# Weiterentwicklung von WisdomTree Cybersecurity für das Zeitalter der KI

Veröffentlicht am 26. Oktober 2026

**Elvira Kuramshina**
Associate Director, Quantitative Research

## Wichtige Erkenntnisse

- Eine neue Ära des Cyberrisikos: Generative KI hat die wirtschaftlichen Aspekte der Cyberkriminalität bereits verändert. Nun läuten innovative KI-Modelle eine neue Phase der Risiken und der Nachfrage ein. Wir haben die Methode des WisdomTree Team8 Cybersecurity UCITS Index weiterentwickelt, um diesem Wandel Rechnung zu tragen.
- KI verändert die zu schützenden Bereiche: Da KI neue Angriffsflächen und neue Kategorien von Sicherheitsausgaben schafft, verlagern sich die Wachstumsquellen der Cybersicherheit. Die Auswahl und Gewichtung von Unternehmen müssen sich entsprechend anpassen.
- Drei Überarbeitungen der Methode: ein verbesserter, auf mehreren Signalen basierender Fokus-Score, ein zukunftsorientierter Wachstums-Score und eine transparente, modulare Gewichtungsformel – alle darauf ausgelegt, die Chancen der Cybersicherheit im Zeitalter der KI zu erfassen.
- Gleiche Grundlagen, klarere Schwerpunkte: Das Ausgangsuniversum, das Kernkonzept und der kompetente Partner Team8 bleiben unverändert, während sich die Portfoliogewichtungen zugunsten von Unternehmen mit einer stärkeren Positionierung in der Cybersicherheit und besseren Wachstumsprofilen verschieben.
- Cybersicherheit als grundlegende Ebene: Da KI zunehmend in der digitalen Wirtschaft verankert ist, ist der Index so konzipiert, dass er mit den Bereichen Schritt hält, in denen die stärkste Nachfrage besteht.

Cybersicherheit war schon immer ein Wettlauf zwischen Angreifern und Verteidigern, und künstliche Intelligenz (KI) verändert das Tempo dieses Wettlaufs. In den letzten Jahren hat generative KI die wirtschaftlichen Aspekte der Cyberkriminalität bereits neu definiert: Angriffe werden schneller und zahlreicher, gleichzeitig erhalten Verteidiger leistungsfähigere Instrumente zur Erkennung und Reaktion. Nun läuten Fortschritte bei innovativen KI-Modellen eine neue Ära ein. Während sich KI in Unternehmenssystemen ausbreitet, entstehen neue Bereiche, die zu schützen sind – von Modellen über Trainingsdaten bis hin zu autonomen Agenten und Maschinenidentitäten. Die Chance liegt nach wie vor in der Cybersicherheit, doch die Quellen für Wachstum und Differenzierung verschieben sich. Gemeinsam mit unserem kompetenten Partner Team8 untersuchen wir, was diese Veränderungen für die Branche bedeuten.

In den letzten Jahren wurde die Branche von Cloud-nativer, identitätsorientierter und KI-gestützter Sicherheit geprägt. Heute entwickelt sie sich zu einer Umgebung, die zunehmend durch die Möglichkeiten innovativer Modelle, autonome Agenten, Maschinenidentitäten und neue Angriffsflächen gekennzeichnet ist, wobei KI-Systeme selbst einen speziellen Schutz benötigen. Um diesen Wandel zu erfassen, ist ein Ansatz erforderlich, der darauf reagiert, wo KI die stärkste zukünftige Nachfrage erzeugt. Unsere methodische Antwort sind aktualisierte Signale, die auf tiefergehenden Expertenerkenntnissen zur Auswahl und Gewichtung von Unternehmen beruhen, wobei das gleiche Universum und das gleiche Kernkonzept beibehalten werden.

## Warum sich die Chance im Cybersegment verändert

Die Cyberbedrohungslage spitzt sich an mehreren Fronten gleichzeitig zu. Der „2026 Global Threat Report“ von CrowdStrike ergab, dass ein E-Crime-Angreifer im schnellsten Fall in nur 27 Sekunden vom ersten Zugriff zur lateralen Bewegung überging – eine deutliche Erinnerung daran, wie wenig Spielraum für Fehler den Verteidigern bleibt. Auch der Angreiferpool wächst: Die Zahl der aktiven Ransomware-Gruppen ist im Vergleich zum Vorjahr um 49 % gestiegen. Unterdessen nehmen die Kosten für Fehlschläge weiter zu. IBM schätzt die weltweiten Durchschnittskosten einer Datenpanne auf 4,99 Millionen US-Dollar.

KI prägt mittlerweile beide Seiten des Wettlaufs. Einerseits hat sie eine neue Angriffsfläche geschaffen. Untersuchungen von Check Point ergaben, dass etwa jede 80. Eingabe bei generativer KI sensible Daten gefährdet, während IBM die durchschnittlichen Kosten eines Datenlecks, bei dem es zur Inversion eines KI-Modells kommt, auf rund 6 Millionen US-Dollar beziffert. Andererseits erweist sich KI als starker Trumpf für die Verteidiger. Laut der Analyse von IBM sparen Unternehmen, die KI und Automatisierung in großem Umfang in ihren Sicherheitsabläufen einsetzen, durchschnittlich 1,93 Millionen US-Dollar pro Sicherheitsvorfall ein. Diese Dualität führt zu einer eigenständigen Kategorie von Sicherheitsausgaben, deren Schwerpunkt auf dem Schutz von Modellen, Trainingsdaten, autonomen Agenten und Maschinenidentitäten liegt. Nichts veranschaulicht diesen Wandel besser als das Aufkommen von Pioniermodellen mit fortschrittlichen Cyberfähigkeiten.

**Abbildung 1: KI entwickelt sich zu einer neuen Angriffsfläche und zu einem neuen Instrument sowohl für Cyberkriminelle als auch für Cyberverteidiger**

| Bei > 90 Unternehmen | 1 von 80 GenAI-Prompts | 6 Millionen US-Dollar |
|---|---|---|
| Angreifer nutzten legitime GenAI-Tools aus und fügten bösartige Prompts ein, um Befehle zum Diebstahl von Zugangsdaten und Kryptowährung zu generieren (CrowdStrike) | Machen sensible Daten Angreifern zugänglich (Check Point) | Die weltweit durchschnittlichen Kosten eines Angriffs durch Inversion eines KI-Modells, die die zunehmende Schwierigkeit widerspiegeln, Trainingsdaten und sensible Informationen zu schützen (IBM) |

| 56% | 7,5 % der GenAI-Prompts | 1,93 Millionen US-Dollar |
|---|---|---|
| Zunahme von KI-gestützten Angriffen, allen voran KI-Deepfake-Identitätsbetrug und KI-basierte Malware (IBM) | enthalten vertrauliche oder persönliche Angaben (Check Point) | Kosteneinsparungen durch den umfassenden Einsatz von KI und Automatisierung im Sicherheitsbereich im Vergleich zu Unternehmen, die diese nicht einsetzen (IBM) |

Quelle: CrowdStrike, „Global Threat Report“, veröffentlicht im Februar 2026. IBM, „X-Force Threat Intelligence Index 2026“. IBM, „Cost of a Data Breach Report 2026“. Check Point, „AI Security Report 2025“.

Die begrenzte Herausgabe von Claude Mythos Preview von Anthropic und die darauf folgende Initiative Project Glasswing mit rund 50 Partnern stellten einen Wendepunkt dar und demonstrierten ein neues Niveau bahnbrechender KI-Fähigkeiten bei der Suche nach Schwachstellen in großem Maßstab. In nur einem Monat deckten die Partner mehr als 10.000 Schwachstellen mit hohem oder kritischem Schweregrad auf. Das britische AI Security Institute, das Mythos Preview im April 2026 bewertete, beschrieb diese Fähigkeiten als doppelt nutzbar: Sie stellen echte Sicherheitsherausforderungen dar, bieten aber auch das Potenzial für bahnbrechende Verbesserungen in der Verteidigung. Angesichts der zu erwartenden leistungsfähigeren Modelle argumentierte das Institut, dass Investitionen in die Cyberabwehr jetzt unerlässlich seien.

## Einführung des methodischen Ansatzes

Der methodische Ansatz für die sich wandelnde Chance in der Cybersicherheit stützt sich auf drei Neuerungen: einen verbesserten, auf mehreren Signalen basierenden Fokus-Score, einen zukunftsorientierten Wachstums-Score und eine transparente, modulare Gewichtungsformel. Zusammen sollen sie erfassen, in welche Richtung sich die Nachfrage nach Cybersicherheit entwickelt und welche Unternehmen voraussichtlich besser positioniert sind, um davon zu profitieren.

### Ein verbesserter, auf mehreren Signalen basierender Fokus-Score

**Fokus-Score = Breite der Cybersicherheit + Produktführerschaft + Schwerpunktthemen**

Bisher basierte der Fokus-Score auf einem einzigen Signal: der Einstufung des Fokus eines Unternehmens als „Breit“ oder „Eng“. Nun setzt er sich aus drei sich ergänzenden und interpretierbaren Signalen zusammen, die addiert werden. Jedes dieser Signale erfasst eine andere Dimension der Cybersicherheitspositionierung eines Unternehmens:

- Die **Breite der Cybersicherheit (40 %)** belohnt Unternehmen, die die Nachfrage in vielen Bereichen des Marktes bedienen können, anstatt sich auf eine begrenzte Auswahl an Lösungen zu verlassen. Ein Unternehmen gilt als „breit aufgestellt“, wenn es in mindestens der Hälfte der Entwicklungsthemen der Cybersicherheit stark engagiert ist. Unternehmen mit „engem Fokus“, die in mindestens einem Thema stark vertreten sind, bleiben ebenfalls zulässig, sodass Spezialisten weiterhin Teil des Chancenspektrums sind.
- **Produktführerschaft (30 %)** berücksichtigt sowohl Tiefe als auch Breite. Team8 bewertet Cybersicherheitsprodukte innerhalb spezifischer Lösungskategorien und stellt Unternehmen heraus, deren Produkte in ihrem Bereich führend sind, selbst wenn die Gesamtproduktpalette enger gefasst ist. So kann die Strategie in Unternehmen investieren, die durch differenzierte Fähigkeiten in der Lage sind, aufkommende Nachfrage zu erschließen.
- Die **Schwerpunktthemen (20 % oder 30 %)** lenken die Ausrichtung auf Bereiche, in denen die Nachfrage nach Cybersicherheit anziehen dürfte. Ein Unternehmen erhält 20 %, wenn mindestens die Hälfte seines Engagements in diesen Themen liegt, und 30 %, wenn es zudem eine führende Produktposition einnimmt. Die aktuellen Schwerpunktthemen sind **KI-Sicherheit**, das Lösungen zum Schutz von KI-Systemen selbst umfasst, **Intelligentere Sicherheit**, bei dem KI und Automatisierung eingesetzt werden, um Sicherheitsmaßnahmen schneller und anpassungsfähiger zu gestalten, sowie **Grenzenlose Welt**, das sich auf Identitäten und Zugriff konzentriert – ein Thema, das zunehmend an Bedeutung gewinnt, da KI-Agenten ein immer größeres Universum maschineller Identitäten schaffen. Diese Themen sind nicht festgeschrieben und können sich mit der Weiterentwicklung von Technologien und Bedrohungsvektoren ändern.

## Ein zukunftsorientierter Wachstums-Score

Der aktualisierte Wachstums-Score misst, wie gut ein Unternehmen voraussichtlich die Nachfrage nach Cybersicherheit monetarisieren kann, wobei das geschätzte Umsatzwachstum als Signal dient. Soweit zuverlässige Daten es zulassen, blickt der Score in die Zukunft und folgt dabei einer einfachen Rangfolge: An erster Stelle steht die geschätzte durchschnittliche jährliche Wachstumsrate (CAGR) über zwei Jahre, gefolgt von der Ein-Jahres-Schätzung, falls keine Zahl über zwei Jahre vorliegt, und schließlich dem tatsächlichen Wachstum der letzten zwölf Monate, wenn weniger als fünf Analysten Schätzungen abgeben.

Unternehmen werden dann im Vergleich zum Rest des infrage kommenden Cybersicherheitsuniversums und nicht anhand fester Wachstumshürden eingestuft, sodass sich die Schwellenwerte an die Marktbedingungen und das Tempo des Cyberzyklus anpassen. Die unteren 20 % werden ausgeschlossen. Die verbleibenden Unternehmen werden in vier Gruppen mit jeweils eigenem Gewichtungsfaktor eingeteilt:

- **Schnelles Wachstum & Skalierung (1,5x):** Unternehmen mit höherem Wachstum, deren nachlaufender Umsatz unter den Top 10 der Gruppe mit stärkerem Wachstum sowie über dem Median des Universums lag. Die Gruppe ist auf zehn Unternehmen begrenzt.
- **Schnelles Wachstum (1,2x):** Unternehmen mit Wachstum über dem Median des Universums.

- **Wachstum (1x):** Unternehmen mit Wachstum auf der Höhe von oder unter dem Median.
- **Wachstum & Verlangsamung (0,8x):** Unternehmen, die hinsichtlich ihres Wachstums-Scores zu den unteren 40 % gehören und deren aktuelles Wachstum über den Schätzungen der Analysten liegt – ein Zeichen dafür, dass sich die Dynamik abschwächt.

### Eine transparente Gewichtungsformel

**Endgültige Gewichtung = Gleichgewichtung × Fokusfaktor × Wachstumsfaktor**

Jedes Unternehmen startet mit der gleichen Gewichtung. Diese Ausgangsgewichtung wird dann mit zwei Faktoren multipliziert – einem aus dem Fokus-Score und einem aus dem Wachstums-Score. Die Ergebnisse werden so neu skaliert, dass sich das Portfolio auf 100 % summiert:

Der **Fokusfaktor** beträgt 1 plus den Fokus-Score des Unternehmens. Jedes der drei Signale trägt seinen eigenen Bonus bei: bis zu 40 % für Breite, 30 % für Produktführerschaft und 20 % bzw. 30 % für das Engagement in Schwerpunktthemen. Ein Unternehmen kann daher vor Anwendung des Wachstumsfaktors um bis zu 100 % übergewichtet sein.

Der **Wachstumsfaktor** passt die Gewichtung dann entsprechend der Wachstumsgruppe des Unternehmens an – von einer Übergewichtung bei „Schnelles Wachstum & Skalierung“-Unternehmen bis hin zu einer Untergewichtung bei „Wachstum & Verlangsamung“-Unternehmen.

Der Ansatz ist transparent, da jede Gewichtung auf ein bestimmtes Signal zurückgeführt werden kann, und modular, da die Fokus- und Wachstumsfaktoren unabhängig voneinander wirken und für sich allein verstanden werden können. Die Gewichtungen unterliegen zudem den Regeln des Index hinsichtlich Konzentration, Liquidität und Marktkapitalisierung, wodurch das Portfolio diversifiziert und investierbar bleibt.

## Portfoliokontinuität im Kern

Um zu veranschaulichen, wie sich die aktualisierte Methode im Vergleich zum alten Portfolio darstellt, vergleichen wir das nach den neuen Regeln zusammengestellte Zielportfolio für die Neugewichtung im Oktober 2026 mit den bisherigen Indexgewichtungen, die im März 2026 festgelegt wurden.

Der Kern des Portfolios bleibt weitgehend unverändert. Sieben der zehn größten Positionen im neuen Portfolio gehörten bereits im März zu den zehn größten, und die drei größten Positionen – CrowdStrike, Palo Alto Networks und Fortinet – weisen jeweils die gleiche Gewichtung von 7,68 % auf. Die zehn größten Positionen machen zusammen 58,99 % des Portfolios aus.

**Abbildung 2: Die Top 10 der erweiterten Strategie nach der Neugewichtung im Oktober 2026**

| Name des Unternehmens | Gewichtung | Einstufung des Wachstums | Fokus-Gewichtungsfaktor |
|---|---|---|---|
| CrowdStrike Holdings, Inc. | 7,68 % | Schnelles Wachstum & Skalierung | 2,00 |
| Palo Alto Networks, Inc. | 7,68 % | Schnelles Wachstum & Skalierung | 2,00 |
| Fortinet, Inc. | 7,68 % | Schnelles Wachstum & Skalierung | 2,00 |
| Zscaler, Inc. | 6,15 % | Schnelles Wachstum & Skalierung | 1,60 |
| Rubrik, Inc. | 6,15 % | Schnelles Wachstum & Skalierung | 1,60 |
| Varonis Systems, Inc. | 4,92 % | Schnelles Wachstum | 1,60 |
| Netskope, Inc. | 4,92 % | Schnelles Wachstum | 1,60 |
| Cloudflare, Inc. | 4,61 % | Schnelles Wachstum & Skalierung | 1,20 |
| Datadog, Inc. | 4,61 % | Schnelles Wachstum & Skalierung | 1,20 |
| Elastic NV | 4,61 % | Schnelles Wachstum & Skalierung | 1,20 |
| **Top 10 gesamt** | **58,99 %** | | |

Quelle: WisdomTree. Basierend auf der Zielzusammensetzung, die für die Neugewichtung des WisdomTree Team8 Cybersecurity UCITS Index nach Börsenschluss am 23. Oktober 2026 erstellt wurde. **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.**

Die größere Veränderung betrifft die Gewichtung. Das neue Portfolio gewichtet Unternehmen mit einer solideren Positionierung in der Cybersicherheit stärker, wobei diese in allen drei Gruppen des Fokus-Scores einen größeren Anteil ausmachen, insbesondere bei Produktführerschaft und Schwerpunktthemen. Was das Wachstum betrifft, liegt eine größere Gewichtung auf Unternehmen der Kategorie „Schnelles Wachstum & Skalierung“, während die unteren 20 % des Universums nach Wachstums-Score keine Gewichtung erhalten.

**Abbildung 3: Vergleich der neuen und der alten Strategie nach Fokus- und Wachstumsgruppen**

| Gruppen | Neue WCBR-Gewichtung | Alte WCBR-Gewichtung |
|---|---|---|
| **Fokus-Score** | | |
| Breite der Cybersicherheit | 27,14 % | 24,33 % |
| Produktführerschaft | 56,54 % | 49,03 % |
| Schwerpunktthemen | 84,19 % | 76,42 % |
| **Wachstums-Score** | | |
| Schnelles Wachstum & Skalierung | 49,16 % | 41,82 % |
| Schnelles Wachstum | 25,03 % | 25,50 % |
| Wachstum | 9,01 % | 20,54 % |
| Wachstum & Verlangsamung | 16,80 % | 7,99 % |
| Untere 20 % | 0 % | 4,15 % |

Quelle: WisdomTree. Die neuen WCBR-Gewichtungen basieren auf der Zielzusammensetzung, die für die Neugewichtung des WisdomTree Team8 Cybersecurity UCITS Index nach Börsenschluss am 23. Oktober 2026 erstellt wurde. Die alten WCBR-Gewichtungen stellen die Zielzusammensetzung für das Rebalancing im März 2026 dar. **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.**

## Fazit

Cybersicherheit entwickelt sich zu einer grundlegenden Säule der digitalen und KI-Wirtschaft, und die dadurch entstehende Nachfrage wird durch bahnbrechende KI-Entwicklungen neu geprägt. Die überarbeitete Methode behält das bestehende Universum, das Kernkonzept und den Expertenpartner bei, optimiert jedoch die Auswahl und Gewichtung der Unternehmen, um der Entwicklung der Nachfrage Rechnung zu tragen.

**Team8 Disclaimer:** This Article represents the opinions of Team8 Labs Inc. (“Team8”) and is for informational purposes only. You should not treat any opinion expressed by Team8 as a specific inducement to make an investment in any security, but only as an expression of Team8’s opinions. Team8’s statements and opinions are subject to change without notice. Team8 is not registered as an investment adviser under the Investment Advisers Act of 1940, as amended (the “Advisers Act”), and relies upon the “publishers’ exclusion” from the definition of investment adviser under Section 202(a)(11) of the Advisers Act. As such, the information contained in this Article does not take into account any particular investment objectives, financial situation or needs and is not intended to be, and should not be construed in any manner whatsoever as, personalized investment advice. The information in this Article is provided for informational

and discussion purposes only and is not intended to be, and shall not be regarded or construed as, a recommendation for a transaction or investment or financial, tax, investment or other advice of any kind by Team8. You should determine on your own whether you agree with the information contained in this Article. Certain of the securities referenced in this Article may currently, or from time to time, be constituents of an index developed and maintained by WisdomTree Investments, Inc. using data provided by Team8, which has been or will be licensed for a fee to one or more investment funds. In addition, certain officers or employees of Team8 or funds or other persons or entities affiliated or associated with Team8 may hold shares of, be officers or directors of, or otherwise be associated with some or all of the issuers of the securities referenced in this Article or included in such index. Team8 expressly disclaims all liability with respect to any act or omission taken based on, and makes no warranty or representation regarding, any of the information included in this Article.

## WICHTIGE INFORMATIONEN

Dieses Material wurde von WisdomTree und seinen verbundenen Unternehmen erstellt und soll nicht für Prognosen, Research oder Anlageberatungen herangezogen werden. Zudem stellt es weder eine Empfehlung noch ein Angebot oder eine Aufforderung zum Kauf bzw. Verkauf von Wertpapieren oder zur Übernahme einer Anlagestrategie dar. Die geäußerten Meinungen wurden am Herstellungsdatum getätigt und können sich je nach den nachfolgenden Bedingungen ändern. Die in diesem Material enthaltenen Informationen und Meinungen wurden aus proprietären und nicht proprietären Quellen abgeleitet. Daher übernehmen WisdomTree und seine verbundenen Unternehmen sowie deren Mitarbeiter, Führungskräfte oder Vertreter weder die Haftung für ihre Richtigkeit oder Zuverlässigkeit noch die Verantwortung für anderweitig auftretende Fehler und Auslassungen (einschließlich Verantwortlichkeiten gegenüber einer Person aufgrund von Fahrlässigkeit). Die Verwendung der in diesem Material enthaltenen Informationen erfolgt nach eigenem Ermessen des Lesers. **Wertsteigerungen in der Vergangenheit lassen keinen Schluss auf zukünftige Ergebnisse zu.**