09. Juni 2021

# Cybersecurity

**Victoria Berggren**
Jürgen Brückner

Frankfurter Vermögen

# Inhaltsverzeichnis

# VORWORT

Aufgrund der digitalen Transformation und dem damit verbundenen exponentiellen Anstieg des Datenvolumens möchten wir das Thema Cybersecurity näher beleuchten. Das Potenzial der Branche ist enorm und wurde durch die Corona-Pandemie und das resultierende Arbeiten von Zuhause weiter angetrieben. Investoren in diesem Sektor wurden in den letzten Jahren reich belohnt. Aber kann dieser Trend bestehen bleiben?

Wir haben uns näher mit dem Thema beschäftigt. Dabei wird schnell deutlich, dass sich die Landschaft rund um Cybersecurity ständig weiterentwickelt. Disruptionen wie Cloud- und Edge-Computing haben die Arbeitswelt, sowie die Art und Weise wie Unternehmen mit Kunden interagieren und Geschäfte abwickeln, verändert. Heute ist es Arbeitnehmern möglich, von überall und von einer beliebigen Anzahl von Geräten auf Geschäftsanwendungen zuzugreifen. Dies führt zu komplexen Sicherheitsrisiken, zudem nimmt die Datenmenge im Internet rapide zu. Gleiches gilt für die Notwendigkeit, alle diese Daten zu schützen.
Die Herausforderungen der Investoren besteht darin, die zukunftsträchtigen Lösungen gegen Cyber-Kriminalität klar herauszufiltern. Dabei die Gewinner zwischen den zahlreichen jungen Unternehmen am Markt zu ermitteln, ist keine leichte Aufgabe.

Dieser Bericht soll dem Leser einen ersten Eindruck über das komplexe Thema Cybersecurity geben. Dabei gehen wir zuerst auf die Frage „Was ist Cybersecurity eigentlich?“ ein und beleuchten danach die wichtigsten Treiber des Sektors. Daraufhin werden die verschiedenen Arten von Cyber-Angriffen beschrieben, sowie die bestehenden Lösungen und deren Wachstumspotenzial erläutert. Zuletzt wird auf die von uns tiefgreifend analysierten und als zukunftsträchtig bewerteten Cybersecurity-Investitionen aufmerksam gemacht.

# 1. WAS GENAU IST CYBERSECURITY EIGENTLICH?

Cybersecurity hat sich in den letzten Jahren zu einem immer lauter werdenden Thema etabliert. Es ist allerdings nicht immer klar, dass Cybersecurity von den Themen der Informationssicherheit und IT-Sicherheit zu trennen ist. Daher folgt nun eine kurze Übersicht, welche die Bedeutung und die Unterschiede verdeutlicht.

• Der Begriff *Informationssicherheit* beschreibt den Schutz von Informationen auf einem Datenträger oder auf Papier. "Informationen" werden dabei als "interpretierte Daten" definiert. Dies bedeutet, dass reine Daten erst nach der Interpretation zu Informationen werden. Ein einfaches Beispiel dafür sind Zahlen, die nach ihrer Interpretation zu Geburtsdaten werden. Die Informationssicherheit zielt darauf ab, diese Informationen vor unbefugtem Zugriff Dritter zu schützen.
• Die *IT-Sicherheit* ist der Teilbereich der Informationssicherheit, der sich auf IT-Systeme und elektronisch gespeicherte Informationen bezieht. Insbesondere zunehmend digital gespeicherte und übertragene Informationen sind einigen möglichen Bedrohungen ausgesetzt: vom unbefugten Zugriff Dritter über Spionage und Datenvernichtung bis hin zu Hackerangriffen. Ziel der IT-Sicherheit ist es, Unternehmen und Organisationen, vor diesen Bedrohungen und den damit verbundenen Schäden zu schützen.
• Die *Cybersecurity* bezieht sich grundsätzlich auf den Bereich der IT-Sicherheit, erstreckt sich jedoch auf den gesamten Bereich des Internets und alle Netzwerke. Viele Daten und mittlerweile auch Anlagen und Maschinen (durch das Internet der Dinge (IoT)) sind über Netzwerke mit dem Internet und untereinander verbunden. Auf Grund dessen muss die Cybersecurity als Ganzes betrachtet werden und auf Netzwerken basierende Anwendungen, Prozesse und Kommunikation berücksichtigen.

Unternehmen sollten sich vor entstehenden Cyber-Bedrohungen schützen und wirtschaftliche Schäden präventiv verhindern. Dafür gibt es zahlreiche Schutzmaßnahmen, die sich stetig weiterentwickeln. Alle Maßnahmen sollten dabei als Teil eines ganzheitlichen Sicherheitskonzeptes betrachtet werden und flexibel auf die Weiterentwicklung von digitalen Angreifern reagieren.

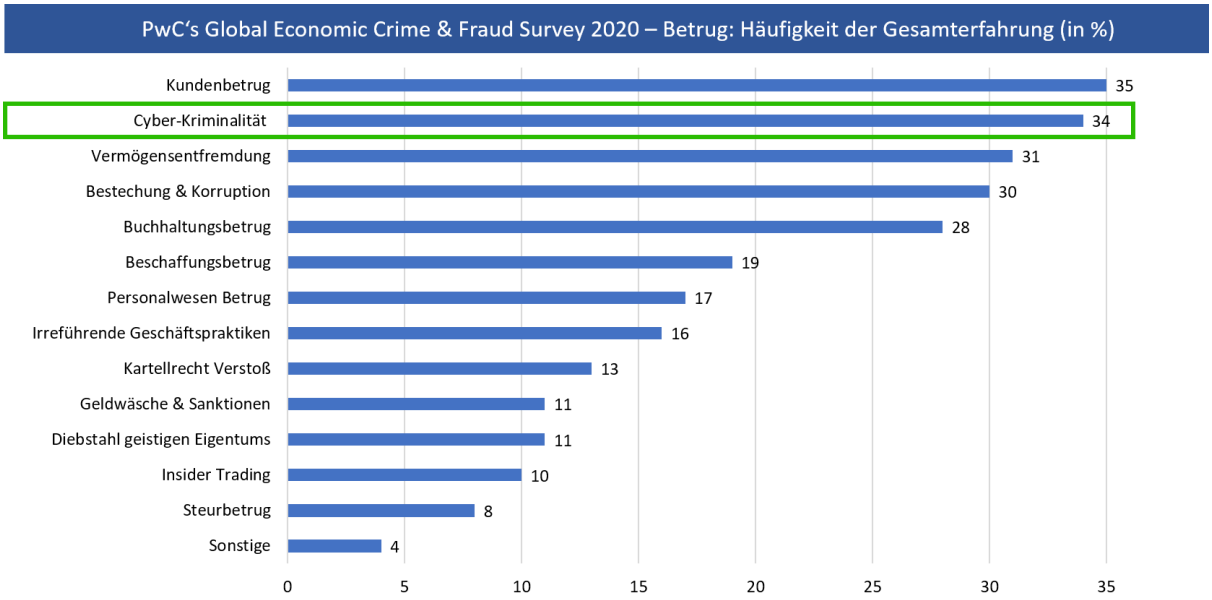
## 2. ANTREIBER DER CYBERSECURITY-INDUSTRIE

WiFi und intelligente Geräte (z.B. Smartphones, Lautsprecher und andere tragbare Geräte) sind mittlerweile allgegenwärtig und nicht mehr wegzudenken. Die Vernetzung von Systemen und Geräten, insbesondere im Zusammenhang mit den führenden Trends wie E-Commerce, soziale Medien, IoT, 5G, Cloud- und Edge-Computing, Big Data, Maschinelles Lernen, mobiler Zahlungsverkehr sowie der vermehrte Einsatz von Robotern und KI-Systeme, erhöhen das Cyberrisiko für Nutzer und Unternehmen.

Sichere Geräte, Verbindungen, Netzwerke und Daten sollten für jeden, der das Internet für geschäftliche und private Aktivitäten nutzt, oberste Priorität haben. Dieser Schutz umfasst eine sich ständig erweiternde digitale Landschaft. Weltweit wird es voraussichtlich bis 2023 29,3 Milliarden vernetzte Geräte geben, gegenüber 18,4 Milliarden im Jahr 2018. Etwa die Hälfte dieser Verbindungen wird eine Vielzahl von IoT-Anwendungen unterstützen (14,7 Milliarden bis 2023 im Vergleich zu 6,1 Milliarden im Jahr 2018). Dies kurbelt das Angriffspotential Dritter weiter an. Daher ist es sowohl für Privatpersonen als auch Unternehmen essenziell den richtigen Cybersecurity-Partner zu finden, der Sicherheitsverletzungen schnell erkennt und beheben kann.

Die Frankfurter Vermögen AG hat sich tiefgreifend mit den Auswirkungen von Cyber-Kriminalität auf Unternehmen beschäftigt. Die nachfolgenden Ausschnitte von verschiedenen Studien verdeutlichen die Relevanz der Industrie und ihr Ausmaß. In der Studie „PwC's Global Economic Crime & Fraud Survey" aus dem Jahr 2020 wurden 5.000 Unternehmen zu Betrugsfällen und deren Häufigkeit innerhalb der Firma befragt. 47 % der befragten Unternehmen hatten während der letzten 24 Monate mindestens einen Betrugsfall gemeldet, was infolgedessen zu rund 42 Milliarden US-Dollar an Verlusten geführt hat. Die Cyber-Kriminalität wurde dabei als zweithäufigster Betrugsfall - nach Kundenbetrug – genannt (siehe Abb. I. auf der nächsten Seite).

Abbildung I.:

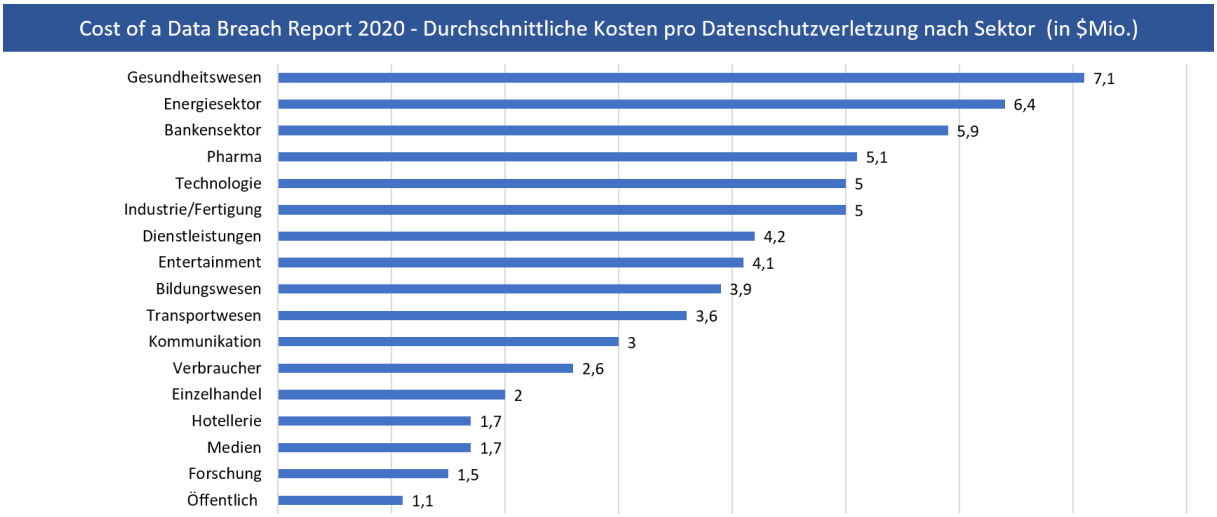



Quelle: PwC's Global Economic Crime and Fraud Survey 2020

Für das potenzielle Wachstum der Cyber-Industrie ist neben der Häufigkeit der Cyber-Betrugsfälle die finanzielle Belastung für Unternehmen ausschlaggebend. Der „Cost of Data Breach Report 2020“ von der International Business Machines Corporation (IBM) beleuchtet dieses Problem genauer. Dabei wurden 524 Unternehmen aus 17 Ländern bezüglich der Kosten pro Datenschutzverletzung befragt. Durchschnittlich lagen die Gesamtkosten im Jahr 2020 weltweit bei 3,86 Millionen US-Dollar pro Datenschutzverletzung. Laut IBM konnten Unternehmen mit einer vollständig implementierten Sicherheitsautomatisierung jedoch 3,58 Millionen US-Dollar dieser Kosten pro Datenschutzverletzung einsparen. In den Vereinigten Staaten operierende Unternehmen hatten mit 8,86 Millionen US-Dollar die höchsten durchschnittlichen Gesamtkosten. Zudem wurden die Gesamtkosten auf Sektorenebene untersucht.

Die kostspieligste Branche ist, wie auch in den Jahren zuvor, das Gesundheitswesen. Mit durchschnittlich 7,1 Millionen US-Dollar pro Datenschutzverletzung ist sie der absolute Anführer der nachfolgenden Abbildung.

Abbildung II.:




Quelle: Cost of a Data Breach Report 2020 | IBM

Die Kosten für einen verlorenen oder gestohlenen Datensatz steigen weiter an, was vor allem durch die digitale Transformation und die Cloud angetrieben wird. Dabei handelt es sich um Anwendungen, Datenspeicherungen und Rechenprozesse, welche meistens außerhalb des Unternehmens in einem zentralen Rechenzentrum in der Ferne durchgeführt werden und über das Internet zugänglich sind. Da viele Unternehmen ihr Kerngeschäft auf digitale Plattformen verlagern, wächst der Bedarf an internen Cybersicherheitsrichtlinien und -initiativen rapide an. Daraus resultiert der Bedarf an externem Know-how wie beispielsweise Cybersecurity-Schulungen für Mitarbeiter. Angesichts des Ausmaßes von monetären und markenbezogenen Schäden, die mit Datenschutzverletzungen verbunden sind, wird Cybersecurity als Geschäftsrisiko und nicht nur als IT-Thema behandelt.

## 3. ARTEN DER CYBER-ANGRIFFE & IHRE ENTWICKLUNG

Ein konkretes Beispiel, welches ein absolutes Horrorszenario für Jedermann darstellt und die möglichen Ausmaße von Cyber-Angriffen verdeutlichen soll, lautet wie folgt: Sie fahren wie jeden Morgen mit dem Auto zur Arbeit. Allerdings fahren Sie ein autonomes Fahrzeug, welches über Künstliche Intelligenz (KI) gesteuert wird. Was passiert nun, wenn Ihr Auto böswillig gehackt wird? Genau diesem Problem hat sich die Europäische Kommission gewidmet, welche Anfang des Jahres einen Bericht zu dem Thema vorlegte. Um böswillige Eingriffe Dritter zu erschweren, soll Cybersecurity ein zentrales Element des Fahrzeugdesigns werden.

IT-Konzepte, Maßnahmen und Richtlinien sowie spezielle Hard- und Software tragen zum Schutz von Systemen und Daten bei. Im Fokus stehen dabei unbefugte Zugriffe Dritter beziehungsweise Hacker, welche über Schadsoftware oder Netzwerke Angriffe vornehmen. Die Attacken erfolgen meistens auf Unternehmen und deren Mitarbeiter. Dabei sind drei Typen von Hackern zu unterscheiden: White-Hats, Grey-Hats und Black-Hats. White-Hat-Hacker dienen der Cybersecurity in der Hinsicht, dass sie nicht zwangsweise negative Absichten verfolgen. Vielmehr weisen sie Unternehmen und deren Kunden darauf hin, dass eine hundertprozentige Sicherheit bei Computern und in Netzen nicht gewährleistet ist. Grey-Hats hingegen geht es vor allem darum, ihre Vorstellung vom freien Zugang von Informationen für Alle zu verbreiten. Dass die Freiheit von anderen dabei verletzt werden könnte, ist ihnen gleichgültig. Lediglich der letzte Typus von Hackern, die Black-Hats, handeln aus kriminellen Gründen. Sie nutzen bewusst Sicherheitslücken aus, um Systeme einzunehmen, zu beschädigen, oder Daten zu entwenden. Ihre Auftraggeber sind dabei häufig Regierungen und Unternehmen. Laut IBM waren rund 52 % der verursachten Datenschutzverletzungen im Jahr 2020 durch böswillige Angriffe verschuldet.

Anhand eines aktuellen Beispiels lässt sich das Ausmaß solch böswilliger Angriffe verdeutlichen: der Ransomware-Angriff (zu Deutsch: Erpressersoftware) auf E-Mail- und Exchange-Server von Microsoft Anfang 2021. Ursprünglich wurde der

Angriff mit einer Hackergruppe, welche Verbindungen zur chinesischen Regierung hat, assoziiert. Allerdings haben auch zahlreiche andere Hacker die Schwachstellen ausgenutzt, um Lösegeld zu fordern und haben nicht, wie zuerst angenommen, aus Spionage-Absicht gehandelt. Diese Art von Erpresser-Angriffen können Betriebsabläufe von Unternehmen stören, indem Hacker in Systeme eindringen, diese von innen abriegeln und erst gegen Lösegeld wieder freigeben. Falls Letzteres nicht eintritt, können große Mengen an kostbaren Daten verloren gehen. Mit rund 300.000 kompromittierten Servern ist der Angriff auf die E-Mail- und Exchange-Server, welche per Internet erreichbar sind, eine der schwerwiegendsten Cyber-Attacken der letzten Zeit. Ein wichtiges Opfer dieses Angriffes war beispielsweise die Europäische Bankenaufsichtsbehörde (EBA). Sie gab bekannt, dass die ausgenutzte Sicherheitslücke mit ihren E-Mail-Servern zusammenhänge. Daher vermuten die Behörden, dass die Angreifer über E-Mails, welche auf diesen Servern gespeichert sind, Zugriff auf personenbezogene Daten erhalten haben. Die EBA schaltete daraufhin als Vorsichtsmaßnahme ihr E-Mail-System kurzfristig ab.

Aber wie kann ein solches Bedrohungspotenzial überhaupt entstehen? Die Antwort darauf ist essenziell, um zu verstehen, was den Cybersecurity-Markt letztendlich antreibt. Es gibt zahlreiche Einfallstore, die Angreifer ausnutzen, um in Netzwerke einzudringen. In diesem Bericht wird auf zwei dieser Einfallstore genauer eingegangen:

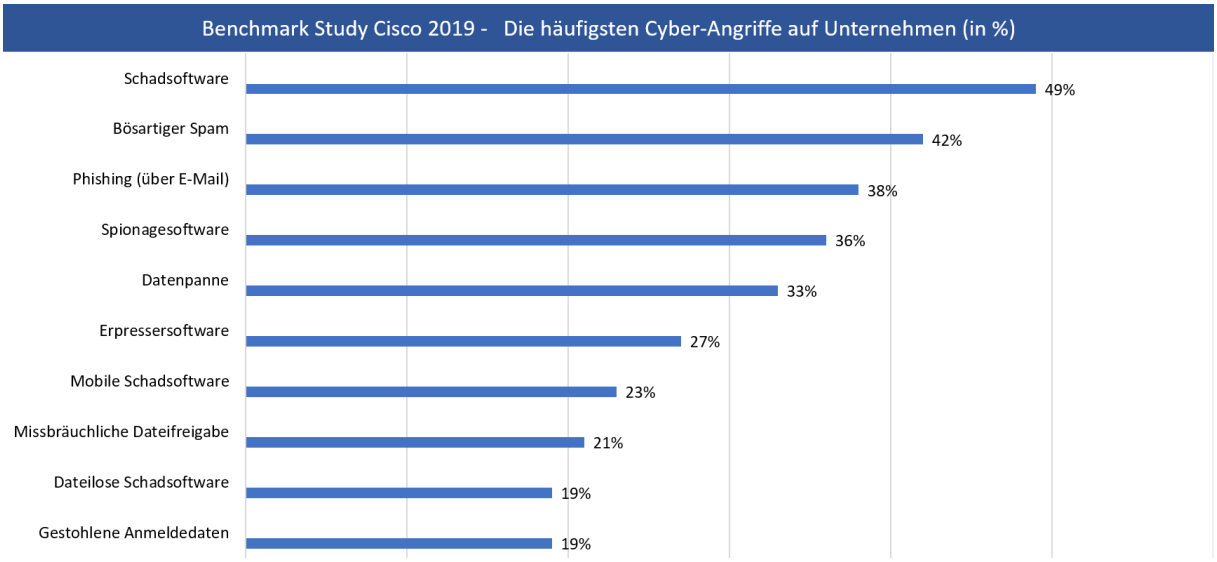
1. Distributed-Denial-of-Service (DDoS): Bei einem DDoS-Angriff versuchen Hacker den normalen Verkehr eines anvisierten Servers, Dienstes oder Netzwerks zu stören, indem das Ziel oder seine umgebende Infrastruktur mit einer Flut von Internet- bzw. Datenverkehr überschwemmt wird. Dadurch werden die Kapazitäten der Netzwerkressourcen gesprengt, wodurch sich ein Tor für Angreifer öffnet. Ziel der Attacke ist meistens die vollständige Störung des normalen Betriebes – eben eine vollständige „Dienstverweigerung“. Die durchschnittliche DDoS Angriffsgröße beträgt 1 GigaBits (Gbps bzw. GigaBytes pro Sekunde und ist ein Maß für die Geschwindigkeit der peripheren Datenübertragung oder der Netzwerkübertragung), was ausreicht, um die meisten Organisationen komplett

offline zu nehmen. Ein aktuelles Beispiel einen solchen DDoS-Angriffs ist die Cyber-Attacke auf die Rechenzentren des IT-Dienstleisters der Volks- und Raiffeisenbanken. Dadurch wurde das Onlinebanking zeitweise vollständig lahmgelegt, was zu Einschränkungen bei Bankkunden geführt hat. Vor allem Ausfälle der Infrastruktur stellen bei DDoS-Angriffen eine große Bedrohung dar. Mehr als die Hälfte der Betreiber sind von solchen Angriffen betroffen. Cybersecurity-Unternehmen sind damit beschäftigt sicherzustellen, dass diese Art von Cyber-Angriffen für Kriminelle finanziell unrentabel ist. Nichtsdestotrotz wird sich die Gesamtzahl der DDoS-Angriffe voraussichtlich von 7,9 Millionen im Jahr 2018 auf 15,4 Millionen bis 2023 verdoppeln (Cisco Annual Internet Report 2018-2023). Dieser starke Anstieg entspricht einer jährlichen Wachstumsrate von 14 % (2018-2023) und birgt somit ein enormes Potential für Cybersecurity Investoren.

2. DNS(-Tunneling): Das Domain Name System (DNS) ist das Protokoll, welches Nutzerfreundliche URLs, wie beispielsweise www.frankfurter-vermoegen.com, in maschinenfreundliche IP-Adressen, wie beispielsweise 192.168.x.x, umwandelt. Das DNS ist damit eine Art Telefonbuch, in dem für jede Domain die dazugehörige IP Adresse gespeichert ist. Da DNS nicht für die Datenübertragung gedacht ist, überwachen viele Unternehmen ihren DNS-Verkehr nicht auf bösartige Aktivitäten. Infolgedessen können eine Reihe von DNS-basierte Angriffe gegen Unternehmensnetzwerke effektiv sein. DNS-Tunneling ist ein Beispiel für einen derartigen Angriff. Es ist eine Methode des Cyberangriffs, bei welcher die Daten anderer Programme oder Protokolle in DNS-Anfragen und -Antworten verschlüsselt werden. DNS-Tunneling enthält oft Nutzdaten, die einem angegriffenen DNS-Server hinzugefügt und zur Steuerung eines entfernten Servers verwendet werden können.

Die Anzahl der Sicherheitsverletzungen und die Gesamtzahl der pro Sicherheitsverletzung offengelegten Datensätze nehmen weiter zu. Erschwerend kommt hinzu, dass die Arten der Bedrohungen immer vielfältiger werden. Die nachfolgende Abbildung (III.) zeigt die am häufigsten auftretenden Arten der Cyberbedrohungen in Unternehmen. Die Grafik von Cisco aus dem Jahr 2019 berücksichtigt die Antworten von 2.909 Unternehmen.

Abbildung III.




Quelle: Anticipating the Unknowns: Chief Information Security Officer (CISO) Benchmark Study, Cisco, March 2019

Laut der Chief Information Security Officer Benchmark-Studie von Cisco beziehen sich zwei der drei wichtigsten Sicherheitsprobleme auf die E-Mail-Sicherheit. Diese ist und bleibt Bedrohungsfaktor Nummer Eins. Die Tatsache, dass es sich bei zwei der Top-10-Angriffe um Insider-Bedrohungen handelt, (missbräuchliche Dateifreigabe und gestohlene Anmeldedaten) zeigt, dass man die Vorgänge innerhalb eines Unternehmens genauso im Auge behalten sollte wie Einwirkungen von außen. Einige Kriminelle können sich einfacher in das jeweilige System einloggen, anstatt einzubrechen.

# 4. CYBERSECURITY-LÖSUNGEN UND IHR POTENZIAL

Cybersecurity bestand traditionell aus einer Hardware, welche als Firewall bezeichnet wird und Teil des Business-Servers ist. Sie überwacht und bestimmt, welche Daten im Netzwerk ein- und ausgehen dürfen und welche blockiert werden müssen, was demnach vergleichbar mit der Sicherheitskontrolle am Flughafen ist. Diese traditionelle Auffassung hat sich allerdings weiterentwickelt. Neben der Firewall wurden in den letzten Jahren zahlreiche weitere Produkte auf den Markt gebracht (siehe Abbildung IV.), die sich gegen die Cyber-Kriminalität richten. Die Cloud wird für diese Entwicklung häufig als Haupttreiber genannt. Die zunehmende Etablierung von Cloud-Anwendungen in der Arbeitswelt hat dazu geführt, dass Mitarbeiter von überall und von beliebigen Geräten auf Geschäftsanwendungen zugreifen können. Dies wurde durch die Corona-Pandemie und das einhergehende „Home-Office“ weiter vorangetrieben. Diese Entwicklung hat, neben vielen positiven Aspekten, zu einem erhöhten Sicherheitsrisiko geführt (siehe Kapitel 5. Exkurs – Cybersecurity und das Corona-Virus).

Abbildung IV.:

| Produktarten | | | |
|---|---|---|---|
| IAAM | Schutz der Infrastruktur | Netzwerksicherheit | Sicherheits-dienstleistungen |
| Privilegiertes Zugangs-Management (PAM) | Endpunkt-Sicherheit | ISP Ausrüstung | Implementierung |
| Identitäts-Zugriffs-Management (IAM) | Cloudbasierte E-Mail/Web-Gateways | Virtuelles Privates Netzwerk (VPN) | Verwaltete Sicherheitsdienste |
| | Sicherheit-Information & Event Management (SIEM) | UTM | Consulting & Training |
| | Cloud Sicherheit | Firewall | Hardware Dienste |
| | Daten-Verlust-Prävention (DLP) | Kein-Vertrauen Netzwerk Zugang (ZTNA) | Versicherungen |
| Sicherer Zugriffsdienst Edge (SASE): Firewall, Cloud, ZTNA und Web-Gateways | | | |

Die Abbildung IV. zeigt die wichtigsten Lösungen gegen Cyber-Kriminalität, die wir identifizieren konnten. Sie baut auf dem aktuellen Industriebericht von Global Market Insights auf. Dabei sind vier Produktbereiche zu unterscheiden: Identitäts-,

Authentifizierungs- und Zugriffsmanagement (auf Englisch: Identity, Authentication and Access Management; kurz: IAAM), Schutz der Infrastruktur, Netzwerksicherheit und Sicherheitsdienstleistungen. Diese Lösungen dienen als Grundlage für die qualitative Analyse potenzieller Cybersecurity-Unternehmen am Markt und folglich für die Aktienauswahl, die am Ende des Berichtes vorgestellt wird. Die grün umrandeten Unterpunkte wurden bewusst hervorgehoben, da hier das größte Wachstumspotential erwartet wird:

- Privilegiertes Zugangs-Management (PAM): Das IAAM stellt sicher, dass Anwendungen und Daten von Unternehmen nur für Mitarbeiter zugänglich sind, die dafür autorisiert sind. Dieser Cybersecurity-Bereich hat in den letzten Jahren an Bedeutung gewonnen und wurde mit einer jährlichen Wachstumsrate von 17 % (2020-2024) bewertet. Das PAM (auf Englisch: Privileged Access Management) stellt eine der beiden Lösungen unter dem Schirm der IAAM Produkte dar. Es ist dafür zuständig, spezifische und hochsensible Konten wie beispielsweise die Anmeldedaten des oberen Managements zu sichern.
- Identitäts-Zugriffs-Management (IAM): Die zweite Lösung im Bereich IAAM ist das IAM (auf Englisch: Identity Access Management), welches darauf ausgerichtet ist, den Mitarbeitern Zugang zu den Systemen des Unternehmens zu gewährleisten. Beide Lösungen werden meistens in Kombination angewendet. Zudem wird erwartet, dass die wachsende Beliebtheit von IAAM-Lösungen in Unternehmen, die fortschrittliche Authentifizierung wie Biometrie und Zwei-Faktor-Authentifizierung nutzen, die Marktnachfrage steigern wird.
- Endpunkt-Sicherheit: Bei der Endpunkt-Sicherheit geht es um den Schutz der Endgeräte, die an Netzwerke angeschlossen sind und dabei meist über die Cloud interagieren. Dazu zählen unter anderem Laptops, Tablets, Smartphones und IoT-Anwendungen. Die Bewertung dieses Cybersecurity-Bereiches überschneidet sich mit dem IoT-Boom. Analysten gehen davon aus, dass die Anzahl an vernetzen Geräten im kommenden Jahrzehnt um mehrere Milliarden ansteigen wird. Hier ist also ein unumgängliches Skalierungspotenzial vorhanden. Ein weiterer Zuspruch für Endpunkt-

Sicherheit resultiert daraus, dass rund 70 % aller Cyber-Attacken ihren Ursprung im Endgerät haben.

- Cloudbasierte E-Mail-/Web-Gateways: Die Gateways beschäftigen sich mit den Übergängen von Daten und Informationen zwischen Cloud und Endgeräten. Sie überprüfen und verschlüsseln die zu übertragenen Inhalte während dem Übergang vom und zum Rechenzentrum. Dies bietet eine große Angriffsfläche, die durch die Corona-Pandemie weiter auf die Spitze getrieben wurde. Seit Februar 2020 sind beispielsweise sogenannte Spear-Phishing-E-Mail-Angriffe um 667 % gestiegen.
- Cloud Sicherheit: Die Cloud Sicherheit umfasst eine Reihe von Maßnahmen, die zusammenwirken, um Cloud-basierte Systeme und Daten zu schützen. Sie ist von entscheidender Bedeutung für Unternehmen, die den Weg in die Cloud-Technologie einschlagen. Dabei kann die Cloud Sicherheit genau auf die Bedürfnisse der Kunden konfiguriert werden und den Verwaltungsaufwand reduzieren. Die jährliche Wachstumsrate wurde mit ca. 26 % (2020-2027) bewertet, was nicht überraschend ist, da rund 90% der Unternehmen weltweit Cloud-basierte Dienste einsetzen.
- Daten-Verlust-Prävention (DLP): DLP-Lösungen (auf Englisch: Data Loss Prevention) ermöglichen den Datenverkehr in Netzwerken zu überwachen, um potenzielle Anomalien zu erkennen. Dies umfasst sowohl die Inspektion von Daten, die per E-Mail versendet werden, als auch die Analyse von Datenströmen sowie die Überprüfung der Datennutzung auf einem verwalteten Endpunkt und die Überwachung von Daten im Ruhezustand auf lokalen Dateiservern oder Cloud-Anwendungen. Wird ein potenzieller Verstoß festgestellt, löst die DLP-Lösung eine Abhilfemaßnahme wie beispielsweise die automatische Erzwingung der Verschlüsselung von Daten, aus. Diese Lösung gegen Cyber-Kriminalität hat sich in größeren Unternehmen bereit stark etabliert. Trotzdem ist mit einem jährlichen Wachstum von rund 24 % (2021-2026) zu rechnen, da insbesondere KMU's als neue Zielgruppe anvisiert werden.
- Virtuelles Privates Netzwerk (VPN): Hierbei handelt es sich um eine Technologie, mit der sich ein sicherer Remote-Zugriff auf interne

Unternehmensanwendungen herstellen lässt. Dabei wird eine Art verschlüsselter Tunnel zwischen dem Netzwerk des Mitarbeiters und dem Netzwerk des Unternehmens hergestellt. Dieses Konzept könnte jedoch in den nächsten Jahren vom ZTNA abgelöst werden, da es besser zu Cloud-basierten Umgebungen passt.

- Kein-Vertrauen Netzwerk Zugang (ZTNA): Das Akronym ZTNA steht für Zero Trust Network Access. Diese Art von Zugang stellt - ebenso wie ein VPN - einen sicheren Remote-Zugriff auf Anwendungen eines Unternehmens dar. Unabhängig vom Netzwerk werden hierbei grundsätzlich alle Mitarbeiter, Anwendungen und Geräte als nicht vertrauenswürdig behandelt. Vor jeglichem Zugriff müssen Dienste und Mittarbeiter überprüft und authentifiziert werden. Mögliche Anwendungsbereiche sind beispielweise das „Home-Office“ sowie Zugänge zu Cloud-basierten und hybriden Umgebungen.
- Sicherer Zugriffsdienst Edge (SASE): SASE (auf Englisch: Secure Access Service Edge) wurde erstmals im Jahr 2019 definiert und ist eine der neuesten Lösungen gegen Cyber-Kriminalität. Mit einer sehr starken jährlichen Wachstumsrate von ca. 120 % (2020-2024) ist es eines der interessantesten Produkte auf dem Markt. Die Besonderheit an SASE ist, dass es das sogenannte Wide Area Networking (WAN) und die Netzwerksicherheitsdienste: Firewall, Web-Gateways und ZTNA zu einem cloudbasierten Servicemodel zusammenwachsen lässt. Damit hat sich ein leistungsstarkes Produkt etabliert, das sich den Herausforderungen der Netzwerkkonfiguration und rasant erweiterten Angriffsflächen stellt.

Als letzte Instanz gegen Cyber-Kriminalität gilt die Verschlüsselung (auf Englischen: Encryption). Dabei gibt es zwei Komponenten: Zum einen ist das die symmetrische Verschlüsselung nach AES-128 und AES-256 (Advanced Encryption Standard) und zum anderen die asymmetrische Verschlüsselung nach RSA (Data Encryption Standard), welche nach den Entwicklern Rivest, Shamir und Adleman benannt wurde. Diese Verschlüsselungen sollen dann greifen, wenn alle anderen Lösungen, die ein Unternehmen gegen Cyber-Angriffe implementiert hat, scheitern.

# 5. EXKURS - CYBERSECURITY UND DAS CORONA-VIRUS

Verschiedene Formen von Cyberkriminalität haben, insbesondere durch das Arbeiten von Zuhause während der COVID-19-Pandemie, rapide zugenommen. Laut Gartner haben ca. 90 % aller Dienstleistungsunternehmen weltweit aufgrund der Pandemie alle ihre Mitarbeiter angewiesen oder ermutigt, aus dem „Home-Office“ heraus zu arbeiten. Dabei sind ungesicherte Internetverbindungen als Haupttreiber für die zunehmenden Cyber-Attacken zu nennen. Dies hat zu Geschäftsunterbrechungen und finanziellen Verlusten auf der ganzen Welt geführt. Im April 2020 meldete Check Point Technologies Ltd., ein Cybersecurity-Unternehmen aus Israel, einen 700-prozentigen Anstieg der Cyberkriminalität während des Coronavirus-Ausbruchs.

Eine weitere Studie von INTERPOL hat ergeben, dass zwischen Februar und März 2020 ein Anstiegt von fast 570 % bei „bösartigen Registrierungen“ zu verzeichnen war. Dabei handelt es sich um die Registrierung von neuen Webseiten, auf welchen Hacker mit bekannten Firmen-Namen werben, um Besuchern auf der Website Informationen zu entwenden oder Malware (auf Deutsch: Schadsoftware) an diese weiterzureichen. Häufiger Bestandteil solcher gefälschten Webseiten ist das sogenannte Phishing, bei welchem Daten – meistens Passwörter - von Besuchern der Website abgefangen und missbraucht werden.

Der Anstieg der Cyberkriminalität aufgrund der erhöhten Nutzung von ungesicherten Internetverbindungen hat sich deutlich auf die Nachfrage von Cybersecurity-Lösungen ausgewirkt. Wie bereits in Kapitel 4 angeschnitten, sind vor allem die virtuellen privaten Netzwerke davon betroffen. VPNs werden von Mitarbeitern genutzt, um den Zugang zum Unternehmensnetzwerk für die Remote-Arbeit, also das Arbeiten aus der Ferne, zu erleichtern. Unter COVID-19-Bedingungen hat sich die VPN-Lösung allerdings als ungeeignet für Unternehmen mit längerfristiger Nutzung erwiesen. Grund dafür ist, dass VPNs Latenzzeiten einführen, die Produktivität beeinträchtigen, schwer zu skalieren sind und Mitarbeitern übermäßigen Zugriff auf interne Ressourcen gewähren können. Gartner prognostiziert, dass deswegen ca. 60 % der Unternehmen bis 2023 von Remote-Access-VPNs auf ZTNA umsteigen werden. Bei einer Zero-Trust-

Implementierung haben Benutzer ausschließlich Zugriff auf Berechtigungen, die für die Ausführung ihrer Arbeitsaufgaben erforderlich sind. Diese Bewegung von VPN auf ZTNA ist ein gutes Beispiel für die sich ständig weiterentwickelnde Cybersecurity-Landschaft.

Laut dem „Cost of Data Breach Report 2020“ von IBM hatte COVID - 19 und das damit einhergehende „Home-Office“ messbare Auswirkungen auf die Kosten der Cyber-Kriminalität für Unternehmen. 70 % der Befragten gaben an, dass die Telearbeit die Kosten von Datenschutzverletzungen erhöht hat. Zudem gaben 76% der Befragten Unternehmen an, dass Telearbeit die Zeit der Erkennung und Eindämmung von Datenschutzverletzungen verlängert.

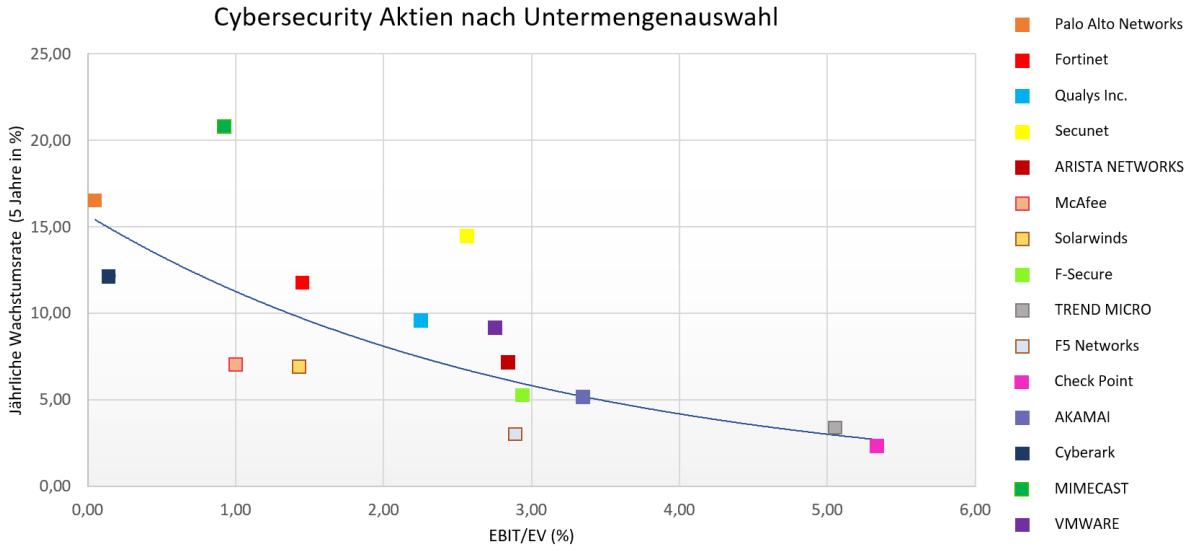
Es gibt zahlreiche weitere Studien, die sich letztendlich alle für eine ähnliche Entwicklung aussprechen: Die Corona-Pandemie hat durch das „Home-Office“ die Angriffsfläche vergrößert und die Cyber-Kriminalität, sowie die damit einhergehenden Kosten für Unternehmen, erhöht. Die Frage bleibt nur, ob diese Entwicklung rückläufig ist oder ob der Trend des „Arbeitens aus der Ferne“ und das erhöhte Cyber-Risiko über ungesicherte Internetverbindungen in dem Ausmaß bestehen bleibt.

# 6. DIE 10 WICHTIGSTEN CYBERSECURITY-UNTERNEHMEN

Das Potenzial für Cybersecurity ist enorm. Eine Studie von Market Insights schätzt den globalen Markt für die Branche bis 2026 auf 400 Milliarden US-Dollar, was einer jährlichen Wachstumsrate (2020-2026) von 15 % entspricht. Innerhalb der Branche gibt es zudem sehr interessante Teilbereiche, die noch stärker wachsen könnten. Die Cybersecurity-Aktien mit den größten Kurschancen werden die sein, welche solide Fundamentaldaten aufweisen und gleichzeitig in den Teilbereichen tätig sind, die ein besonders großes Wachstumspotenzial aufweisen. Die Skalierung deren Produkte wird zudem eine wichtige Rolle spielen.

Die in Kapitel 3 beschriebenen Sicherheitslücken und in Kapitel 4 aufgezeigten möglichen Lösungen gegen Cyber-Kriminalität hat die FV Frankfurter Vermögen AG genutzt, um ein großes Investment-Universum mit rund 45 potenziellen Cybersecurity-Unternehmen aufzubauen. Nach einer Untermengenauswahl sind die Unternehmen, die neben der Abbildung V. gelistet sind, vorerst übriggeblieben. Diese erwarten besonders gute jährliche Wachstumsraten in den kommenden 5 Jahren sowie gute Ertragsrenditen (EBIT/EV).

Abbildung V.:




Nach dieser quantitativen Analyse wurden die Produkte sowie weitere Fundamentaldaten der verbleibenden Unternehmen analysiert. Daraufhin hat die

FV Frankfurter Vermögen AG 10 Cybersecurity-Aktien für potenzielle Investments selektiert (tabellarische Übersicht im Anhang; Stand 17.05.2021):

1. **Palo Alto Networks** (ISIN: US6974351057): Dieses Cybersecurity-Unternehmen wurde 2005 gegründet und hat ursprünglich mit Antivirenprogrammen und der Herstellung von hard- als auch softwarebasierten Firewalls angefangen. Das Unternehmen expandiert stets aggressiv innerhalb der Branche und kauft seit Jahren kleinere Cyber-Unternehmen auf, um die Produktpalette zu erweitern. Diese Strategie hat zu einem guten Umsatzwachstum geführt, ist jedoch aufgrund der Gewinnreduzierung auf Kritik gestoßen. Der CEO Nikesh Arora verteidigt die Strategie und ist davon überzeugt, dass seine Kunden ihre verschiedenen Sicherheitsbedürfnisse aus einer Hand zugespielt bekommen möchten. Das Management handelt entsprechend und erwartet in den kommenden Jahren ein Umsatzwachstum von durchschnittlich 20 % im Jahr. Zudem trug Palo Alto maßgeblich bei der Problembehebung des unter Kapitel 3 beschriebenen Angriffs auf die Microsoft Exchange-Server bei.

2. **Fortinet** (ISIN: US34959E1091): Das Unternehmen wurde 2000 gegründet und zählt neben Palo Alto zu den Playern, welche die Branche disruptiv verändert haben. Der Gründer und CEO Ken Xie verfolgt im Vergleich zu Palo Alto einen konservativeren Expansionsansatz. Er und sein Team erwarten für die kommenden Jahre ein niedriges zweistelliges Umsatzwachstum und ein Gewinnwachstum, was deutlich im zweistelligen Bereich liegt. Sowohl Palo Alto als auch Fortinet sind gut im Bereich Cloud- und Nischensicherheitslösungen aufgestellt und bieten schrittweise neue Dienste wie IAAM, Endpunkt-Sicherheit und SASE an. Sie bilden eine solide Grundlage für Investoren, welche vom Cybersecurity-Boom profitieren wollen.

3. **Arista Networks** (ISIN: US0404131064): Dieses Unternehmen ist seit seiner Gründung im Jahr 2004 ein Favorit von Wachstumsinvestoren im Technologiesektor. Mit ihren innovativen Ansätzen konnte Arista frühzeitig auf den Cloud-Boom aufspringen und den hohen Anforderungen von Cloud-Rechenzentren gerecht werden. Auch wenn die Aktie in den letzten fünf Jahren um mehr als 350 % gestiegen ist, besteht weiterhin Potential für ein organisches

Wachstum. Dafür investiert die Firma aktuell mehr als 20 % ihres Umsatzes für Forschung & Entwicklung und weitet ihre Produktpalette durch Zukäufe von Startups aus.

4. **Check Point** (ISIN: IL0010824113): Dieses israelische Cybersecurity-Unternehmen ist führend im Bereich der Endpunkt-Sicherheit. Zudem ist das Unternehmen gut im Bereich der Cloud-Sicherheit aufgestellt und kann neuere Entwicklungen im Bereich Cybersecurity, wie beispielsweise Zero-Trust Security, bedienen. Mit einer durchschnittlichen Free-Cash-Flow-Rendite von ca. 6 % ist das Unternehmen bereits sehr profitabel und kann eine Umsatzrendite von mehr als 40 % einfahren. Check Point ist attraktiv für Value-Investoren, die ein sehr solides und beständiges Unternehmen mit hervorragenden langfristigen Fundamentaldaten suchen.

5. **Crowdstrike** (ISIN: US22788C1053): Auch wenn dieses Unternehmen bei der Unternehmensauswahl aufgrund eines kleinen negativen EBIT/EV ausgeschieden ist, kann es ein interessantes Investment sein. Dafür gibt es zwei Gründe: Erstens hat das Unternehmen mit einer geschätzten jährlichen Wachstumsrate von 65 % (5 Jahre) das größte Wachstumspotential im Vergleich zu allen 45 Cybersecurity-Unternehmen. Zweitens ist Crowdstrike, ähnlich wie der Marktführer Check Point, hauptsächlich im Bereich der Endpunkt-Sicherheit tätig und somit auf einen Markt mit enormem Skalierungspotential konzentriert. Das Unternehmen konnte vor seinem IPO im Juli 2019 seinen Umsatz jedes Jahr verdoppeln, was sich auch nach Börsengang nicht verändert hat. Für Growth-Investoren bietet sich hier eine gute Chance.

6. **CyberArk** (ISIN: IL0011334468): Dieses Unternehmen konzentriert sich auf PAM und ist führend in dieser Cybersecurity-Nische des Identitäts-, Authentifizierungs- und Zugriffsmanagements (IAAM). Ein weiteres interessantes Unternehmen, welches an dieser Stelle kurz genannt werden sollte, ist Okta (ISIN: US6792951054). Okta ist Marktführer im Bereich IAM, dem zweiten Standbein des IAAM. CyberArk und Okta können ihre Dienste miteinander verknüpfen, um Kunden eine abgerundete IAAM-Sicherheitsstrategie anzubieten.

CyberArk wurde bereits 1999 gegründet und ist laut den Zahlen der letzten Jahre nach wie vor in der Lage den Umsatz zweistellig zu steigern. Den Grund dafür nannte der CEO Udi Mokady in einem Interview, indem er betonte, dass das Identitätsmanagement so lange und so schnell wachsen könne, da identitätsbasierte Vorstöße bei Unternehmen immer präsenter werden und die staatlichen Aufsichtsbehörden diesen mit hohen Bußgeldern entgegenwirken. Diese Abgaben liegen dabei teilweise im neunstelligen Bereich.

7. **Mimecast** (ISIN: GB00BYT5JK65): Dieses britische Unternehmen wurde 2003 gegründet und ist ein weltweit führender Anbieter von Cloud-Sicherheits- und Risikomanagement-Dienstleistungen für E-Mails und Unternehmensinformationen. Das Unternehmen weist eine starke jährliche Wachstumsrate von über 20 % für die kommenden fünf Jahre aus. Durch Zukäufe zahlreicher Startups in den vergangenen drei Jahren konnte Mimecast seine bestehenden Produkte optimieren und die Produktpalette weiter ausbauen. Besonders hervorzuheben ist das starke Management der Firma. Die beiden Gründer Peter Bauer - ehemaliger Microsoft Systems Ingenieur - und Neil Murray kommen aus der Tech-Gründerszene. Ebenso zu nennen ist der wissenschaftliche Leiter Nathaniel Borenstein, welcher zu den ursprünglichen Entwicklern der Multipurpose Internet Mail Extension (MIME) gehörte und den weltweit ersten E-Mail-Anhang im Jahr 1992 verschickte.

8. **Trend Micro** (ISIN: JP3637300009): Dieses japanische Cybersecurity-Unternehmen wurde bereits 1988 gegründet und ist der Weltmarktführer für Server-Sicherheit. Durch stetige Zukäufe von kleineren Cyber-Unternehmen konnte Trend Micro seinen ursprünglichen Fokus vom klassischen Virenschutz auf die cloudbasierte Sicherheitstechnik verschieben. Mit einer Free-Cash-Flow-Rendite von über 5 % ist das Unternehmen bereits profitabel, hat jedoch im Vergleich eine eher solide erwartete jährliche Wachstumsrate von rund 3 % für die kommenden fünf Jahre. Für Investoren, die einen längerfristigen Anlagehorizont anstreben, ist diese Quality-Aktie durchaus interessant.

9. **Qualys** (ISIN: US74758T3032): Das Unternehmen wurde 1999 gegründet und war bis 2019 Marktführer im Bereich Schwachstellen-Management (auf Englisch:

Vulnerability Assessment), bevor es vom Wettbewerber Tenable auf Platz 2 verdrängt wurde. Nichtsdestotrotz ist die Aktie interessant, da das Unternehmen plant mit einer vollumfänglichen Cloudlösung den Markt aus einer neuen Richtung einzunehmen. Wie unter Kapitel 4 beschrieben, ist bei Cloud-Applikationen ein enormes Wachstumspotential zu verzeichnen. Mit einer Gewinnspanne von knapp 20 % und einer Free-Cash-Flow Rendite von 1,81 % ist das Unternehmen, im Gegensatz zu den meisten Wettbewerbern, profitabel. Damit kann das Unternehmen die Investitionsvorhaben aus eigener Kraft finanzieren.

10. **Secunet Security** (ISIN: DE0007276503): Der einzige deutsche Player, der es in die Endauswahl geschafft hat, ist Secunet Security. Dieses Unternehmen ist vor allem auf die Netzwerksicherheit spezialisiert und hat einen Teil der Produktpalette in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelt. Die Produkte des Unternehmens werden unter anderem vom Auswärtigen Amt bei der Übermittlung von Daten genutzt. Zudem trug eine von Secunet entwickelte Software-Applikation maßgeblich zur Auslesung elektronischer Reisepässe bei. Wer schon einmal die automatisierte Grenzkontrolle am Frankfurter Flughafen genutzt hat, wurde durch die Identitätsfeststellung und den drauf folgenden biometrischen Vergleich des Gesichts mit dem Reisepass von Secunet überprüft. Da das Unternehmen auf Produktseite gut aufgestellt ist, ist weiterhin ein organisches Wachstum zu erwarten. Kritisch zu hinterfragen, sind die derzeit vergleichsweise niedrigen Investitionen in Forschung und Entwicklung.

Die FV Frankfurter Vermögen AG hat aktuell vier der genannten Aktien im DigiTrends Aktienfonds – E (DE000A2PWS72). Dazu gehören Palo Alto Networks, Arista Networks, Check Point und Cyberark. Neben diesen reinen Cybersecurity-Unternehmen ist selbstverständlich zu berücksichtigen, dass auch große Unternehmen Cybersecurity-Sparten unterhalten und den genannten Cybersecurity-Unternehmen durchaus den Rang ablaufen könnten. Dazu zählen unter anderem Firmen wie IBM, Cisco, Siemens und Microsoft, welche zum Teil auch in unserem vermögensverwaltenden DUI Wertefinder Mischfonds (DE000A0NEBA1) und in einigen Privatkundendepots vertreten sind.

## FAZIT

Die potenziellen Folgen von Cyber-Attacken sind spätestens nach Lesen dieses Berichtes präsenter geworden: finanzielle Verluste für die betroffenen Unternehmen, wertvolle Datenverluste, Rückschläge für Marken und Ruf sowie erschüttertes Vertrauen der Aktionäre. Die starke Zunahme von Cyber-Verletzungen erfolgt durch alle Sektoren hinweg. Diese Omnipräsenz führt zu einer deutlich steigenden Nachfrage für Cybersecurity-Unternehmen. Das Thema Cybersecurity steckt noch in den Startlöchern und ist keineswegs als kurzzeitiger Trend zu bewerten. Die FV Frankfurter Vermögen AG wird sich langfristig mit dem Thema auseinandersetzen, die Marktgeschehnisse verfolgen, neue Cybersecurity-Lösungen beurteilen und sowohl bestehende als auch neu hinzukommende Cybersecurity-Unternehmen kontinuierlich analysieren. Wir setzen hiermit einen neuen Schwerpunkt für unsere Spezialthemen im Bereich Aktien-Anlage.

# ANLAGE

| Unternehmen: | Produktangebot: | Sicherheit für: | Land: | Umsatz-rendite: | Erw.* Wachstum | KGV 2021e: |
|---|---|---|---|---|---|---|
| paloalto NETWORKS | Cloud Sicherheit, Firewalls, SASE, Antivirenprogramme, SIEM | Staatsführung, Bankensektor Gesundheitswesen, Bildungswesen, Fertigung |  | -4,88 % | 16,60 % | -88,19 |
| FORTINET | IAM, ZTNA, Firewalls, SIEM, Endpunkt Sicherheit, SASE, Web-Gateways | Telekommunikation, Bankensektor, Gesundheitswesen, Bildungswesen, Hotellerie |  | 19,54 % | 12,78 % | 67,25 |
| ARISTA | Cloud Sicherheit, Cloudbasierte Gateways, ZTNA, SASE, DLP, Electronischer Handel | Bankensektor, IT & Telekommunikation, Gesundheitswesen, Bildungswesen |  | 30,50 % | 8,38 % | 36,64 |
| Check Point SOFTWARE TECHNOLOGIES LTD. | Endpunkt Sicherheit, Cloud Sicherheit, Firewall, ZTNA | Bankensektor, Staatsführung, Telekommunikation, Gesundheitswesen |  | 44,03 % | 2,38 % | 18,55 |
| CROWDSTRIKE | Endpunktsicherheit, Cloud Sicherheit, Einsatz von KI, Sicherheitsdienstleistungen | Bankensektor, Staatsführung, Einzelhandel, Gesundheitswesen |  | -10,15 % | 64,73 % | -533,69 |
| CYBERARK | Führend im IAAM, Endpunkt Sicherheit, Cloud Sicherheit | Bankensektor, Einzelhandel, Energiewirtschaft, Gesundheitswese, Staatsführung |  | -1,81 % | 12,44 % | -193,78 |
| mimecast | Cloudbasierte E-Mail/Web-Gateways, Consulting & Training, DLP | Gesundheitswesen, Bankensektor, Justiz, Staatsführung, IT, Fertigung & Bau, Bildungswesen |  | 7,02 % | 17,63 % | 99,33 |
| TREND MICRO | Endpunkt Sicherheit, DLP, SIEM (Cloud-basierte KI-Technologie), E-Mail Sicherheit | IT & Telekommunikation, Gesundheitswesen & Pharma, Transportwesen, Bankensektor |  | 23,55 % | 3,48 % | 27,69 |
| QUALYS ON DEMAND SECURITY | Cloud Sicherheit, Endpunkt Sicherheit, Firewall, SIEM, Web-Gateways | IT, Fertigung & Bau, Transportwesen, Bankensektor |  | 26,63 % | 9,47 % | 41,65 |
| secunet | Netzwerksicherheit, IAAM, E-Mail/Web-Gateways, Cloud Sicherheit, SASE | Bankensektor, Staatsführung, Versicherungswesen, Gesundheitswesen, Transportwesen, Justiz |  | 19,27 % | 14,36 % | 53,71 |

*Erwartetes durchschnittliches jährliches Umsatzwachstum für die nächsten 5 Jahre (CAGR5)

## Quellenverzeichnis:


Bloomberg.com. 2021. *Virtual Private Network (VPN) Market to Reach $75.59 Bn, Globally, by 2027 at 14.7% CAGR: AMR*. [online] Available at: <https://www.bloomberg.com/press-releases/2021-01-12/virtual-private-network-vpn-market-to-reach-75-59-bn-globally-by-2027-at-14-7-cagr-amr> [Accessed 9 May 2021].

Cisco.com. 2021. *Anticipating the Unknowns: Chief Information Security Officer (CISO) Benchmark Study*. [online] Available at: <https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/1963786/2019CISOBenchmarkReportCiscoCybersecuritySeries.pdf> [Accessed 8 April 2021].

Columbus, L., 2021. *2020 Roundup Of Cybersecurity Forecasts And Market Estimates*. [online] Forbes. Available at: <https://www.forbes.com/sites/louiscolumbus/2020/04/05/2020-roundup-of-cybersecurity-forecasts-and-market-estimates/?sh=d7f34df381d7> [Accessed 13 April 2021].

Ibm.com. 2021. *Cost of a Data Breach Report 2020 | IBM*. [online] Available at: <https://www.ibm.com/security/digital-assets/cost-data-breach-report/?mc_cid=5262c1ddf5&mc_eid=0e200ae170#/de> [Accessed 1 June 2021].

Maddison, J., 2021. *Was ist SASE (Secure Access Service Edge)? | Fortinet*. [online] Fortinet. Available at: <https://www.fortinet.com/de/resources/cyberglossary/sase> [Accessed 17 May 2021].

Rivera, K., 2021. *Fighting fraud: A never-ending battle*. [online] Available at: <https://www.pwc.com/gx/en/forensics/gecs-2020/pdf/global-economic-crime-and-fraud-survey-2020.pdf> [Accessed 4 May 2021].

Verified Market Research. 2021. *Cloud Security Market Size | Share | Analysis | Growth and Forecast*. [online] Available at: <https://www.verifiedmarketresearch.com/product/global-cloud-security-market-size-and-forecast-to-2025/> [Accessed 2 June 2021].

Wadhwani, P. and Kasnale, S., 2021. *Cyber Security Market Share, Statistics - Industry PDF 2026*. [online] Global Market Insights, Inc. Available at: <https://www.gminsights.com/industry-analysis/cybersecurity-market> [Accessed 22 April 2021].