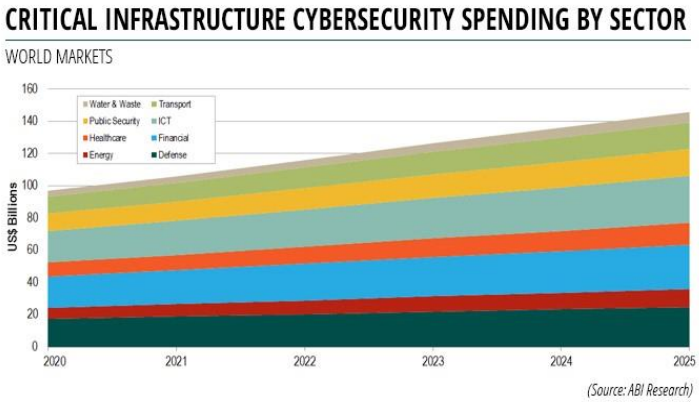
Bedrohung durch Cyber-Kriminelle

Infrastruktur ohne digitale Sicherheit ist nicht mehr denkbar

Mit der fortschreitenden Digitalisierung der Infrastruktur entstehen nicht nur Effizienz- und Komfortgewinne, sondern auch neue Bedrohungen. Kriminelle, Terroristen und Spionageorganisationen nehmen verstärkt Banken und Versorgungsunternehmen ins Visier. Neben finanziellen Risiken können von Hacker-Attacken auch Gefahren für Leben und Gesundheit ausgehen. Die Kapitalmärkte scheinen die Gefahr noch nicht vollständig erkannt zu haben.



Der US-amerikanische Think-Tank ABI Research erwartet allein für kritische Infrastruktur einen Anstieg der Ausgaben für Cyber-Sicherheit auf 150 Milliarden US-Dollar.

Die Vorgehensweise bei GandCrab, einer Organisation von **Cyberkriminellen**, zeigt das Ausmaß der digitalen Gefahr. Es sind keine Einzeltäter, sie haben sich zu regelrechten Unternehmen mit verschiedenen Abteilungen organisiert. Es gibt einen „Kundendienst“, Finanzexperten für die Anlage der Erpressungsgelder, Softwareentwickler sowie auch Experten für die Auswahl von Anschlagszielen. Die „Vertriebsstrategie“: Nach einer Woche verdoppelt sich der Preis für eine Entschlüsselung der Daten. Aber damit nicht genug. GandCrab bietet „**Ransomware as Service**“ über ein Affiliate-Marketing an. Die Ransomware-Betreiber stellen Dritten Malware-Codes zur Verfügung. Für jedes Opfer, das ein Lösegeld bezahlt, teilt der Partner die Einnahmen mit dem Ransomware-Betreiber. Ähnlich wie der nette Influencer eine kleine Umsatzbeteiligung erhält, wenn aufgrund seiner Empfehlung ein Buch oder ein Shampoo im Internet gekauft werden. Nur größer und böser.

„Infrastruktur wurde als lukratives Ziel für Hackerangriffe ausgemacht“

Die beliebtesten Opfer sind aktuell Banken und Versorgungsunternehmen. Während der Corona-Pandemie haben zudem die Anschläge auf das Gesundheitswesen enorm zugenommen. Zuletzt wurden die wichtigsten Öl-Pipelines der USA durch einen **Hackerangriff** stillgelegt. Die Täter beteuerten, ihnen ginge es nur um Geld, man würde keinerlei politische Ziele verfolgen. Bei den Motiven sind die Grenzen fließend. Auch wenn die Akteure nicht direkt im Auftrag eines Staates handeln, so werden ihre Aktionen offenbar gerne geduldet, wenn sie sich nur gegen die richtigen Unternehmen richten. Klar wird bei diesen Hackerangriffen, dass **Infrastruktur** als lukratives Ziel ausgemacht wurde. Deren Unverzichtbarkeit im alltäglichen Leben, oft ohne Ausweichmöglichkeiten, verleiht kriminellen Hackern einen starken Hebel. Auch für politische Akteure könnte es attraktiv sein, unter dem Mantel vermeintlicher Krimineller Sand in das Getriebe westlicher Wirtschaften zu streuen. Es ist davon auszugehen, dass es sich bislang nur um Kostproben dessen handelt, was technisch möglich ist.

Somit ist Infrastruktur ohne digitale Sicherheitslösungen, also **Cybersecurity**, nicht mehr denkbar. Die Kosten von Cyberangriffen steigen mittlerweile erheblich. Für das Jahr 2020 schätzt Cybersecurity Ventures, ein Beratungsunternehmen der Branche, die weltweiten Kosten für Ransomware auf **über 20 Milliarden US-Dollar**. Ein durchschnittlicher Angriff kostet mehr als vier Millionen US-Dollar, wobei die Kosten für Gesundheitsdienstleister in der Regel bei über sieben Millionen US-Dollar liegen. Die Schadenskosten werden für das Jahr 2021 auf 25 Mrd. USD prognostiziert, gegenüber 11,5 Mrd. USD im Jahr 2019 und 325 Mio. USD im Jahr 2015. Es ist daher nicht die Frage, wann eine Cyberattacke stattfindet, sondern ob. In Nordamerika gaben 69% der Unternehmen an, dass sie im Jahr 2020 von Ransomware betroffen waren, gegenüber 57% in Europa. Cybersecurity Ventures schätzt, dass Ransomware bis Ende 2021 **alle 11 Sekunden** ein Unternehmen angreifen wird. Noch immer wird in Unternehmen das Sicherheitsbudget als Kostenstelle betrachtet. Zum Beispiel sehen nur 8% der französischen Unternehmen ihr Sicherheitsbudget als strategisch an, während 56% es jedes Jahr komplett in Frage stellen. Festzustellen bleibt aber, dass die Sicherheitsbudgets generell steigen.

„Der Markt für Sicherheitssoftware wächst um 12,1% p.a. auf 66 Mrd. US-Dollar in 2024“

Das Beratungsunternehmen Gartner Group erwartet, dass der gesamte Sicherheitsmarkt im Zeitraum von 2020 bis 2024 um durchschnittlich 9,1% p. a. wachsen und bis 2024 ein Volumen von 194 Mrd. US-Dollar erreichen wird. Das Segment der **Sicherheitssoftware für Unternehmen** soll um durchschnittlich 12,1% p.a. wachsen und 66 Mrd. US-Dollar bis 2024 erreichen, nach 41 Mrd. im Jahr 2020. Das Segment der Sicherheitsdienstleistungen wird um durchschnittlich 7,9% p.a. wachsen, um bis 2024 auf 90 Mrd. US-Dollar anzuwachsen, von 65 Mrd. US-Dollar im Jahr 2020. Egal ob Energie-, Wasserversorgung oder Transport, sowie auch digitale Infrastruktur wie Rechenzentren, das Rückgrat der zivilisierten Gesellschaft wird durch Vernetzung nicht nur effizienter, sondern gleichzeitig sehr **verletzlich**. In Anbetracht weiter steigender Ausgaben für Digitalisierung bei gleichzeitigem Rückstand der Unternehmen und der öffentlichen Hand beim Schutz dieser Ausgabe vor Cyber-Angriffen wird deutlich, wie hoch das langfristige **Wachstumspotenzial** für IT-Sicherheitsunternehmen ist. Dabei liegen die Bewertungen vieler börsennotierter Anbieter sogar unter denen der IT-Branche.

Michael Gollits ist Vorstand der von der Heydt & Co. AG. Diese ist Portfolioadvisor des OVID Infrastructure HY Income Fonds und des OVID Asia Pacific Infrastructure Equity Fonds. Diese Strategien bieten liquiden Zugang zu Eigenkapital- und Fremdkapitalinvestments in Infrastruktur.

Michael Gollits startete seine Karriere bei F&C Management Ltd in London. 1996 wechselte er zu einer deutschen Privatbank und war dort zuletzt als Bereichsleiter Wertpapiergeschäft verantwortlich für Kapitalmarktresearch, individuelles Vermögensmanagement und verantwortlicher Portfolio-manager einer Fondsfamilie. Von 2005 bis 2013 gestaltete er u.a. den Aufbau einer Privatbank in München und war als Geschäftsführer einer Hamburger Vermögensverwaltung für Kundenportfolios und gemischte Fonds mit Fokus auf Zukunftsthemen zuständig.

Kontaktdaten:
Von der Heydt & Co AG
Michael Gollits
Telefon: +49 (0) 69 / 92 88 48 30
Mail: m.gollits@vonderheydt-co.de

GFD Finanzkommunikation
Joachim Althof
Telefon: +49 152 0205 1413
Mail: althof@gfd-finanzkommunikation.de