

21.11.2025

Autor: Ingo Koczwara, CFA

Fondswerkstatt | Cybersecurity – Ehret den Löwen

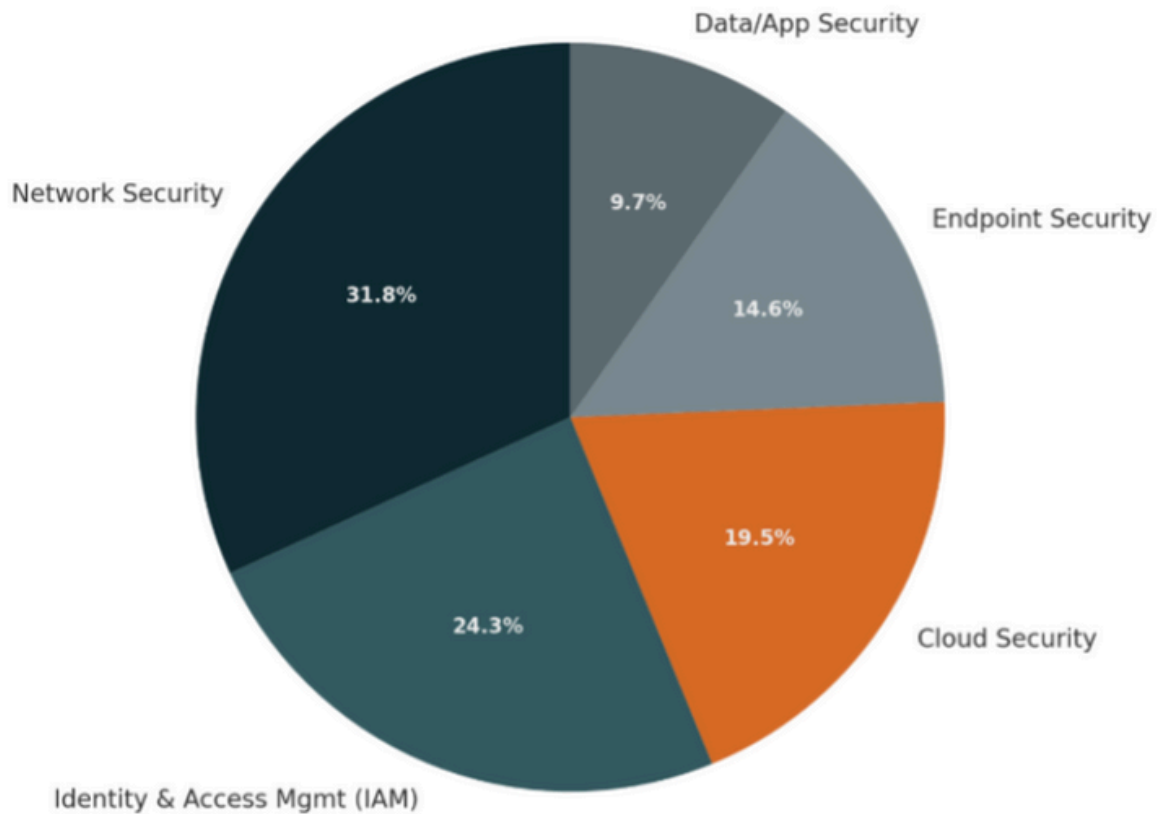
Das Thema Künstliche Intelligenz ist dieser Tage allgegenwärtig. Der einzige begrenzte Faktor für Modellentwicklungen scheint derzeit die Rechenkapazität zu sein, weshalb die großen Technologieunternehmen mehrere 100 Milliarden USD in den Aufbau von Rechenzentren in diesem Jahr investieren. Das weltweit generierte Datenvolumen steigt über die letzten Jahre konstant um etwa 20% pro Jahr. Gleichzeitig werden Datenströme zum zentralen Produktionsfaktor in den Wertschöpfungsketten der Unternehmen. Die Angriffspunkte für Akteure mit schädlicher Absicht vervielfältigen sich dadurch, z.B. in den Bereichen Industrie 4.0, Internet of Things, autonomes Fahren oder vernetzte medizinische Geräte, um nur einige zu nennen. Da ist es nicht überraschend, dass die Anzahl der Cyber-Attacken überproportional um gut 50% pro Jahr steigt.

Der Bibliothekslöwe wacht vor den Eingängen großer Wissensstätten. Er symbolisiert die Idee, dass Wissen kostbar, schützenswert und nur jenen zugänglich ist, die mit Respekt und Neugier kommen. Wie steht es also um die Wachsamkeit des Cybersecurity-Löwen? Und welche Chancen bieten sich für Anleger?

Die Branchenstruktur

Die Cybersecurity-Branche ist in ihrer heutigen Aufstellung sehr fragmentiert. Die sechs in der Grafik dargestellten Hauptkategorien unterteilen sich wiederum in eine Vielzahl von Unterthemen. So mannigfaltig die potenziellen Angriffspunkte sind, so sind es auch die Abwehrmöglichkeiten. Man kann sich das Ganze wie bei einem Haus vorstellen: Gartenzaun, Haustür, Schließsysteme an den Fenstern und Mauern sichern das Gebäude, es gibt aber auch Videokameras, Rauchmelder und Blitzableiter zur Überwachung, und nicht zuletzt Tresore, Feuerlöscher und Fluchtwege für den Fall der Fälle. Idealerweise wird das Sicherheitskonzept von einem Anbieter entworfen und durchgeführt, um ineinandergreifende, ganzheitliche Systeme zu installieren. Dies ist bei Cybersecurity meistens nicht der Fall. Die Branche ist noch jung und sehr zersplittert. So erzielt der Marktführer für Netzwerksicherheit, Palo Alto Networks, gerade mal 9 Mrd. USD Umsatz in diesem Jahr. Gleichzeitig schreitet aber auch die Konsolidierung voran. So hat Palo Alto Networks in diesem Juli die Übernahme des Wettbewerbers CyberArk für 25 Mrd. USD bekannt gegeben.

Für die großen Technologiekonzerne übernimmt das Thema Sicherheit auch eine zentrale Rolle. So erzielt Microsoft schätzungsweise 15% des Umsatzes mit Sicherheitssoftware. Mit der finanziellen Schlagkraft der Big Techs wäre es ein Leichtes, die Konsolidierung der Branche weiter voranzutreiben.



KI und Quantencomputer

Die jährlichen Schäden durch Cyber-Attacken sind schwierig zu schätzen. Das Bundeskriminalamt beziffert den Schaden in Deutschland im Jahr 2024 auf 179 Mrd. EUR, der Branchenverband Bitkom e.V. auf 289 Mrd. EUR. Während der Missbrauch von persönlichen Daten, beispielsweise von Kreditkarten, klar messbar ist, entstehen signifikant hohe Kosten vor allem durch die Störung operativer Abläufe bei Unternehmen. So wurde beispielsweise das Abrechnungssystem des größten US-Krankenversicherers United Health im vergangenen Jahr gestört. In der Folge verzögerten sich Abrechnungen von Ärzten und Krankenhäusern von 190 Millionen Versicherten und brachten so einige Häuser in einen Liquiditätsengpass. Der Gesamtschaden wird auf über 3 Mrd. USD geschätzt. Zur Wiederherstellung wurden dann Spezialisten von Palo Alto Networks hinzugezogen. Von den zahlreichen Beispielen von Cyberattacken ist diese exemplarisch: In die Jahre gekommene Computersysteme bieten eine willkommene Einfallstür für moderne schädliche Programme. Grundlegende Systemanpassungen werden oft erst nach erfolgreichen Angriffen vorgenommen. Eine Kehrseite der Entwicklungen zur künstlichen Intelligenz ist zudem, dass die Programmierung eigener Apps und Codes sehr viel einfacher geworden ist. Interessant wird in dem Zusammenhang auch die Entwicklung von Quantencomputern, mit deren Funktionsreife in 5-10 Jahren gerechnet wird. Theoretisch könnte ein funktionierender Quantencomputer die meisten Internetprotokolle und Sicherheitsmaßnahmen binnen weniger Minuten knacken.

Wie wir investieren

Im Phaidros Funds Schumpeter Aktien ist Cybersecurity ein strategischer Themenblock unseres Anlageuniversums. Wir halten mehrere kleine Positionen in Marktführern der jeweiligen Kategorien, um den Sektor möglichst breit abzudecken: Palo Alto Networks (Netzwerksicherheit), CrowdStrike (Cloud-Security), Fortinet (Endpoint-Security) und ZScaler (Access-Management). Dank der hohen Volatilität gibt es für den aktiven Manager immer wieder Gelegenheiten, Positionen aufzustocken oder abzuschneiden.



Wir sehen also, dass der Cybersecurity-Löwe sich noch viel bewegen muss, um stets ein Stück voraus zu sein. Vielleicht ist seine Flexibilität aber auch der entscheidende Vorteil gegenüber den historischen Vorbildern aus Mörtel und Stein.

DISCLAIMER

Dieser Artikel enthält die gegenwärtigen Meinungen des Autors, aber nicht notwendigerweise die der Eyb & Wallwitz Vermögensmanagement GmbH. Diese Meinungen können sich jederzeit ändern, ohne dass dies mitgeteilt wird. Der Artikel dient der Unterhaltung und Belehrung und ist kein Anlagevorschlag bezüglich irgendeines Wertpapiers, eines Produkts oder einer Strategie. Die Informationen, die für diesen Artikel verarbeitet worden sind, kommen aus Quellen, die der Autor für verlässlich hält, für die er aber nicht garantieren kann.