

<https://warumnichtanders.at/blog/steigende-hackerangriffe-durch-zunehmende-digitalisierung-cyber-security-wird-zum-megatrend/>

# Steigende Hackerangriffe durch zunehmende Digitalisierung: Cyber Security wird zum Megatrend

Eine gravierende Cyber-Attacke hat kürzlich Hackern Zugriff auf mehr als 250 amerikanische Behörden und Unternehmen verschafft. Mindestens 18.000 Computernetzwerke waren betroffen. Der so genannte „Solarwinds-Hack“ konnte in seinem gewaltigen Umfang nur deshalb erfolgen, weil viele Unternehmen und Behörden sich gegen genau solch einen Einbruch wappnen wollten. Die Angreifer infizierten dabei genau jene Software, die eigentlich die Sicherheit all dieser Netzwerke gewährleisten sollte. Diese wurde bei den arglosen Kunden installiert. Der vermeintliche Schutz wurde zum Türöffner – und das unerkannt für mindestens neun Monate. Die Sache dürfte gewaltige Konsequenzen nach sich ziehen. Eine davon scheint schon jetzt sicher: Die Ausgaben für IT-Sicherheit werden 2021 nochmals massiv steigen. Cyber Security – ein neuer Megatrend.

Das Wachstum der Branche wird für die kommenden fünf bis zehn Jahre sogar auf **über 10 % pro Jahr** geschätzt. Ein Ende ist derzeit nicht absehbar, ganz im Gegenteil. Es kommt ein weiterer, massiver Trend zum Tragen: Die Digitalisierung fast aller Branchen und der beschleunigte Trend zum Homeoffice.

## Schlachtfeld Cyber-Kriminalität



Die Pandemie hat zusätzliche Dynamik in diese Entwicklungen gebracht. Die **rasant zunehmende Digitalisierung** führt dazu, dass sich Cyber-Kriminalität nicht nur stark ausgebreitet und mittlerweile zu einem riesigen Geschäftszweig für das organisierte Verbrechen entwickelt hat. Es ist auch ein Schlachtfeld für staatliche und halb-staatliche Akteure weltweit geworden. Das Thema Cyber-(Un)Sicherheit betrifft dabei jeden: Behörden, Regierungen, Unternehmen und Privatpersonen. **Denn unsere Identität wird – egal ob wir das wollen oder nicht – zumindest für behördliche Zwecke, Konsum, Reisen etc. zunehmend digital.**

# Digitalisierung macht uns immer verwundbarer für Cyber-Angriffe

Neben Diebstahl und politischer sowie industrieller Spionage sind es vor allem **Erpressungen gegenüber Unternehmen und Regierungen**, die derzeit stark zunehmen. Dabei infizieren Hacker mit einer Ransomware (Erpressungssoftware) fremde Computer. Diese sorgt dafür, dass die Mitarbeiter **keinen Zugang mehr zu ihrem Computer** bzw. zu ihren Dateien und Daten haben, es sei denn, man zahlt **Lösegeld**.

Dieses Lösegeld wird oft in Kryptowährungen verlangt, weil man so den späteren Weg des erpressten Geldes nicht mehr nachvollziehen kann. In den letzten fünf Jahren haben sich international Unternehmen etabliert, die neue Angriffsverfahren gegen Entgelt für Auftraggeber durchführen, beispielsweise gegen eine Beteiligung von 30 % des erzielten Umsatzes. Es gibt dafür sogar schon den Begriff CaaS (Crime as a Service – Auftragskriminalität als Dienstleistung).

## Phishing, Spyware und Co



Eine andere beliebte Methode von Cyber-Kriminellen ist das Phishing, also **Diebstahl digitaler Identitäten**. Ähnlich verhält es sich mit dem Begriff Spyware: Dies ist eine Software, die den Computer oder das Handy infiziert und **Informationen über den User und seine Gewohnheiten** sammelt. Meist spioniert diese Software über längere Zeit unerkannt im Hintergrund, sammelt Daten oder überwacht Aktivitäten, um bösartige Aktionen auszulösen, die den Computer des Users betreffen.

## Trojaner besonders tückisch

Besonders heimtückisch sind die sogenannten **Trojaner**. Angelehnt an die berühmte Sage über das trojanische Pferd **installieren sie unbemerkt Hintertüren**, durch die Angreifer in Systeme eindringen, Daten stehlen oder verändern und weitere Schadsoftware installieren können. Der eingangs erwähnte „Solarwinds-Angriff“ gehört in diese Kategorie.

## Geld für Cyber-Sicherheit auszugeben bleibt Firmen nicht erspart

Zu den betroffenen Unternehmen gehören weitere IT-Sicherheitsfirmen, wie etwa FireEye. Dort haben Hacker ein Arsenal von digitalen Einbruchswerkzeugen mitgehen lassen. Unvergessen die Sammlung von **Hackertools des US-Geheimdienstes NSA**, die vor einigen Jahren im Internet veröffentlicht wurde und damit sofort ins Waffenarsenal aller Hackergruppen wanderte. Daran wird ein großes Problem in diesem Bereich deutlich, welches aus Investorensicht für langes Wachstum sorgen wird: ein permanenter Wettlauf zwischen den Schwertern der Angreifer und den Schildern der Verteidiger.



Die Angriffsmethoden werden ständig besser, ebenso die dafür verfügbare Hardware. **Firmen, die sich auf Verteidigung gegen Angriffe spezialisiert haben**, müssen daher ihrerseits ständig Erkennungs- und Abwehrmethoden, Verschlüsselungen und Sicherheitssysteme **weiterentwickeln**. Und ihre Kunden müssen, ob sie wollen oder nicht, **kontinuierlich diese verbesserten Sicherheitssysteme beziehen** und Geld für Cyber-Sicherheit ausgeben.

## Wirtschaftlicher Schaden durch Cyber-Kriminalität steigt

Der wirtschaftliche Schaden durch Cyber-Kriminalität wird inzwischen auf **jährlich über eine Billion Dollar** geschätzt, 50 % mehr als noch vor zwei Jahren. Entsprechend hoch ist die Notwendigkeit für Unternehmen und Behörden, ständig in wirksame Sicherheitssysteme zu investieren.

## Cyber Security im Raiffeisen-MegaTrends-Aktien

Wir haben im Raiffeisen-MegaTrends-Aktien **eine ganze Reihe von Softwareunternehmen** im Portfolio, die **Schutz für Firmen und Konsumenten gegen Cyber-Angriffe** anbieten. Derzeit sind wir konkret in folgende Firmen investiert:

- **Cyberark**: Privileged Account Security
- **Okta**: Identity Management
- **Sailpoint**: Identity and Access Management
- **Splunk**: Log-, Monitoring and Reporting Plattform
- **Trend Micro**: Antivirus Komplettlösungen
- **ZScaler**: Cloud Security

Sind Sie an weiteren MegaTrends interessiert, lesen Sie gerne hier: [Wasserstoff als Klimaretter](#).

# Cyber Security Markt stark im Wachsen

Der Markt für Cyber-Sicherheit wird auf absehbare Zeit stark wachsen, nicht zuletzt durch die fortschreitende Digitalisierung aller Lebensbereiche. Zugleich ist das für die dort tätigen Unternehmen aber keine Einbahnstraße. Vieles basiert auch und gerade in diesem Bereich naturgemäß auf Vertrauen. Unternehmen, die das Vertrauen ihrer Kunden nicht (mehr) rechtfertigen können und mit ihren Lösungen nicht die versprochene Sicherheit bieten, werden sehr schnell von jenen verdrängt werden, die dies besser tun.

Daher ist auch in dieser Branche eine **kontinuierliche sorgfältige Beobachtung und eine gute Unternehmensauswahl** durch das Fondsmanagement vonnöten. Dementsprechend können sich die Positionierungen des Fonds auch jederzeit ändern. Die mit Aktieninvestments grundsätzlich verbundenen Risiken gelten selbstverständlich auch für die Unternehmen, die sich im Bereich Cyber-Sicherheit engagieren.

*Dies ist eine Marketingmitteilung der Raiffeisen Kapitalanlage GmbH, Mooslackengasse 12, 1190 Wien.*

*Stand/Erstelldatum: Jänner 2021*

Die Einschätzungen und Positionierungen stellen eine Momentaufnahme dar und können sich jederzeit und ohne Ankündigung ändern. Sie sind keine Prognose für die künftige Entwicklung der Finanzmärkte oder für den Raiffeisen-MegaTrends-Aktien.

**Veranlagungen in Fonds sind mit höheren Risiken verbunden, bis hin zu Kapitalverlusten.**

Der veröffentlichte Prospekt sowie das Kundeninformationsdokument (Wesentliche Anlegerinformationen) des Raiffeisen-MegaTrends-Aktien stehen unter [www.rcm.at](http://www.rcm.at) in deutscher Sprache bzw. im Fall des Vertriebs von Anteilen im Ausland unter [www.rcm-international.com](http://www.rcm-international.com) in englischer (gegebenenfalls in deutscher) Sprache oder ihrer Landessprache zur Verfügung. Darüber hinaus stehen die Dokumente auch bei der Raiffeisen Bank International AG, Zweigstelle

Frankfurt, Wiesenhüttenplatz 26, 60329 Frankfurt am Main, in deutscher Sprache zur Verfügung. Prospekt und Kundeninformationsdokument (Wesentliche Anlegerinformationen) wurden der Österreichischen Kontrollbank AG übermittelt. Vor einem allfälligen Erwerb den Prospekt lesen.

**Der Raiffeisen-MegaTrends-Aktien weist eine erhöhte Volatilität auf, d.h. die Anteilswerte sind auch innerhalb kurzer Zeiträume großen Schwankungen nach oben und nach unten ausgesetzt, wobei auch Kapitalverluste nicht ausgeschlossen werden können.** Die zur Verfügung gestellten Angaben dienen, trotz sorgfältiger Recherchen, lediglich der unverbindlichen Information, basieren auf dem Wissensstand der mit der Erstellung betrauten Personen zum Zeitpunkt der Ausarbeitung und können jederzeit von der Raiffeisen Kapitalanlage GmbH (Raiffeisen KAG) ohne weitere Benachrichtigung geändert werden. Jegliche Haftung der Raiffeisen KAG im Zusammenhang mit diesen Informationen oder einer darauf basierenden Verbalpräsentation, insbesondere betreffend Aktualität, Richtigkeit oder Vollständigkeit der zur Verfügung gestellten Informationen bzw. Informationsquellen oder für das Eintreten darin erstellter Prognosen, ist ausgeschlossen.

**Raiffeisen Capital Management** steht für Raiffeisen Kapitalanlage GmbH oder kurz Raiffeisen KAG

Bildquelle: shutterstock