FIDUKA
Weitblick und Vernunft für Ihr Vermögen

Veröffentlicht als Gastkommentar (18. Juli 2022) bei

DASINVESTMENT

MARCO HERRMANN ÜBER GELDANLAGEN

HACKERANGRIFFE VERURSACHEN MILLIARDENSCHÄDEN

Wie Anleger auf Cyber-Sicherheit setzen können

Marco Herrmann ist seit 1992 für renommierte Banken und Fondsgesellschaften tätig. Seit 2010 verantwortet er als Geschäftsführer die Anlagestrategie der Fiduka.

Phishing, Würmer, Viren, Trojaner, Identitätsmissbrauch oder Datendiebstahl – Cyber-Kriminalität ist ein alltägliches und wachsendes Problem. Marco Herrmann von der Fiduka Depotverwaltung hält Aktien, die für digitale Sicherheit sorgen, für aussichtsreich.

Gemäß dem Branchenverband Bitkom waren 2020 88 Prozent der deutschen Unternehmen von digitalen Attacken betroffen. Dabei verursachten Cyberangriffe allein in Deutschland zuletzt einen jährlichen Schaden in Höhe von 220 Milliarden Euro. Wird die IT eines Unternehmens lahmgelegt, geht es nicht nur um den finanziellen Verlust, der durch Zahlung von Lösegeld oder einem etwaigen Produktionsausfall (teilweise für Monate!) entsteht. Mindestens genauso schwerwiegend ist, dass auch die Reputation leidet.

Eines der ersten großen Opfer von Cyberkriminellen wurde in Deutschland im August 2016 Leonie. Damals gelang es den Angreifern, sich beim Autozulieferer mittels gefälschter Dokumente und Identitäten als Vorgesetzte auszugeben und eine Überweisung von 40 Millionen Euro auf ein ausländisches Konto zu veranlassen.

Aber nicht nur Unternehmen zählen zu den Hacker-Opfern, sondern auch staatliche Einrichtungen wie zum Beispiel der Deutscher Bundestag, der im Jahr 2015 wohl vom russischen Geheimdienst attackiert wurde. Das Netzwerk des deutschen Bundestags musste ausgetauscht werden. Mehr als 20.000 Rechner wurden mit Trojanern infiziert. Rund 20 Gigabyte Datenmateriell sollen abgeflossen sein.

Selbst vor Krankenhäusern machen die digitalen Erpresser nicht halt. Zuletzt wurde sogar das Handy von Alt-Bundekanzlerin Angela Merkel gehackt, um damit an das Whatsapp-Konto von EZB-Chefin Christine Lagarde zu kommen.

Ein aktueller Fall ist der Diebstahl von rund einer Milliarde Datensätze mit vielfältigen Informationen über chinesische Bürger von der Polizei in Shanghai. Angeblich wurden diese Daten in den vergangenen Tagen für zehn Bitcoin, also rund 200.000 Euro pro Satz verkauft. Offiziell dürfte dies wohl nie bestätigt werden.

Fehlende Schutzmaßnahmen

Corona hat dem Trend zum Homeoffice einen Boost verliehen. Doch der Umzug von der Arbeit in die Wohnung oder ins Haus – das alles musste schnell gehen. Damit erhöht sich auch die Gefahr digitaler Kriminalität. Im Regelfall ist der Schutz des heimischen Computers bei Weitem nicht vergleichbar mit den Sicherheitsvorkehrungen im Büro. Bei den meisten Home-Office-Arbeitsplätzen fehlt beispielsweise bis heute die Installation einer Firewall.

Gleichzeitig hat sich durch das vermehrte Arbeiten von zuhause aus der Datenverkehr erhöht.

Auch auf staatlicher Ebene hat die Gefahr von Cyberangriffen zugenommen. Kriege wie der in der Ukraine werden längst auch digital geführt. Die Russen greifen nicht nur physisch, sondern auch digital die Infrastruktur in ihrem Nachbarland an. Immer wieder muss die ukrainische Cyberverteidigung gezielte Angriffe auf die Stromversorgung abwehren. Dabei bekommt sie unter anderem Unterstützung von Spezialisten von Microsoft.

Es gibt keinen 100-prozentigen Schutz gegen Cyberattacken. Werden eigene Mitarbeiter mit umfangreichen Zugriffsrechten untreu oder wird ihnen zum Beispiel von Kriminellen Gewalt angedroht, ist auch der beste Schutzmechanismus überfordert. Dennoch lassen sich größere Schäden durch eine entsprechende Server-Architektur und Backup-Systeme verhindern. Und wenn alles nicht geholfen hat, müssen IT-Experten retten, was zu retten ist und neue Systeme installieren.

Der Markt für IT-Sicherheit untergliedert sich in sechs Segmente. Der größte Bereich ist die sogenannte Endpoint Security. Hier geht es vor allem um Antivirussoftware und Netzwerksicherheit. Die anderen Segmente sind Nachrichten- und Web-Sicherheit sowie Identitätsschutz, Sicherheit- beziehungsweise Schwachstellenmanagement. Fast alle Marktführer der einzelnen Subsektoren kommen aus den USA und sind an der NASDAQ notiert.

Die IT-Sicherheits-Branche wächst seit Jahren mit hohen zweistelligen Prozentwerten. Das haben auch die Anleger an den an der Börse erkannt und die jeweiligen Aktien in die Depots genommen. Hohes Wachstum, bedeutet in der Regel auch eine hohe Bewertung. Allerdings hat der massive Zinsanstieg der zurückliegenden sechs bis neun Monate die sogenannten Growth-Aktien deutlich unter Druck gesetzt.

Der Prime Cyber Security ETF mit dem vielsagenden Ticker „HACK“ notiert rund 20 Prozent unter seinem Hoch vom November 2021. Gleichzeitig haben sich die Unternehmen operativ weiter positiv entwickelt. Damit ist die Bewertung nun recht attraktiv geworden. Diese Gemengelage bietet eine gute Gelegenheit in diesen langfristigen Trend zu investieren. Da die meisten Unternehmen aus der Branche immer noch relativ klein sind, sollten

Investments bevorzugt über Indexfonds erfolgen, um eine möglichst gute Streuung zu erhalten.

www.fiduka.com

Disclaimer