar. Angreifer werden also immer schneller, setzen eine breite Palette von Tools ein und fügen ihren Opfern großen Schaden zu.

Glücklicherweise sind sich Unternehmen dieser Realität zunehmend bewusst. Laut IBM planen 84 % der Führungskräfte, im Jahr 2024 Cybersecurity-Lösungen auf Basis generativer KI gegenüber konventionellen Lösungen den Vorzug zu geben[7].

Die Bedeutung für Anleger

Cybersicherheit zählte zu den Top-Themen im Jahr 2023. Der WisdomTree Team8 Cybersecurity UCITS Index erzielte 2023 eine Rendite von 66,5 % und übertraf damit sogar den NASDAQ CTA Artificial Intelligence Index, der 55,9 % vorweisen konnte[8]. Natürlich lässt sich nicht vorhersagen, ob wir im Jahr 2024 wieder ähnliche Zahlen sehen werden. Wenn aber die Marktperformance für thematische Strategien eine Funktion starker positiver Strömungen in den zugrunde liegenden Technologien in Kombination mit einer breiteren Wertschätzung dieser Trends ist, gibt es sicherlich viele Gründe, auch weiterhin von generativer KI und ihren Auswirkungen auf die Cybersicherheit begeistert zu sein.

[1] Crowdstrike „2024 Global Threat Report“

[2] https://slashnext.com/blog/wormgpt-the-generative-ai-tool-cybercriminals-are-using-to-launch-business-email-compromise-attacks/

[3] https://www.sangfor.com/blog/cybersecurity/what-is-generative-ai-cybersecurity

[4] https://www.weforum.org/agenda/2024/02/4-ways-to-future-proof-against-deepfakes-in-2024-and-beyond/

[5] Crowdstrike „2024 Global Threat Report“

[6] Crowdstrike „2024 Global Threat Report“

[7] https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/ceo-generative-ai/cybersecurity

[8] Quelle: Bloomberg, auf der Grundlage von Netto-Gesamtrenditeindizes.

Important Risks Related to this Article

Wichtige Informationen

Im Europäischen Wirtschaffsraum („EWR“) herausgegebene Marketingkommunikation: Dieses Dokument wurde von WisdomTree Ireland Limited, einer von der Central Bank of Ireland zugelassenen und regulierten Gesellschaff, herausgegeben und genehmigt.

In Ländern außerhalb des EWR herausgegebene Marketingkommunikation: Dieses Dokument wurde von WisdomTree UK Limited, einer von der United Kingdom Financial Conduct Authority zugelassenen und regulierten Gesellschaff, herausgegeben und genehmigt.

WisdomTree Ireland Limited und WisdomTree UK Limited werden jeweils als „WisdomTree“ bezeichnet. Unsere Richtlinie über Interessenkonflikte und unser Verzeichnis sind auf Anfrage erhältlich.

Nur für professionelle Kunden. Wertsteigerungen in der Vergangenheit lassen keinen Schluss auf zukünffige Ergebnisse zu. Jegliche in diesem Dokument enthaltene historische Wertentwicklung kann u. U. auf Backtesting beruhen. Backtesting ist der Prozess, bei dem eine Anlagestrategie evaluiert wird, indem sie auf historische Daten angewandt wird, um zu simulieren, was die Wertentwicklung solch einer Strategie in der Vergangenheit gewesen wäre. Durch Backtesting erzielte Wertsteigerungen sind rein hypothetisch und werden in diesem Dokument einzig und allein zu Informationszwecken aufgeführt. Daten, die durch Backtesting gesammelt wurden, stellen keine tatsächlichen Wertsteigerungen dar und dürfen nicht als Indikator für tatsächliche oder zukünffige Wertsteigerungen angesehen werden. Der Wert jeder Anlage kann durch Wechselkursbewegungen beeinflusst werden. Anlageentscheidungen sollten auf den Angaben im entsprechenden Prospekt sowie auf unabhängiger Anlage-, Steuer- und Rechtsberatung basieren. Diese Produkte sind gegebenenfalls nicht in Ihrem Markt verfügbar oder für Sie geeignet. Der Inhalt dieses Dokuments stellt weder eine Anlageberatung noch ein Angebot zum Verkauf bzw. eine Aufforderung oder ein Angebot zum Kauf eines Produktes oder zum Tätigen einer Anlage dar.

Eine Anlage in börsengehandelte Produkte („ETPs“) ist abhängig von der Wertentwicklung des Basisindexes, abzüglich Kosten, aber es wird nicht erwartet, dass ihre Wertentwicklung genau mit der des Indexes übereinstimmt. ETPs unterliegen mehreren Risiken, darunter allgemeine Marktrisiken im Zusammenhang mit dem jeweiligen Basisindex, Kreditrisiken des Anbieters von Index-Swaps, die im ETP genutzt werden, Wechselkursrisiken, Zinsrisiken, Inflationsrisiken, Liquiditätsrisiken sowie rechtliche und regulatorische Risiken.

Bei den in diesem Dokument enthaltenen Informationen handelt es sich nicht um Werbung bzw. eine Maßnahme zum öffentlichen Angebot der Anteile in den USA oder einer zugehörigen Provinz bzw. einem zugehörigen Territorium der USA, wo weder die Emittenten noch deren Produkte zum Vertrieb zugelassen oder registriert sind und wo die Prospekte der Emittenten nicht bei einer Wertpapieraufsichtsbehörde oder sonstigen Aufsichtsbehörde eingereicht wurden, und dürfen unter keinen Umständen als solche verstanden werden. Weder dieses Dokument noch Informationen in diesem Dokument sollten in die USA mitgenommen, (direkt oder indirekt) übermittelt oder verteilt werden. Weder die Emittenten noch etwaige

von ihnen ausgegebenen Wertpapiere wurden oder werden gemäß dem United States Securities Act von 1933 oder dem Investment Company Act von 1940 registriert oder qualifizieren sich unter jeglichen anwendbaren bundesstaatlichen Wertpapiergesetzen.

Dieses Dokument kann unabhängige Marktkommentare enthalten, die von WisdomTree auf der Grundlage öffentlich zugänglicher Informationen erstellt wurden. Obwohl WisdomTree bestrebt ist, die Richtigkeit des Inhalts dieses Dokuments sicherzustellen, übernimmt WisdomTree keine Gewährleistung oder Garantie für seine Richtigkeit oder Genauigkeit. Die Drittanbieter, deren Dienste in Anspruch genommen werden, um die in diesem Dokument enthaltenen Informationen zu beziehen, übernehmen keine Gewährleistung oder Garantie jeglicher Art bezüglich dieser Daten. Dort, wo WisdomTree seine eigenen Ansichten in Bezug auf Produkte oder Marktaktivitäten äußert, können sich diese Auffassungen ändern. Weder WisdomTree, noch eines seiner verbundenen Unternehmen oder einer seiner jeweiligen leitenden Angestellten, Verwaltungsratsmitglieder, Partner oder Mitarbeiter übernimmt irgendeine Haffung für direkte Schäden oder Folgeschäden, die durch die Verwendung dieses Dokuments oder seines Inhalts entstehen.

Dieses Dokument kann zukunffsorientierte Aussagen enthalten, einschließlich Aussagen hinsichtlich unserer Einschätzung oder aktuellen Erwartungen im Hinblick auf die Wertentwicklung bestimmter Anlageklassen und/oder Sektoren. Zukunffsorientierte Aussagen unterliegen gewissen Risiken, Unsicherheiten und Annahmen. Es gibt keine Sicherheit, dass

diese Aussagen zutreffen, und die tatsächlichen Ergebnisse können von den erwarteten Ergebnissen abweichen. WisdomTree empfiehlt Ihnen deutlich, sich nicht in unangemessener Weise auf diese zukunffsgerichteten Aussagen zu verlassen.

WisdomTree Issuer ICAV

Die in diesem Dokument erörterten Produkte werden von WisdomTree Issuer ICAV („WT Issuer“) begeben. WT Issuer ist eine als Umbrella-Fonds strukturierte Anlagegesellschaff mit variablem Kapital und Haffungstrennung zwischen den Fonds, die nach irischem Gesetz als Irish Collective Asset-management Vehicle errichtet und von der Zentralbank von Irland („CBI“) zugelassen wurde. Die WT-Emittentin ist als Organismus für gemeinsame Anlagen in Wertpapieren („OGAW“) nach irischem Recht strukturiert und gibt eine separate Anteilsklasse („Anteile“) aus, die jeden Fonds repräsentiert. Anleger sollten den Verkaufsprospekt der WT-Emittentin („ WT-Prospekt“) vor einer Investition lesen und im Abschnitt des WT-Prospekts mit dem Titel„ Risikofaktoren“ weitere Einzelheiten über die mit einer Anlage verbundenen Risiken in entsprechende Anteile erfahren.

WisdomTree Artificial Intelligence UCITS ETF

Nasdaq® und der Nasdaq CTA Artificial Intelligence Index sind eingetragene Marken von Nasdaq, Inc. (gemeinsam mit ihren verbundenen Unternehmen als die „Unternehmen“ bezeichnet) und sind für die Nutzung durch WisdomTree Management Limited lizenziert. Die Unternehmen geben kein Urteil über die Rechtmäßigkeit oder Eignung des WisdomTree Artificial Intelligence UCITS ETF (der „Fonds“) ab. Anteile des Fonds werden von den Unternehmen nicht ausgegeben, empfohlen, verkauff oder beworben. DIE

UNTERNEHMEN ÜBERNEHMEN KEINE GARANTIEN UND KEINE HAFTUNG IN BEZUG AUF DEN FONDS.

Für Anleger in der Schweiz – Qualifizierte Anleger

Dieses Dokument dient als Werbung für die hier genannten Finanzprodukte.

Der Verkaufsprospekt und die wesentlichen Anlegerinformationen (KIID) sind auf der Website von WisdomTree verfügbar: **https:** //www.wisdomtree.eu/de-ch/resource-library/prospectus-and-regulatory-reports

Einige der Teilfonds, auf die in diesem Dokument verwiesen wird, wurden möglicherweise nicht bei der Eidgenössischen Finanzmarktaufsicht („FINMA“) registriert. In der Schweiz werden solche Teilfonds, die nicht bei der FINMA registriert sind, ausschließlich an qualifizierte Anleger im Sinne des Schweizer Bundesgesetzes über die kollektiven Kapitalanlagen oder seiner Durchführungsverordnung (jeweils in der jeweils gültigen Fassung) vertrieben. Die Vertretung und Zahlstelle der Teilfonds in der

Schweiz ist Société Générale Paris, Niederlassung Zürich, Talacker 50, Postfach 5070, 8021 Zürich, Schweiz. Der Prospekt, die wesentlichen Anlegerinformationen, die Satzung sowie die Jahres- und Halbjahresberichte der Teilfonds sind kostenlos bei der Vertretung und Zahlstelle erhältlich. Hinsichtlich des Vertriebs in der Schweiz befinden sich der Erfüllungsort und Gerichtsstand am Sitz der Vertretung und Zahlstelle.

Für französische Anleger

Die in diesem Dokument enthaltenen Informationen richten sich ausschließlich an professionelle Anleger (wie im Rahmen der MiFID definiert), die auf eigene Rechnung investieren, und dieses Material darf in keiner Weise öffentlich verteilt werden. Die Verteilung des Prospekts und das Angebot, der Verkauf und die Lieferung von Anteilen in anderen Ländern können gesetzlichen Beschränkungen unterliegen. Der Emittent ist ein OGAW, der der irischen Gesetzgebung unterliegt, und von der Finanzaufsichtsbehörde als OGAW, der den europäischen Verordnungen entspricht, zugelassen. Dennoch muss er möglicherweise nicht denselben Regeln entsprechen, die für ein ähnliches Produkt gelten, das in Frankreich zugelassen wurde. Der Fonds wurde in Frankreich von der Finanzaufsichtsbehörde (Autorité des Marchés Financiers) für den Vertrieb registriert und darf an Anleger in Frankreich vertrieben werden. Exemplare aller Dokumente (d. h. des Prospekts, des Dokuments mit den wesentlichen Informationen für den Anleger, aller zugehörigen Ergänzungen oder Nachträge, der neuesten Jahresberichte und der Gründungsurkunde und Satzung) sind in Frankreich kostenlos bei der französischen Zentralisierungsstelle Societe Generale unter der Adresse 29, boulevard Haussmann – 75009 Paris, Frankreich, erhältlich. Alle

Zeichnungen von Anteilen des Fonds erfolgen auf der Grundlage der Bedingungen des Prospekts und aller zugehörigen Ergänzungen oder Nachträge.