Cyberkriminelle auf dem Vormarsch/– Cybersicherheit muss jetzt zurückschlagen

Veröffentlicht am 31. März 2025

Mobeen Tahir
Director, Macroeconomics and Thematic Research

Die wichtigsten Erkenntnisse

- Cyberkriminelle nutzen KI und Social Engineering, um immer raffiniertere Angriffe zu starten.
- Eine schnelle Erkennung ist entscheidend – manche Sicherheitsverstöße eskalieren in weniger als einer Minute.
- Bekannte Cyberangriffe zeigen geopolitische Risiken auf: von der Beeinflussung von Wahlen bis hin zu staatlich unterstützen Verstößen.

Vor Kurzem habe ich eine Website erstellt. Doch nach der Veröffentlichung bemerkte ich, dass sie in Google-Suchen nicht angezeigt wurde. Bei meiner Suche nach einer Lösung für dieses Problem erhielt ich eine E-Mail mit einer schrittweisen Anleitung, was zu tun ist. Nichts an der E-Mail erschien verdächtig, nicht einmal die Adresse des Absenders. Doch als ich künstliche Intelligenz (KI) zur Überprüfung ihrer Echtheit einsetzte, wurde die Nachricht als verdächtig eingestuft.

Vor einigen Jahren wiesen Phishing-E-Mails offensichtliche Warnsignale auf: schlechte Grammatik, seltsame Formatierung oder zweifelhafte Links. Angesichts der KI-gestützten Tools, die Cyberkriminellen heute zur Verfügung stehen, sind sie weitaus raffinierter. Und wenn sie immer schlauer werden, muss die Cybersicherheit noch schlauer werden.

Die untragbaren Kosten eines Datenschutzverstoßes

Die durchschnittlichen Kosten einer Datenschutzverletzung kletterten im Jahr 2024 auf beinahe 5 Millionen US-Dollar[1]. Und das ist nur der Durchschnitt, d. h. viele Verstöße führten zu weitaus größeren Verlusten. Diese Zahl tendiert zwar seit Jahren nach oben, doch 2024 war ein sprunghafter Anstieg zu verzeichnen. Das unterstreicht, dass die weit verbreitete Nutzung fortschrittlicher KI-Tools Cyberkriminelle schlauer und Angriffe kostspieliger denn je macht.

„Die Angriffsgeschwindigkeit kann um bis zu 100-mal höher sein, wenn Bedrohungsakteure generative KI nutzen.“ – Palo Alto Networks

In vielen Fällen gehen die wahren Kosten einer Datenschutzverletzung über Dollar und Cent hinaus – sie sind unermesslich. Was, wenn das Vertrauen der Kunden in die Sicherheit eines Unternehmens erschüttert ist? Der Reputationsschaden kann irreversibel sein. Was, wenn ein Krankenhaus gehackt wird und Menschenleben gefährdet sind? Es könnte nicht mehr auf dem Spiel stehen. Darum ist Cybersicherheit

nicht nur eine Priorität, sondern eine Notwendigkeit. Und die Welt wacht endlich auf und wird sich dieser Realität bewusst.

Cyberkriminelle werden immer intelligenter

442 % **Zunahme von Voice-Phishing (Vishing) im H2/2024 ggü. H1/2024**	**79 %** **der Angriffe im Jahr 2024 erfolgten ohne Malware (ggü. 40 % im Jahr 2019)**
51Sekunden schnellste erfasste Breakout-Time von Internetkriminalität	**257** verfolgte feindliche Akteure, darunter 26 neue im Jahr 2024

Zunahme von Voice-Phishing (Vishing) im H2/2024 ggü. H1/2024

der Angriffe im Jahr 2024 erfolgten ohne Malware (ggü. 40 % im Jahr 2019)

51Sekunden

schnellste erfasste Breakout-Time von Internetkriminalität

verfolgte feindliche Akteure, darunter 26 neue im Jahr 2024

Quelle: Crowdstrike „Global Threat Report 2025“, März 2025.

Wenn Cyberkriminelle ein Ziel kompromittieren, versuchen sie, das Unternehmen über eine Schwachstelle zu infiltrieren und tiefer in das Netzwerk einzudringen. Die Breakout-Time für E-Crime-Akteure bezieht sich darauf, wie schnell Kriminelle die Kontrolle über kritische Systeme erlangen – vom ersten Eindringen über den Diebstahl von Daten und die Deaktivierung von Sicherheitssystemen bis hin zum Einsatz von Ransomware. Manche Angreifer schaffen das in weniger als einer Stunde, daher sind eine schnelle Entdeckung und Reaktion von entscheidender Bedeutung. 2024 betrug die schnellste aufgezeichnete Zeit, in der Angreifern dies gelang, 51 Sekunden[2].

Angreifer setzen nicht immer auf E-Mails – auch die unerwünschten Anrufe, die wir manchmal erhalten, können Übles im Sinn haben. Bei Vishing-Angriffen (Voice-Phishing) geben sich Cyberkriminelle per Telefonanruf als vertrauenswürdige Einrichtungen wie Banken, Behörden oder Dienstleister aus, um ihre Opfer zur Preisgabe vertraulicher Informationen oder zur Überweisung von Geld zu bewegen. Diese Betrügereien haben drastisch zugenommen: Im zweiten Halbjahr 2024 kletterte die Zahl der Vishing-Scams im Vergleich zum ersten Halbjahr 2024 um 442 %[3]. Das zeigt, wie Kriminelle das menschliche Vertrauen übers Telefon ausnutzen, um herkömmliche Cybersecurity-Abwehrmaßnahmen zu umgehen.

Vor einigen Wochen sah ich auf LinkedIn einen Beitrag über einen Mann, der von Polizeibeamten umringt war. Er erzählte, wie er physisch in ein Unternehmen eindrang, Sicherheitskontrollen passierte, sich Zugang zu gesperrten Bereichen verschaffte und sein Glück herausforderte, bis er schließlich erwischt

wurde. Es handelte sich jedoch nicht um einen echten Angriff, sondern um einen Penetrationstest – d. h. eine kontrollierte Sicherheitsübung, die dazu dient, Schwachstellen zu erkennen, bevor sie von Kriminellen ausgenutzt werden. Unternehmen führen diese Tests durch, weil Hacker immer ausgefeiltere Social-Engineering-Techniken anwenden. Sie manipulieren Menschen und nicht Systeme, um die Sicherheit zu umgehen und sich Zugang zu verschaffen. Die Bedrohung nimmt zu: 79 % der Angriffe im Jahr 2024 erfolgten ohne Malware – gegenüber 40 % im Jahr 2019[4]. Das beweist, dass Cyberkriminelle nicht immer Malware benötigen, wenn sie Menschen einfach dazu bringen können, die Tür zu öffnen.

Bekannte Cyberangriffe zeigen geopolitische Risiken auf

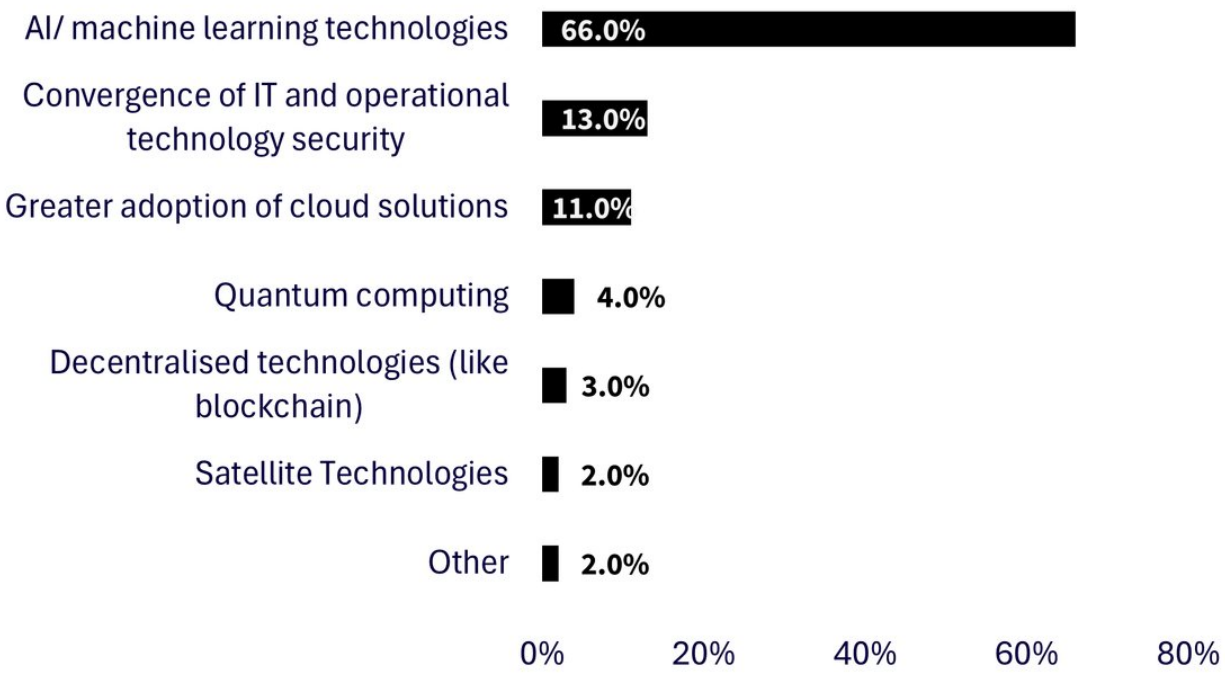
Zu Beginn des Wahljahres 2024 war die Sorge über Cyberrisiken groß. Viele Länder konnten den Wahlzyklus ohne größere bekannte Cybervorfälle überstehen, doch die rumänischen Präsidentschaftswahlen im Dezember wurden aufgrund von Vorwürfen der russischen Einmischung annulliert. Der unerwartete Vorsprung des rechtsextremen Kandidaten C lin Georgescu in der ersten Runde führte zu Untersuchungen, die eine koordinierte Online-Kampagne und Cyberangriffe zur Unterstützung seiner Kandidatur aufdeckten. Die Gerichte erklärten die Wahl daraufhin für ungültig.

Im selben Monat meldete das US-Finanzministerium einen schwerwiegenden Cybersecurity-Verstoß, der von China unterstützten Hackern zugeschrieben wird. Die Angreifer nutzten einen externen Softwareanbieter aus, um sich Zugang zu Arbeitsrechnern und nicht klassifizierten Dokumenten des Finanzministeriums zu verschaffen. Bei dem Verstoß wurde ein Sicherheitsschlüssel gestohlen, der den Remote-Zugriff auf die Systeme der Behörde ermöglichte. Obwohl das chinesische Außenministerium die Anschuldigungen bestritt, unterstreicht der Vorfall die zunehmende Überschneidung von geopolitischen und Cybersicherheitsrisiken.

Führungskräfte sind über Risiken durch KI besorgt

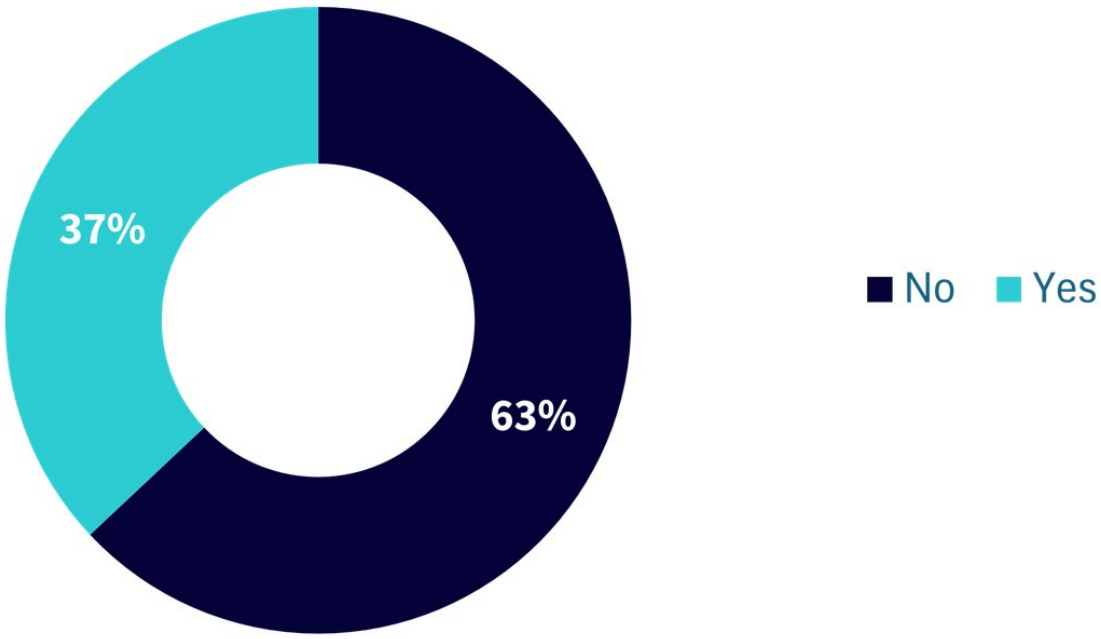
Eine aktuelle Umfrage des Weltwirtschaftsforums[5] unter Führungskräften ergab, dass nach Ansicht von 66 % der Teilnehmer KI und maschinelles Lernen in den nächsten zwölf Monaten die größten Auswirkungen auf die Cybersicherheit haben werden. Dennoch gaben 63 % der Befragten zu, dass es in ihren Unternehmen keine Verfahren gibt, um die Sicherheit von KI-Tools vor deren Einsatz zu bewerten – das zeigt eine kritische Lücke zwischen Innovation und Risikomanagement auf.

Abbildung 1: Welche der folgenden Faktoren werden Ihres Erachtens die Cybersicherheit in den nächsten zwölf Monaten am stärksten beeinflussen?



Quelle: Weltwirtschaftsforum „Global Cybersecurity Report 2025“.

Abbildung 2: Hat Ihr Unternehmen Verfahren zur Bewertung der Sicherheit von KI-Tools vor deren Einsatz eingerichtet?



Quelle: Weltwirtschaftsforum „Global Cybersecurity Report 2025“.

Cybersicherheit muss einen Schritt voraus sein

Die Cybersicherheit muss ständige Innovationen hervorbringen und Spitzentechnologien nutzen, um den sich entwickelnden Bedrohungen einen Schritt voraus zu sein. Dieser unerbittliche Wettlauf zwischen Abwehr und Angriff macht das Feld der Cybersicherheit so spannend und dynamisch. Aktuelle Schlagzeilen über Quantencomputer deuten darauf hin, dass das Quantenzeitalter näher sein könnte, als wir bisher dachten – eine Zukunft, in der ein Quantencomputer selbst die raffiniertesten Verschlüsselungen mühelos knacken könnte. Damit würde die Cybersicherheit, wie wir sie kennen, neu definiert. Ob Quantencomputer, KI oder Blockchain – jeder Durchbruch bringt neue Schwachstellen mit sich, und ihre Absicherung darf kein reaktives Unterfangen sein, sondern muss proaktiv erfolgen. Denn wenn wir warten, bis der Angriff stattfindet, könnte es bereits zu spät sein.

[1] IBM, 2025.
[2] Quelle: Crowdstrike „Global Threat Report 2025“, März 2025.
[3] Quelle: Crowdstrike „Global Threat Report 2025“, März 2025.
[4] Quelle: Crowdstrike „Global Threat Report 2025“, März 2025.
[5] Quelle: Weltwirtschaftsforum „Global Cybersecurity Report 2025“.

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.

Diese Marketingmitteilung wurde für professionelle Anleger erstellt. Die in diesem Dokument beschriebenen Produkte von WisdomTree können jedoch in einigen Ländern unter Einhaltung der geltenden Gesetze und Bestimmungen für alle Anleger erhältlich sein. Da das Produkt in Ihrem Land möglicherweise nicht zugelassen ist oder nur eingeschränkt angeboten werden darf, liegt es in der Verantwortung jeder Person oder jedes Unternehmens, sich über die umfassende Einhaltung der Gesetze und Bestimmungen des jeweiligen Landes zu informieren. Anlegern wird empfohlen, sich vor der Anwendung hinsichtlich aller rechtlichen, aufsichtsrechtlichen, steuerlichen und anlagetechnischen Folgen einer Anlage in den Produkten beraten zu lassen. 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 der 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 Recht als Irish Collective Asset-management Vehicle errichtet und von der Zentralbank von Irland („CBI“) zugelassen wurde. WT Issuer ist als Organismus für gemeinsame Anlagen in Wertpapieren („OGAW“) nach irischem Recht strukturiert und gibt eine separate Anteilsklasse („Anteile“) aus, die jeden Fonds repräsentiert.

Der Fonds wird in den wesentlichen Anlegerinformationen (Key Information Document, KID) bzw. den wesentlichen Anlegerinformationen für britische Anleger (Key Investor Information Document, KIID) und im Prospekt von WT Issuer (der „WT-Prospekt“) beschrieben. Eine Kopie des WT-Prospekts und des KID/KIID ist, ausschließlich für den EWR und das Vereinigte Königreich, in englischer Sprache verfügbar unter www.wisdomtree.eu. Wo dies nach nationalen Vorschriffen erforderlich ist, ist das KID auch in der Landessprache des jeweiligen EWR-Mitgliedstaates verfügbar. Anleger sollten vor einer Anlage den WT-Prospekt lesen und weitere Informationen zu den mit einer Anlage in den Anteilen verbundenen Risiken dem Abschnitt „Risk Factors“ im WT-Prospekt entnehmen.

Eine Zusammenfassung der mit einer Anlage in dem Fonds verbundenen Anlegerrechte ist in englischer Sprache auf der Website von WisdomTree Europe verfügbar. WisdomTree Management Limited kann für die Vermarktung ihrer Organismen für gemeinsame Anlagen getroffene Vereinbarungen kündigen. Unter diesen Umständen werden die Anteilsinhaber in den betroffenen EWR-Mitgliedstaaten über diese Entscheidung informiert und erhalten die Möglichkeit, ihre Anteile an dem Fonds innerhalb eines Zeitraums von mindestens 30 Werktagen ab dem Datum der entsprechenden Mitteilung frei von Kosten und Abzügen zurückzugeben.

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.