Cybersecurity: Wachstumsmarkt mit Substanz

Gleichzeitig wächst die Verwundbarkeit. Die geopolitische Lage – etwa durch den Krieg in der Ukraine – hat gezeigt, wie sehr Staaten, Unternehmen und Infrastrukturen digitalen Angriffen ausgesetzt sind. Cyberwar ist kein Szenario mehr, sondern Realität. Sabotage, Erpressung und Desinformation geschehen zunehmend über digitale Kanäle. Wer in Cybersicherheit investiert, investiert deshalb in Stabilität und Funktionsfähigkeit moderner Volkswirtschaften.

Die Bedrohungslage eskaliert – und mit ihr die Budgets

Cyberangriffe werden häufiger, professioneller und destruktiver. KI-gestützte Schadsoftware, Ransomware-Dienste im Abo-Modell und Angriffe durch staatlich unterstützte Gruppen setzen Unternehmen unter Druck. Das Risiko liegt längst nicht mehr nur bei IT-Abteilungen – ganze Geschäftsmodelle stehen auf dem Spiel.

Laut Cybersecurity Ventures wird der wirtschaftliche Schaden durch Cyberangriffe weltweit auf über 10,5 Billionen US-Dollar jährlich bis 2025 geschätzt. Der globale Markt für Cybersicherheit wächst jährlich um rund 10 Prozent – auf etwa 267 Milliarden US-Dollar bis 2025. Bis 2030 wird ein Volumen von über 500 Milliarden US-Dollar erwartet.

Regulatorik als Wachstumstreiber – von NIS 2 bis DORA

Die zunehmende Bedrohungslage führt auch regulatorisch zu mehr Druck. Die NIS-2-Richtlinie verpflichtet Betreiber kritischer Infrastrukturen in der EU, umfangreiche Sicherheitsmaßnahmen umzusetzen. Mit dem Digital Operational Resilience Act (DORA) steigen auch für Banken, Versicherungen und Vermögensverwalter die Anforderungen: Sie müssen ihre digitale Resilienz systematisch prüfen, dokumentieren und nachweisen.

Die SEC in den USA fordert mehr Transparenz bei Sicherheitsvorfällen, asiatische und lateinamerikanische Staaten ziehen nach. Unternehmen, die diese Standards erfüllen müssen, investieren zunehmend in Cloud-Sicherheit, Notfallwiederherstellung und Compliance-Lösungen. Besonders betroffen sind FinTechs, Kryptoplattformen und kleinere Anbieter – hier steigen die Sicherheitsbudgets oft um über 100 %. Der Cybersecurity Leaders Fonds investiert gezielt in Anbieter, die von diesen Entwicklungen profitieren.

Digitale Souveränität – Europas strategische Antwort

Die EU will unabhängiger von außereuropäischer IT werden. Programme wie „Digitales Europa“ fördern gezielt Technologien wie Künstliche Intelligenz, Cybersicherheit und digitale Infrastrukturen. Rund 1,3 Milliarden Euro sind allein bis 2027 für diese Themen vorgesehen. Ziel ist es, Know-how und Kapazitäten in Europa aufzubauen – und so technologische Souveränität zurückzugewinnen.

Davon profitieren auch europäische Cybersicherheitsfirmen wie Clavister, WIIT oder Secunet. Der Cybersecurity Leaders Fonds berücksichtigt diese Entwicklung gezielt in der Portfolio-Allokation.

Vom Schutz zur Resilienz – neue Anforderungen an IT-Sicherheit

Früher galt: Angriff blockieren. Heute lautet die Devise: Systeme widerstandsfähig machen. Wer nur verhindern will, hat schon verloren – Unternehmen müssen in der Lage sein, Angriffe zu erkennen, zu begrenzen und sich schnell zu erholen.

Gefragt sind:

EDR- und XDR-Plattformen für Echtzeitanalyse

Zero-Trust-Architekturen, die kein Gerät mehr blind vertrauen

Disaster-Recovery-Lösungen zur schnellen Wiederherstellung

Cloud-native Sicherheitskonzepte für hybride Infrastrukturen

Laut Gartner zählen diese Technologien zu den wichtigsten Treibern des Sicherheitsmarktes. Besonders KI-gestützte Erkennungsplattformen wie bei CrowdStrike gelten als Vorreiter. Gartner beschreibt KI dabei nicht nur als Risiko, sondern auch als entscheidendes Werkzeug zur frühzeitigen Erkennung komplexer Angriffe.

Investmentstrategie: Klarer Fokus statt Technologiemix

Im Gegensatz zu breiten Tech-ETFs konzentriert sich der Cybersecurity Leaders Fonds auf Unternehmen aus der Cybersicherheitsbranche. Die Auswahl erfolgt aktiv – mit Fokus auf:

Marktführerschaft in einem klar definierten Segment

Wiederkehrende Erlöse (SaaS) mit hoher Kundenbindung

Globale Skalierbarkeit

Relevanz für kommende Bedrohungsszenarien wie Deepfakes oder kritische Infrastrukturen

Neben den USA liegt ein zunehmender Schwerpunkt auf europäischen Titeln – auch aufgrund geopolitischer Entwicklungen und regulatorischer Nähe.

Track Record und Besonderheiten

Der Fonds baut auf dem erfolgreichen wikifolio Cybersecurity Innovators auf, das seit 2017 über 400 % Wertzuwachs erzielt hat. Seit 2023 steht diese Anlagestrategie als regulierter Publikumsfonds auch professionellen und privaten Anlegern offen.

Ein steuerlicher Vorteil: Die Vorabpauschale wird ausgeschüttet, was eine kontinuierliche Ertragskomponente bietet – im Gegensatz zu thesaurierenden Technologiefonds, bei

denen Anleger rein auf Kursgewinne angewiesen sind.

Warum jetzt investieren?

Cyberkriegsführung ist Realität – Sicherheit wird zur Infrastrukturfrage

Regulierungen machen Cybersicherheit zur Pflicht, nicht zur Option

Neue Technologien wie KI und Quantum Computing erhöhen die Komplexität

Staatliche Investitionsprogramme schaffen Rückenwind für Anbieter

Der Bedarf an leistungsfähigen Sicherheitslösungen wird weiter steigen – und mit ihm das Potenzial für Unternehmen, die diese Lösungen entwickeln. Der Cybersecurity Leaders Fonds bietet Anlegern die Möglichkeit, gezielt an diesem strukturellen Wachstumsfeld zu partizipieren.

Dies ist keine Anlageberatung. Bitte informiert euch vor einer Geldanlage über die Risiken und beachtet unsere Hinweise hier.

Hier kann man den Fonds kaufen. Hier geht es zu den Konditionen.