Innovative Investmentchancen im dynamischen Markt der IT-Sicherheit

Von Johannes Ries, Gründer und Technologieanalyst bei APUS Capital GmbH

Das internationale Wirtschaftsumfeld unterliegt permanenten Veränderungen und wird geprägt von globalen Megatrends und strukturellen Wachstumstreibern. Kaum ein Megatrend verändert unsere Umwelt so sehr wie die Digitalisierung. Nahezu jedes Gerät wird „intelligent" gemacht und mit eigener IP-Adresse mit dem Internet verbunden. Hierdurch erweitern sich allerdings auch die Angriffsmöglichkeiten für „Online-Kriminelle" geradezu exponentiell. Die Cyberkriminalität hat in den letzten Jahren einen wahren Boom erlebt und ein Ende ist nicht absehbar. Hier zeigt sich die Kehrseite der ansonsten so segensreichen Digitalisierung.

Auch die Coronazeit und der sprunghafte Anstieg von Home-Office Arbeitsplätzen hat die Anfälligkeit von Unternehmensnetzen weiter erhöht. Das gleiche gilt für die deutlich zunehmende Nutzung von Cloudlösungen anstatt von auf den eigenen Rechnern eingesetzter Software.

Auf welchen Wegen gelangen die Online-Kriminellen auf unsere Rechner und Netzwerke?

Die größte Schwachstelle ist und bleibt der Mensch, weil auf seine Schwächen Verlass ist. Obwohl die typischen Gefahrenquellen eigentlich bekannt sind, gelingen noch immer viele Angriffe über fingierte Emails, USB-Sticks oder den leichtfertigen Umgang mit Passwörtern – wie z. B. der gelbe „Post-It Zettel" am Bildschirm. Fairerweise muss man allerdings anmerken, dass die Methoden der Angreifer immer filigraner werden. Trojaner zu erkennen, wird immer schwieriger, da sie sich zum Beispiel als normalen PDF-Anhang „tarnen" oder in Installationsprogrammen für Cloud Dienstleistungen verstecken.

Darüber hinaus können Mitarbeiter natürlich auch bewusst Schadsoftware in das System einschleusen oder Daten stehlen. Die Beweggründe sind dabei unterschiedlich: Die einen möchten sich am Unternehmen für vermeintliches Unrecht „rächen", die anderen einen lukrativen Nebenverdienst erschließen. So versuchen auch Cyberkriminelle, Mitarbeiter von besonders attraktiven Zielfirmen über soziale Netzwerke als gut bezahlte „Handlanger" anzuwerben.

Das zweite Zugangstor in Unternehmensnetze sind oft technische Schwachpunkte in den immer komplexeren IT-Landschaften. Dies beginnt mit der zunehmenden Nutzung von privaten Geräten der Mitarbeiter („bring your own device") und der Tatsache, dass diese Geräte meist nicht dem vollen Zugriff der IT-Abteilung unterliegen. Das gleiche gilt für Laptops von Geschäftspartnern, die bei Besuchen ans Firmennetz angeschlossen werden. Häufig eröffnen auch fehlende Software-Updates oder von außen zugängliche Produktivsysteme (zum Beispiel für den Manager auf Reisen) Einfallsmöglichkeiten für Schadsoftware. Das gleiche gilt für Fernwartungslösungen von Maschinenherstellern. Hier ist eine umfassende Sicherung unumgänglich. Kommt es schließlich zu einem Eintritt von Fremdsoftware, kann sie sich oft schnell verbreiten, da einzelne Netzteile nicht umfassend voneinander getrennt sind oder eine Dokumentation der IT-Infrastruktur schlichtweg nicht vorhanden ist.

Welche verschiedenen Arten von Cyberattacken gibt es und welche Ziele werden damit verfolgt? Die häufigsten Formen von Cyberangriffen lassen sich wie folgt kategorisieren:

Phishing: Diese Art von Attacke dürfte jeder von uns schon einmal erlebt haben. Dabei werden täuschend echt wirkende „Köder-Mails" verschickt, um Personen zur Freigabe persönlicher Daten wie Passwörtern für Bankkonten zu bewegen. In Unternehmen wurden gefälschte Emails von vermeintlichen Vorgesetzten auch schon dazu benutzt, Mitarbeiter zur Überweisung von Geldbeträgen auf Konten von Cyberkriminellen zu bewegen. Der bekannteste und spektakulärste Fall dieser Art ereignete sich 2017 beim Kabelspezialisten Leoni, wo aufgrund einer fingierten Mail 40 Millionen Euro unwiederbringlich auf Konten in Hongkong und China transferiert wurden.

DoS oder DDoS-Attacken: Bei „Denial of Service" oder "Distributed Denial of Service" ist es das Ziel, die Server von Unternehmen oder Behörden durch zahlreiche gezielte Anfragen lahm zu legen. Diese Sabotageangriffe sind zwar wirksam, haben aber oft nur einen kurzfristigen Ausfall der Systeme zur Folge.

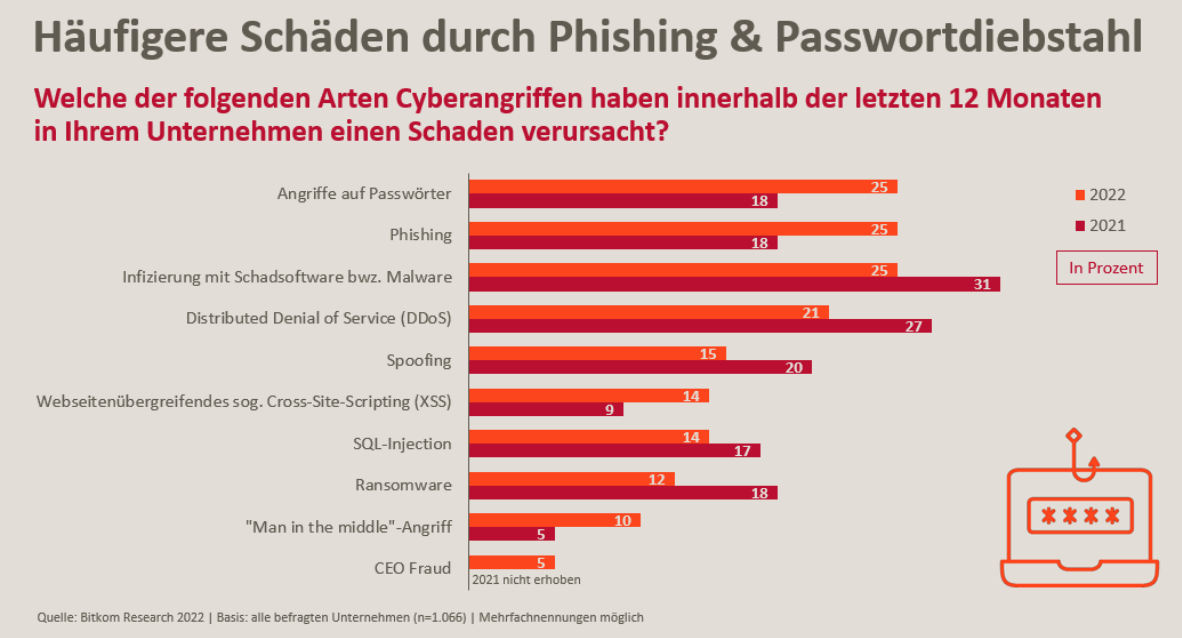
Schadsoftware: Die bekannteste Variante von Schadsoftware sind **Viren.** Dies sind versteckte Programmcodes, die an Dateien angehängt werden. Beim Aufruf der Wirtsdatei wird der zusätzliche Programmcode des Virus mit ausgelöst. Das Virus kann dabei je nach Ausprägung unterschiedliche Vorgänge anstoßen: Daten löschen, das Betriebssystem stören oder Schäden an anderer Software auslösen. Auch kann eine Übertragung von Daten an Dritte erfolgen. Noch gefährlicher, insbesondere für Unternehmen, ist eine andere Form von Schadsoftware – die **Ransomware**. Diese Form der Schadsoftware blockiert den Zugriff auf Systeme und Daten oft ganzer Unternehmen, die nur gegen Zahlung eines Lösegelds (englisch: Ransom) wieder freigegeben werden. Häufig haben die Betroffenen aber keine Gewissheit, ob sie nach der Zahlung eines Lösegeldes wieder Zugriff auf ihre Daten haben. Das macht den Umgang mit einem solchen Angriff besonders schwierig.

Man-in-the-Middle Angriffe: Hierbei versucht ein Angreifer sich unbemerkt zwischen die Kommunikation zweier oder mehrerer Parteien zu positionieren, diese mitzulesen oder auch zu manipulieren. Besonders im Mittelpunkt steht hier die Kommunikation im wirtschaftlichen Leben, zum Beispiel zwischen einer Bank und ihren Kunden. Häufig gelingen diese Angriffe bei der Nutzung ungeschützter W-LAN Hotspots. Um „Man-in-the-Middle Angriffe" zu vermeiden, kommt bei immer mehr Online-Transaktionen das zweistufige Authentifizierungsverfahren zur Anwendung, das zum Beispiel die zusätzliche Eingabe eines per SMS übermittelten Codes zur Identitätsüberprüfung verlangt.

Angriff auf Kennwörter: Passwörter stehen besonders im Interesse von Cyberkriminellen. Neben der Phishing Methode versuchen Kriminelle daher Plattformen mit zahlreichen Nutzern (zum Beispiel Telekommunikations-Unternehmen, Versicherungen, Onlinehändler) auch direkt zu knacken und dort im größeren Stil Passwörter zu entwenden. Da viele Menschen privat und geschäftlich die gleichen Passwörter nutzen, werden diese zum Beispiel wieder zu Angriffen auf Unternehmensnetze genutzt. Der Datendieb nutzt die erbeuteten Kennwörter häufig nicht selbst, sondern verkauft sie über das Darknet an hierauf spezialisierte

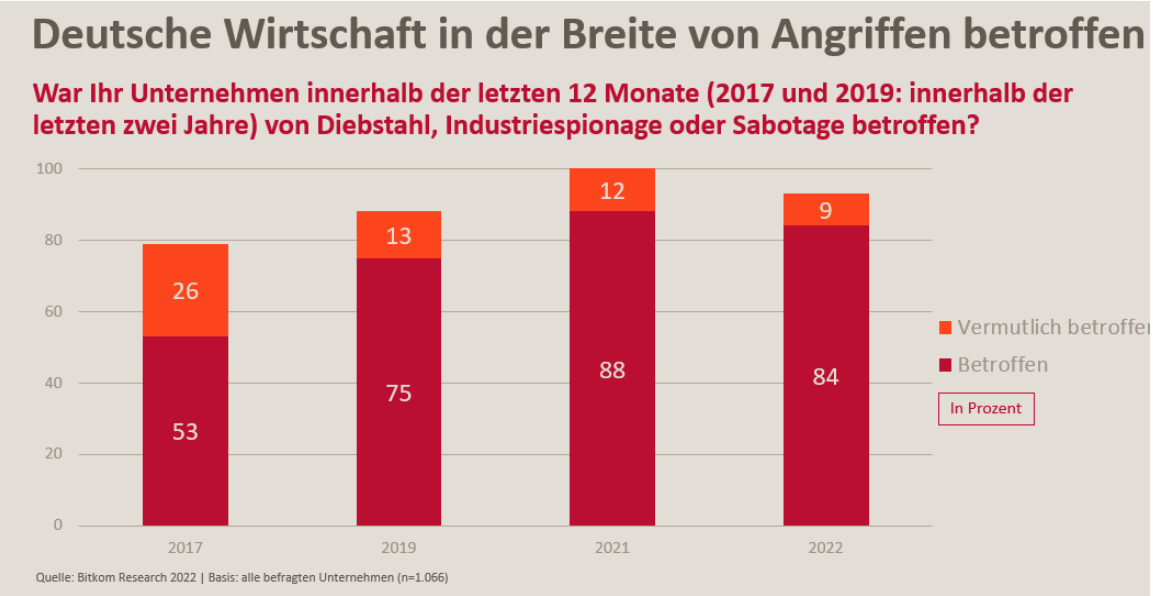
Kriminelle. Angesichts der hohen Anzahl von Betroffenen und des potentiellen Schadens können solche Fälle erhebliche Schadensersatzforderungen nach sich ziehen.

Eine weitere Methode des Angriffs auf Kennwörter ist der umfassende Einsatz von Rechnerleistung, bei der man so lange verschiedene Passwortkombinationen ausprobiert, bis man die passende ermittelt hat. Diese sogenannte „Brute-Force-Methode" ist aber bei langen Passwörtern äußerst zeitaufwendig und damit wenig effizient.



Wenn auch gerade Unternehmen versuchen, sich mit zahlreichen Hard- und Softwarelösungen gegen die Cyberattacken zu wappnen, hat man doch den Eindruck, in der Geschichte vom Hasen und Igel zu sein. Die Kriminellen finden immer neue Wege, in einzelne Endgeräte oder Unternehmensnetze zu gelangen. Genauso wie bei der Abwehr von Onlineangriffen zunehmend künstliche Intelligenz genutzt wird, kommt sie auch auf der anderen Seite bei der Entwicklung neuer, perfiderer Angriffsmethoden zum Einsatz. Es findet quasi ein ständiges „Wettrüsten" statt. Die Anzahl der Angriffe nimmt dabei stetig zu. So entstehen wohl täglich 200.000 neue Varianten von Viren, Trojanern und Würmern. Wie häufig große Netze dabei attackiert werden, zeigt der Online-Sicherheitstacho der Deutschen Telekom, die täglich alleine 450.000 Angriffe auf ihre Locksysteme verzeichnet.

Laut einer Umfrage von Bitkom, dem Branchenverband der deutschen Informations- und Telekommunikationsbranche unter deutschen Unternehmen waren 84% von ihnen im Jahr 2022 von Datendiebstahl, Industriespionage und Sabotage betroffen – deutlich mehr noch als 2017, wo die Quote nur bei 53 Prozent lag.



Die Angriffe verlagern sich dabei immer mehr auf den digitalen Bereich. 45 Prozent der befragten Unternehmen befürchten inzwischen, dass Cyberattacken ihre geschäftliche Existenz bedrohen können. Ein dramatischer Anstieg zum Vorjahr, als nur 9 Prozent diese Befürchtung hatten.

Das Problem verschärft sich, da in der Cyberkriminalität innerhalb weniger Jahre professionelle Strukturen entstanden sind. So waren 2022 bereits mehr als die Hälfte aller Attacken auf Unternehmen auf professionelle Gruppierungen zurückzuführen, nach nur 21 Prozent im Jahr 2019! Hier hat sich eine arbeitsteilige kriminelle Industrie gebildet, die über das Darknet kommuniziert. So gibt es fokussierte Malware-Entwickler, Dienstleister für das Testen und Verbreitung der Schadprogramme und Spezialisten für das Eintreiben von Lösegeldern oder das Verkaufen gestohlener Daten. Die Erlöse werden unter den Beteiligten aufgeteilt. Häufig erfolgen die Taten auch im Auftrag Dritter. Man könnte analog zu den Trends im Softwarebereich auch von einer Entwicklung hin zum **„Crime as a Service"** sprechen.

Vor dem Hintergrund des immer professionelleren Vorgehens der Angreifer stiegen die Schadenssummen in den letzten Jahren dramatisch an. Sie haben sich laut der Umfrage des Bitcom alleine in Deutschland in nur fünf Jahren auf über 200 Milliarden Euro pro Jahr vervierfacht. Der Schaden entsteht dabei nicht nur aus dem möglichen Stillstand der IT-Systeme oder der nur bedingten Handlungsfähigkeit des Unternehmens. Das weitaus größere Risiko sind bleibende Umsatzeinbußen durch Marktanteilsverluste, plagiierte Produkte, Schadensersatzklagen und nur schwer wieder zu behebende Imageverluste. Viele Unternehmen versuchen daher, die Attacken nicht öffentlich werden zu lassen und geräuschlos intern zu lösen. Aufgrund der erheblichen Auswirkungen auf die Lieferfähigkeit und Erreichbarkeit ist dies jedoch oft nicht möglich. So waren alleine in den letzten Monaten in Deutschland so bekannte Namen wie Metro, Aurubis, Hipp, Knauf, die Deutsche Presse Agentur oder Continental von Cyberattacken betroffen. Die Angreifer fokussieren sich dabei nicht nur auf kommerzielle Institutionen. So wurden 2022 auch der Caritasverband München, die IHK, der TÜV-Nord oder das Fraunhofer-Institut in Stuttgart von Online-Angriffen heimgesucht. Selbst führende Firmen aus dem IT-Bereich wie die Software AG oder der französische IT-Dienstleister Sopra-Steria wurden in den letzten Jahren Opfer. Bei Sopra-Steria alleine entstand dabei ein Schaden von 50 Millionen Euro.

202 Milliarden Euro Schaden pro Jahr

Wodurch sind Ihrem Unternehmen innerhalb der letzten 12 Monate Schäden im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage entstanden?

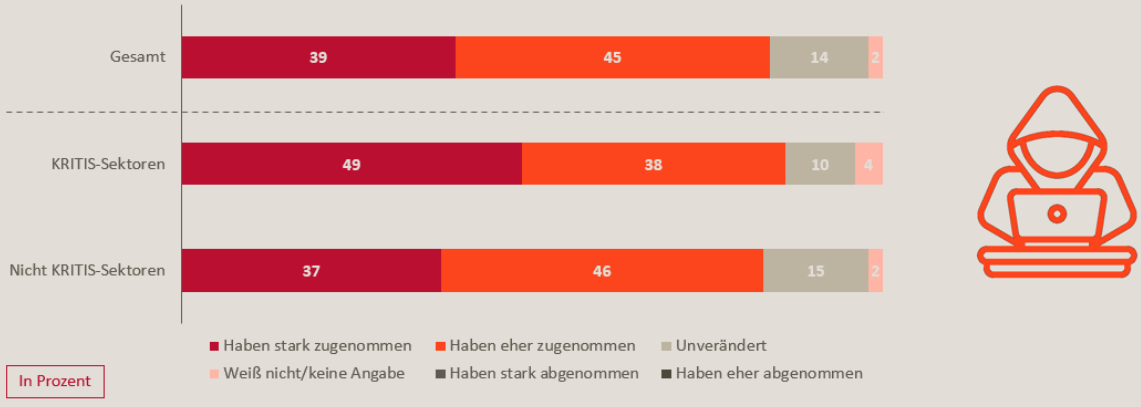
Schaden durch…	Schadenssummen in Mrd. Euro (2022)	Schadenssummen in Mrd. Euro (2021)	Schadenssummen in Mrd. Euro (2019)	Schadensummen in Mrd. Euro (2017)
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	41,5	61,9	13,5	5,3
Erpressung mit gestohlenen Daten oder verschlüsselten Daten	10,7	24,3	5,3	0,7
Datenschutzrechtliche Maßnahmen (z.B. Information von Kunden)	18,3	17,1	4,4	3,2
Patentrechtsverletzungen (auch schon vor der Anmeldung)	18,8	30,5	14,3	7,7
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	41,5	29	11,1	8,6
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	21,1	22,7	11,1	3,5
Imageschaden bei Kunden oder Lieferanten / Negative Medienberichterstattung	23,6	12,3	9,3	7,7
Kosten für Ermittlungen und Ersatzmaßnahmen	10,1	13,3	18,3	10,6
Kosten für Rechtsstreitigkeiten	16,2	12,4	15,6	5,5
Höhere Mitarbeiterfluktuation / Abwerben von Mitarbeitern	-	-	-	2,2
Sonstige Schäden	0,9	0	<0,1	<0,1
Gesamtschaden pro Jahr	**202,7**	**223,5**	**102,9**	**54,8**

Quelle: Bitkom Research 2022 | Basis: alle befragten Unternehmen, die in den letzten 12 Monaten (2019: 2 Jahren) von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (2022: n=899; 2021: n=935; 2019: n=801) | Mehrfachnennungen möglich

Dramatische Auswirkungen können auch Angriffe auf staatliche Institutionen, Städte und insbesondere auf die kritische Infrastruktur haben. Die medienwirksame Attacke auf den Deutschen Bundestag in 2015 war dabei noch vergleichsweise harmlos, ebenso der Ausfall von Informationstafeln der Deutschen Bahn in 2017. Der Hackerangriff, der Mitte 2021 die öffentliche Verwaltung des gesamten Landkreises Anhalt-Bitterfeld traf, hatte da schon eine andere Dimension. Zeitweise konnten keine Gehälter ausgezahlt, Kraftfahrzeuge zugelassen oder Sozialhilfen angewiesen werden. Am Ende war ein Schaden von 1,5 bis 2 Millionen Euro entstanden.

Kritische Infrastruktur rückt in den Fokus von Cyberangriffen

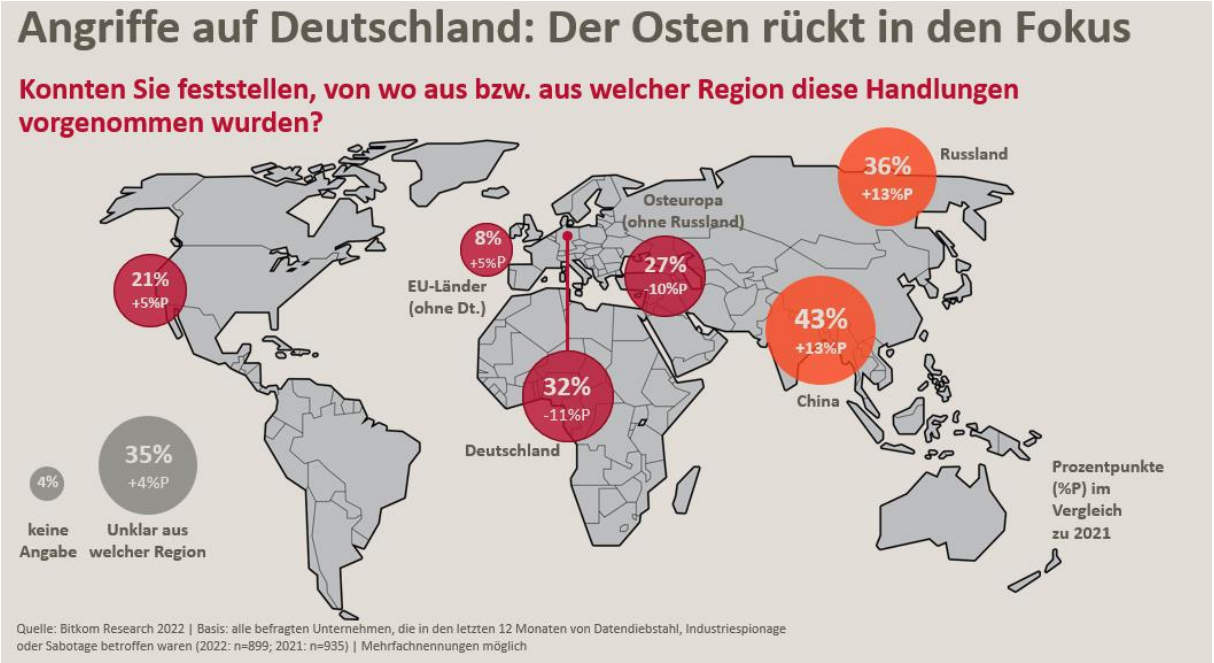
Wie hat sich die Anzahl der Cyberattacken auf Ihr Unternehmen in den vergangenen 12 Monaten entwickelt?



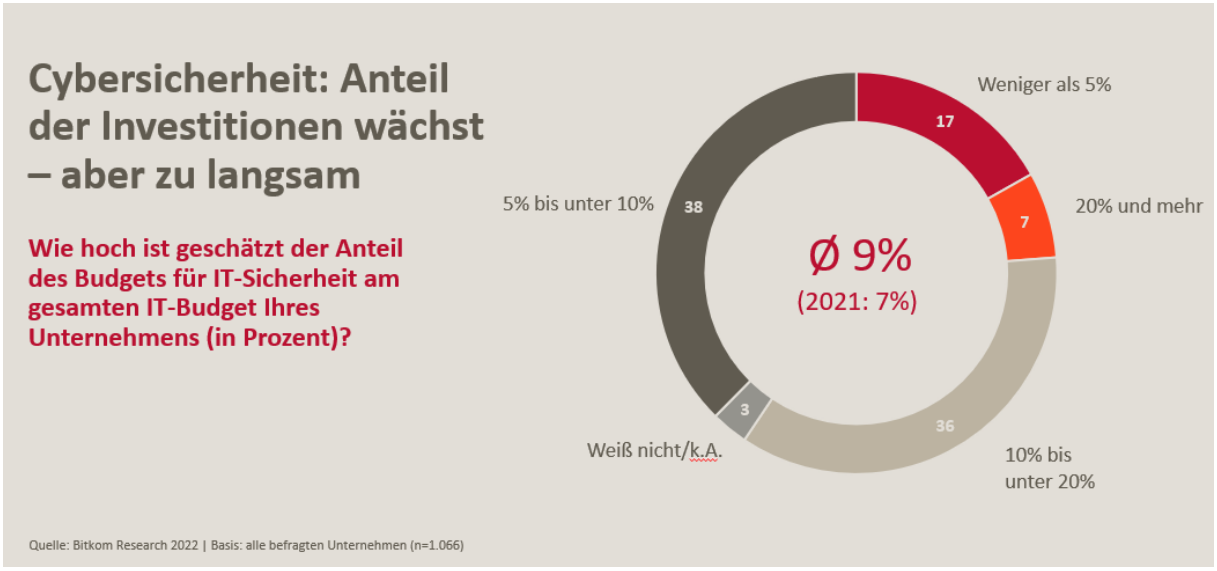
Quelle: Bitkom Research 2022 | Basis: alle befragten Unternehmen (n=1.066)

Hier droht wohl in Zukunft noch größeres Ungemach! Die militärischen Cyberaktivitäten autoritär regierter Länder wie Russland und China könnten vor dem Hintergrund des Ukraine-Kriegs und eines möglichen Konflikts um Taiwan völlig neue Dimensionen annehmen. So beobachteten deutsche Unternehmen bereits seit 2021 eine merkliche Zunahme der Angriffe aus beiden Ländern. Nicht

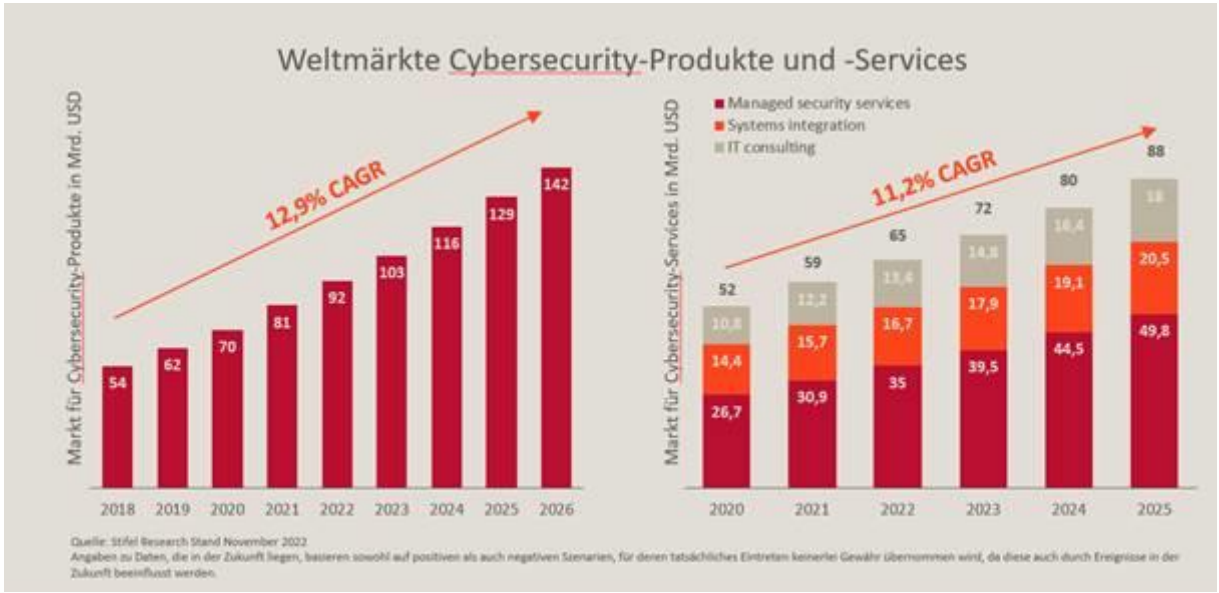
völlig unberechtigt sind daher Befürchtungen, dass aus dieser Richtung großflächige Angriffe auf Stromnetze, Wasserversorgungen oder Bahnnetze erfolgen könnten, zumal diese Netze oft nur unzureichend gesichert sind. Darüber hinaus arbeiten die staatlichen Angreifer auch vermehrt mit den im Darknet organisierten professionellen Cyberkriminellen zusammen. So werden direkte Aufträge für Attacken erteilt oder Daten, die die Kriminellen aus Attacken erbeutet haben, von staatlichen Stellen dieser Länder erworben. Wie es Thomas Haldenwang, der Präsident des Bundesamts für Verfassungsschutz, formulierte: „Die Grenzen zwischen kriminellen Hackern und staatlichen oder halbstaatlichen Stellen verschwimmen zunehmend".



All dies zeigt, dass durch die umfangreiche Digitalisierung und Vernetzung und die damit ansteigenden Bedrohungen auch ein stark wachsender, lukrativer Markt zur Abwehr dieser Gefahren entsteht. Deutsche Unternehmen verwendeten im Vorjahr rund 7% ihrer IT-Ausgaben für die Cybersicherheit. Dieser Anteil wird laut der Bitcom-Umfrage in 2022 angesichts der gestiegenen Bedrohungslage auf 9% steigen. Fachleute halten auf mittlere Sicht sogar eine Quote von 15-20% für nötig.



Der Markt für Cybersicherheitssoftware, -hardware und Dienstleistungen war 2021 weltweit bereits 140 Milliarden US-Dollar groß. Angesichts der aufgezeigten Trends soll er die kommenden fünf Jahre um jeweils 12 Prozent wachsen. Damit würde der Markt in 2026 bereits rund 230 Milliarden Dollar groß sein. Dieses Wachstum könnte angesichts der geopolitischen Situation und einer damit verbundenen zunehmenden Bedrohungslage noch zu niedrig geschätzt sein.



Der Cybersecurity-Markt ist damit ein besonders gutes Beispiel, wie die aktuellen Krisen neue Investmentchancen eröffnen oder bereits attraktive Wachstumsbereiche weiter befeuern können. Die extremen Lieferprobleme und die Energiekrise werden nicht nur den Markt für alternative Energielösungen und die Digitalisierung der westlichen Wirtschaft antreiben. Auch der ohnehin bereits prosperierende Markt für IT-Sicherheitslösungen erfährt weitere Belebung. Außerdem scheint eine umfassende Konsolidierung angesichts von alleine über 3.000 Softwareanbietern anzustehen. Gerade kleinere Unternehmenskunden wünschen sich immer mehr Lösungen aus einer Hand, beziehungsweise möchten

angesichts der enormen Dynamik und Komplexität des Themas ihre IT-Sicherheit aussourcen. Es entstehen daher auch Konzepte wie „Cybersecurity as a Service", die für die entsprechend positionierten Anbieter erhebliche Wachstumspotentiale bieten.

Das Team der APUS Capital GmbH beschäftigt sich intensiv mit dem Thema Cybersecurity. Sowohl in unserem APUS Capital ReValue Fonds als auch in unserem APUS Capital Marathon Fonds finden sich wachstumsstarke innovative Einzelwerte, die vom Trend zu Cybersecurity profitieren. Zwar stammen die meisten großen Anbieter in diesem Bereich aus den USA oder Israel, es finden sich aber auch unter den europäischen Unternehmen genug attraktive Anlageziele. Neben Softwaregesellschaften profitieren auch europäische IT-Serviceunternehmen, Halbleiterhersteller und Telekommunikationsausrüster von der stark steigenden Nachfrage nach IT-Sicherheit. Zudem könnten hier in den kommenden zwölf Monaten einige spannende Börsengänge oder Übernahmen anstehen. Aktien aus dem Bereich Cybersecurity werden in Zukunft einen wichtigen Baustein darstellen, um vom beschleunigten Wandel unserer Welt zu profitieren.

Kurzvita:

Johannes Ries, ist Gründer und Technologieanalyst der APUS Capital GmbH. Der gebürtige Rheingauer hat den Aktienmarkt sein gesamtes Berufsleben lang begleitet. Ende der 80er Jahre begann er als Finanzanalyst bei der Commerzbank. Er spezialisierte sich als Analyst auf Technologiewerte und weitete seine Expertise von 1998 bis 2010 als weltweit tätiger Buy-Side-Analyst aus. Zahlreiche Auszeichnungen belegen sein tiefes Verständnis für die Technologiebranche. Im Jahr 2011 gründete er mit seinem langjährigen Kollegen Harald Schmidt die APUS Capital GmbH, die zwei Aktienfonds initiiert hat. Diese tätigen Investments in Gesellschaften, die man als Gewinner des Wandels identifiziert, den APUS Capital ReValue Fonds und den APUS Capital Marathon Fonds.

Über APUS Capital GmbH

Die APUS Capital GmbH ist eine Inhabergeführte Frankfurter Investment - Boutique. APUS Capital wurde 2011 gegründet, um Anlegern fokussierte und klar strukturierte Fondskonzepte anzubieten. Unsere starke Überzeugung ist, dass man mit gezielten Aktieninvestments langfristig überdurchschnittliche Erträge erzielen kann. Mit einem 7-köpfigen Team mit langjähriger Erfahrung, kontinuierlichen Management-Kontakten und unserer Fokussierung auf fundamentale Unternehmensanalyse, identifizieren wir die Gewinner von morgen. Die APUS Capital GmbH fungiert als Berater für den APUS Capital ReValue Fonds mit ca. 76 Millionen Euro Assets under Management (AuM) und für den APUS Capital Marathon Fonds mit ca. acht Millionen Euro AuM.

Mehr Informationen unter: https://apuscapital.de/