Im Jahr 2025 mit Cybersicherheit breite Benchmarks übertreffen

Veröffentlicht am 16. Juni 2025

Elvira Kuramshina
Associate Director, Quantitative Research

Die wichtigsten Erkenntnisse

- Die Welt ist zunehmend digital – damit steigt auch die Nachfrage nach Cybersicherheitslösungen. Neben der laufenden Digitalisierungswelle wird das Wachstumspotenzial der Cybersicherheit durch mehrere Impulse weiter gestärkt.
- Während sich Zins- und Zollsorgen in höherer Volatilität und einem geringeren Vertrauen in Unternehmensausgaben niederschlagen, bieten langfristige Faktoren eine dauerhafte Grundlage für nachhaltige Investitionen in Cybersicherheit.
- Dank des Differenzierungspotenzials, das der WisdomTree Team8 Cybersecurity UCITS Index bietet, und der robusten Nachfrage nach Cybersicherheit ist er eine attraktive langfristige Anlage neben den traditionellen Kernengagements.

Das Jahr 2025 hat die Geduld der Anleger auf eine harte Probe gestellt. Von zollbedingter Unsicherheit über steigende geopolitische Risiken bis hin zur zunehmenden Verbreitung von KI haben die Märkte heftige Turbulenzen und Volatilität verzeichnet. Vor diesem schwierigen Hintergrund sticht der WisdomTree Team8 Cybersecurity UCITS Index mit seiner seit Jahresbeginn erzielten Outperformance gegenüber den breit gefassten Tech- und Aktien-Benchmarks hervor und unterstreicht damit seine Widerstandsfähigkeit trotz eines sich eintrübenden makroökonomischen Umfelds und veränderter Prioritäten und Ausgaben der Unternehmen (siehe Abbildung 1). In diesem Blog befassen wir uns mit der Beständigkeit der langfristigen Nachfrage nach Cybersicherheit, beleuchten den kurzfristigen Gegenwind durch makroökonomische Unsicherheit und erörtern schließlich, wie eine Satellitenallokation in Cybersicherheit die Renditen Ihres Portfolios über die Renditen der breiten Benchmarks hinaus steigern kann.

Beständigkeit der Cybersecurity-Nachfrage

Die Welt ist zunehmend digital – damit wird die Cybersicherheit zu einem der wichtigsten Megatrends für die Sicherung unserer Zukunft. Neben der laufenden Digitalisierungswelle wird das Wachstumspotenzial der Cybersicherheit durch mehrere Impulse weiter gestärkt.

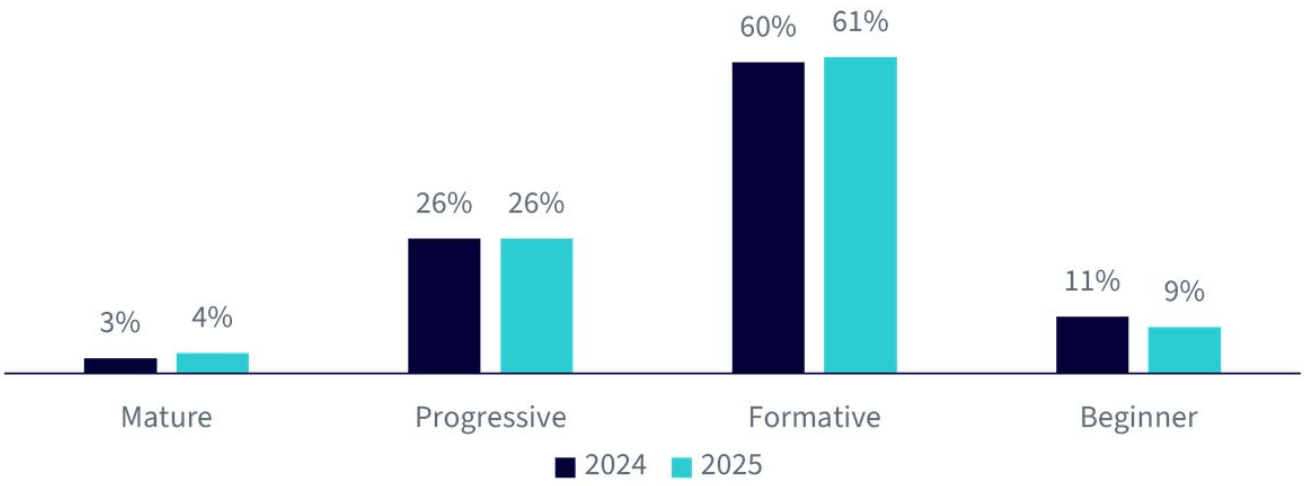
1. Neudefinition von Widerstandskraft und Wettbewerbsfähigkeit von Unternehmen

Die Digitalisierung, die durch die globale Pandemie stark vorangetrieben wurde, erhielt durch die sich abzeichnende KI-Revolution weiteren Aufwind. Doch jede neue Ebene digitaler Infrastruktur erfordert

robuste Sicherheitsmaßnahmen – im heutigen digitalen Zeitalter ist die Cybersicherheit eine Frage der Widerstandskraft von Unternehmen. Der vor Kurzem bei Marks & Spencer, einem der größten britischen Einzelhändler, aufgetretene Cybervorfall ist ein Beispiel dafür, wie lähmend und kostspielig ein Cyberangriff in der modernen Realität sein kann. Laut Schätzungen des Unternehmens werden die Gewinneinbußen 300 Millionen US-Dollar betragen und die Unterbrechung des Online-Betriebs bis Juli andauern[1].

Dieser Vorfall macht deutlich, wie wichtig angemessene Cybersecurity-Lösungen für jedes moderne Unternehmen sind, und erklärt, warum die Nachfrage nach Cybersicherheitslösungen auch in Zeiten wirtschaftlicher Turbulenzen ungebrochen ist. Parallel dazu berichtet Cisco in seinem Cybersecurity Readiness Index 2025, dass Unternehmen nicht mit der Weiterentwicklung der Bedrohungslandschaft Schritt halten, da nur 30 % von ihnen einen „reifen“ oder „fortschrittlichen“ Bereitschaftsstatus aufweisen, um den heutigen Cybersecurity-Risiken zu begegnen, und die Dynamik gegenüber 2024 nahezu unverändert ist (siehe Abbildung 2). Das wiederum zeigt das zukünftige Wachstumspotenzial für Cybersicherheitsanbieter, da Unternehmen, die ihre Wettbewerbsfähigkeit stärken wollen, ihre Ausgaben für Cybersicherheit erhöhen werden. Beispielsweise können Unternehmen mit angemessenen Cybersecurity-Lösungen einen vertrauensbasierten Wettbewerbsvorsprung schaffen und neue Technologien sicher einführen, um der Konkurrenz einen Schritt voraus zu sein.

Abbildung 1: Globale Bereitschaft zur Bewältigung von Cybersicherheitsrisiken



Quelle: Cisco Cybersecurity Readiness Index 2025. Der Cisco Cybersecurity Readiness Index 2025 bewertet anhand von fünf Säulen, inwieweit Unternehmen auf die heutigen Cybersecurity-Risiken vorbereitet sind: Identity Intelligence (Identitätsdaten), Machine Trustworthiness (Vertrauenswürdigkeit von Maschinen), Network Resilience (Ausfallsicherheit von Netzwerken), Cloud Reinforcement und Artificial Intelligence (AI) Fortification (Stärkung künstlicher Intelligenz). Die Bewertung basiert auf einer Doppelblind-Umfrage unter 8.000 Unternehmen und Führungskräften im Bereich Cybersicherheit in 30 globalen Märkten und einem breiten Spektrum von privatwirtschaftlichen Branchen.

2. Geopolitische Risiken und politischer Rückenwind

Darüber hinaus ist Cybersicherheit angesichts der zunehmenden geopolitischen Spannungen und der öffentlichkeitswirksamen Cyberangriffe nicht nur für Unternehmen, sondern auch für Regierungen ein wichtiges Thema. Die rasante Weiterentwicklung der Bedrohungslandschaft, zu der auch staatliche Akteure gehören, führte zu einer Welle von regulatorischen und strategischen Maßnahmen, die die langfristige Nachfrage nach Cybersicherheitslösungen verstärken. Die National Cybersecurity Strategy (2023) der USA betont die Dringlichkeit eines gezielteren und besser koordinierten Ansatzes für die Cyberverteidigung sowie die Neuausrichtung der Anreize zur Förderung langfristiger strategischer Investitionen im Cyberbereich. In Europa zielt das EU-Cybersolidaritätsgesetz darauf ab, die kollektive Bereitschaft, Erkennung und Reaktion durch Finanzmittel im Rahmen des strategischen Ziels „Cybersicherheit“ und gemeinsame Bereitschaftsmaßnahmen, Situationsbewusstsein und grenzüberschreitende Zusammenarbeit zu fördern. Gleichzeitig konzentriert sich die NATO verstärkt auf die kollektive Cyberverteidigung und passt ihre Verteidigungsstrategie als Reaktion auf die sich rasch entwickelnde Bedrohungslage an.

3. Verbreitung generativer KI

Generative KI erobert seit der Einführung von ChatGPT am 30. November 2022 die Welt im Sturm. Während KI-Technologie innovative Möglichkeiten für Cybersecurity-Unternehmen eröffnet, wie etwa die Automatisierung der Bedrohungserkennung und die Verbesserung der Datenanalyse, schafft sie auch neue Schwachstellen und treibt Innovationen in der Bedrohungslandschaft voran. Mit ihrer raschen Verbreitung und Weiterentwicklung erweist sich die Technologie als einer der wesentlichen Impulsgeber für die Zunahme von Cyberangriffen. Von böswilligen Tools zur Generierung von Deepfakes für Imitationen und Social Engineering über Data Poisoning (Vergiftung von Daten) von großen Sprachmodellen (LLMs) bis hin zum Jailbreaking (nicht autorisiertes Entfernen von Nutzungsbeschränkungen) von LLMs zur Verbesserung der Malware-Erstellung nutzen Bedrohungsakteure KI, um ihre Ziele noch effizienter, erfolgreicher und schneller zu erreichen.

Gleichzeitig sehen sich Unternehmen aufgrund der Nutzung von KI-Modellen einem höheren Risiko von Datenlecks ausgesetzt. Check Point berichtet in seinem ersten „AI Security Report 2025“, dass eine von 13 KI-Eingaben sensible oder private Daten enthält und eine von 80 Eingaben sensible Daten für Angreifer preisgibt. Darüber hinaus wies Check Point darauf hin, dass Unternehmen, die keine KI einsetzen, möglicherweise feststellen, dass ihre Mitarbeiter KI-Tools unerlaubt nutzen, was weitere Risiken birgt. Als Reaktion darauf bieten verschiedene Cybersicherheitsunternehmen bereits Lösungen an, die speziell auf die Risiken im Zusammenhang mit der geschäftlichen Nutzung von LLMs zugeschnitten sind. Da KI-gestützte Cyberbedrohungen immer häufiger auftreten, wird die Nachfrage nach Cybersicherheitslösungen in gleichem Maße steigen.

Kurzfristiger makroökonomischer Gegenwind

Trotz der starken zugrunde liegenden Nachfrage und des attraktiven zukünftigen Wachstumspotenzials sind Cybersicherheitsunternehmen nicht immun gegen allgemeine makroökonomische Turbulenzen. Tatsächlich sind sie mit Blick auf die Sensitivität gegenüber Zinserwartungen häufig mit Tech-Aktien

mit längerer Duration vergleichbar. Das liegt vor allem daran, dass viele führende Cybersicherheitsunternehmen ein schnelles Wachstum verzeichnen, wobei ein Großteil der erwarteten Cashflows in die Zukunft projiziert wird. Bei steigenden Zinsen werden diese zukünftigen Cashflows stärker abgezinst, wodurch die Bewertungen heftiger auf Änderungen der Zinserwartungen reagieren.

Die neuesten geldpolitischen Entwicklungen in den USA haben vor dem Hintergrund der durch die Ankündigung von Zöllen ausgelösten makroökonomischen Unsicherheit zu einer gesteigerten Marktvolatilität und einer Neubewertung der Erwartungen hinsichtlich künftiger Zinssenkungen geführt, die durch die Veröffentlichung des Sitzungsprotokolls des Offenmarktausschusses (FOMC) vom Januar in Gang gesetzt wurde. Aufgrund der Unsicherheit im Zusammenhang mit Zöllen preisen die Märkte ein höheres Rezessionsrisiko ein, insbesondere in Anbetracht der nachlassenden Konjunktur und der Tatsache, dass die US-Notenbank es vorzieht, die Leitzinsen konstant zu halten, anstatt eine frühzeitige Zinssenkung zu riskieren.

Geplante Zölle schlagen sich in höherer Volatilität und einem geringeren Vertrauen in Unternehmensausgaben nieder. In diesem Umfeld könnte es im Bereich der Cybersicherheit zu langsameren Geschäftsabschlüssen kommen, da Unternehmen die kurzfristigen Aussichten abwägen. Außerdem könnten sich die US-Zölle über Hardware-Anwendungen auf Cybersicherheitsunternehmen auswirken, z. B. über Firewalls, sichere Router und Intrusion Detection/Prevention Systems (IDS/IPS). Einige Unternehmen könnten ihre Software mit Hardware von Drittanbietern bündeln und über ihre Partner betroffen sein. Auf Software spezialisierte Cybersecurity-Unternehmen sind hier besser aufgestellt, könnten aber auch indirekt durch Zölle belastet werden. Cloud-basierte Dienste sind auf die Hardware physischer Rechenzentren angewiesen und Anbieter öffentlicher Clouds könnten ihre Preise erhöhen, wenn ihre Kosten steigen.

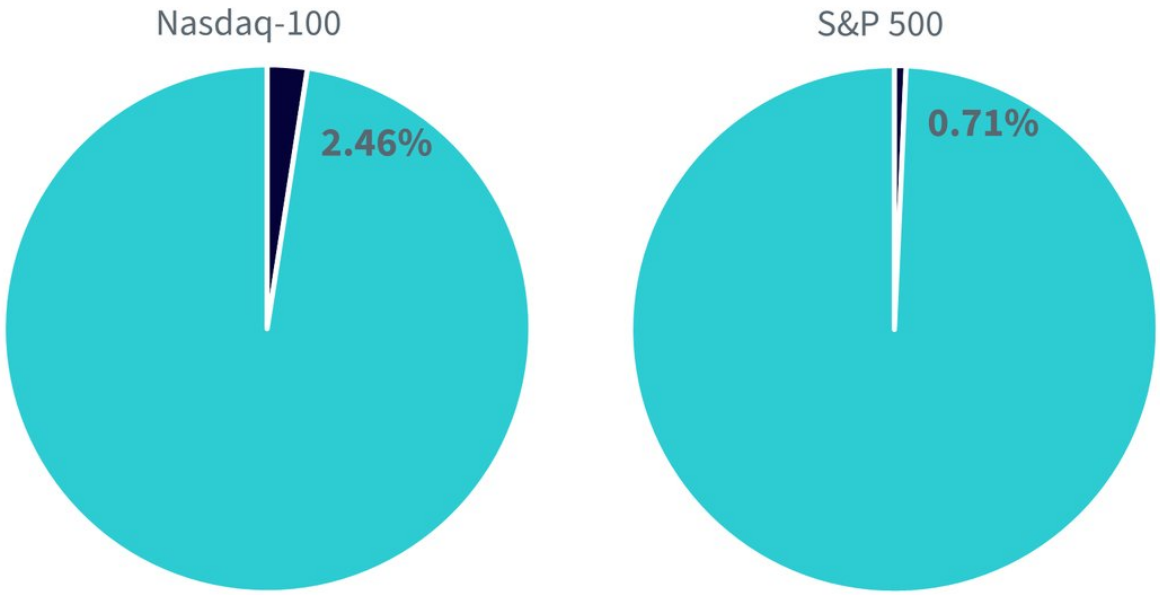
Während Zins- und Zollsorgen die Ausgaben kurzfristig unter Druck setzen könnten, bieten langfristige Faktoren wie die rasante Digitalisierung und Verbreitung von KI sowie die zunehmenden geopolitischen Bedrohungen eine dauerhafte Grundlage für nachhaltige Investitionen in Cybersicherheit. Das langfristige Wachstumspotenzial des Sektors bleibt erhalten und der Aktienmarkt sieht das offenbar genauso. Das lässt sich aus der starken Erholung des WisdomTree Team8 Cybersecurity UCITS Index nach der Ankündigung einer 90-tägigen Pause durch Präsident Trump am 9. April sowie aus der Renditedifferenz ableiten, die die Strategie in der ersten Hälfte des ersten Quartals 2025 gegenüber den breiten Tech- und Aktien-Benchmarks verzeichnet hat (siehe Abbildung 1).

Ein attraktives Satellitenengagement für einen langfristigen Kern

Eines der wichtigsten Wertversprechen thematischer Strategien ist die Differenzierung, die sie gegenüber breit angelegten Aktienengagements bieten. Dieses Differenzierungspotenzial kann sich je nach Thema unterscheiden. Bei Cybersecurity-Unternehmen ist das Engagement, das Anleger über breit angelegte Aktien- oder Tech-Benchmarks erzielen können, minimal, vor allem aufgrund der geringen Gewichtung dieser Unternehmen in breit angelegten Benchmarks. Beispielsweise sind Palo Alto und CrowdStrike, die gemessen an der Marktkapitalisierung zu den größten reinen Cybersicherheitsunternehmen gehören, am 30. Mai 2025 im NASDAQ-100 nur mit 0,79 % und 0,68 % gewichtet. Ein Blick auf die Überschneidungen zwischen dem WisdomTree Team8 Cybersecurity UCITS Index, der derzeit 25 Cybersecurity-Un-

ternehmen umfasst, zeigt eine Überschneidung von weniger als 2,5 % mit dem NASDAQ-100 und von weniger als 1 % mit dem S&P 500 (siehe Abbildung 3).

Abbildung 2: Überschneidungen zwischen dem WisdomTree Team8 Cybersecurity UCITS Index und breiten Tech- und Aktien-Benchmarks



Quelle: WisdomTree, Bloomberg, MSCI. Stand: 30. Mai 2025. WisdomTree Cybersecurity ist durch den WisdomTree Team8 Cybersecurity UCITS Index (WTCBRUN) dargestellt. NASDAQ-100 ist der NASDAQ 100 Index S&P 500 bezieht sich auf den S&P 500 Index. Die Überschneidung gemeinsamer Wertpapiere ist die Summe aller sich überschneidenden Gewichtungen mit WTCBRUN innerhalb eines bestimmten Index. Die Überschneidung der Gewichtung wird als die niedrigere Gewichtung eines Wertpapiers berechnet, das sowohl im WTCBRUN als auch in einem bestimmten Index enthalten ist. **Es ist nicht möglich, direkt in einen Index zu investieren. Die historische Wertentwicklung ist kein Hinweis auf die künftige Wertentwicklung, und Anlagen können im Wert sinken.**

Geringe Überschneidungen deuten darauf hin, dass die Beimischung dieser Art von Engagement zu Ihrer Tech- oder Aktien-Kernallokation das Potenzial hat, die Renditen durch Diversifikationsvorteile zu steigern. Darüber hinaus ist eine Cybersicherheitsstrategie aufgrund der robusten Nachfrage nach Cybersicherheit eine attraktive langfristige Investition neben den traditionellen Kernengagements.

[1] https://www.bbc.co.uk/news/articles/c93llkg4n51o

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. Die in diesem Dokument enthaltenen Informationen dienen ausschließlich Ihrer Information und stellen weder ein Angebot zum Verkauf bzw. eine Aufforderung oder ein Angebot zum Kauf von Wertpapieren oder Anteilen dar. Dieses Dokument sollte nicht als Basis für eine Anlageentscheidung verwendet werden. Anlagen können an Wert zunehmen oder verlieren und Sie können einen Teil oder den gesamten Betrag der Anlage verlieren. Die Wertentwicklung in der Vergangenheit ist nicht notwendigerweise ein Hinweis auf zukünffige Ergebnisse. Anlageentscheidungen sollten auf den Angaben im entsprechenden Prospekt sowie auf unabhängiger Anlage-, Steuer- und Rechtsberatung basieren.

Die Anwendung von Verordnungen und Steuergesetzen kann off zu unterschiedlichen Interpretationen führen. Alle in dieser Mitteilung dargestellten Ansichten oder Meinungen spiegeln die Auffassung von WisdomTree wider und sollten nicht als aufsichtsrechtliche, steuerliche oder rechtliche Beratung ausgelegt werden. WisdomTree übernimmt keine Garantie oder Zusicherung hinsichtlich der Richtigkeit der in dieser Mitteilung geäußerten Ansichten oder Meinungen. Anlageentscheidungen sollten auf den Angaben im entsprechenden Prospekt sowie auf unabhängiger Anlage-, Steuer- und Rechtsberatung basieren.

Bei diesem Dokument handelt es sich nicht um Werbung bzw. eine Maßnahme zum öffentlichen Angebot von Anteilen oder Wertpapieren in den USA oder einer zugehörigen Provinz bzw. einem zugehörigen Territorium der USA, und es darf unter keinen Umständen als solche verstanden werden. Weder dieses Dokument noch etwaige Kopien dieses Dokuments sollten in die USA mitgenommen, (direkt oder indirekt) übermittelt oder verteilt werden.

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.