invest 02 2022

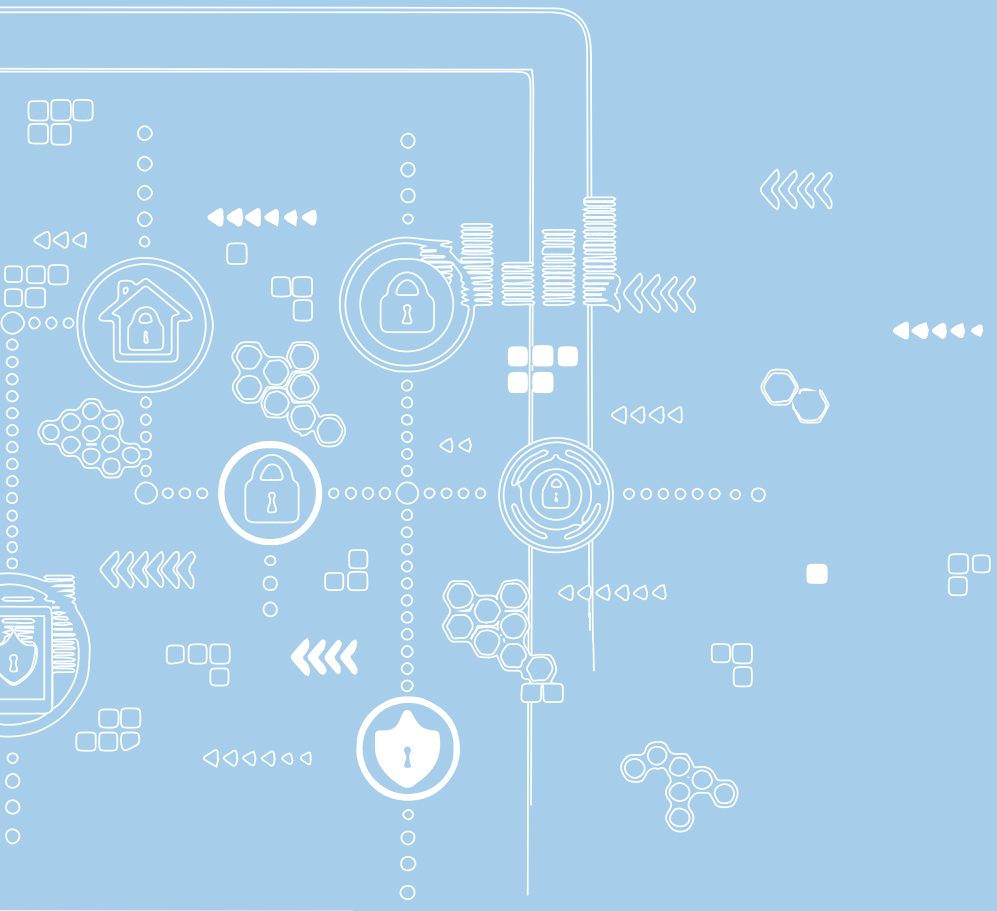
Ihre Anlageperspektiven

Sicherheit als höchstes Gut

Im Visier der Hacker

acrevis spektrum®

acrevis
Meine Bank fürs Leben



« Die Angreifer werden immer professioneller und es wird immer schwieriger, sich adäquat zu schützen. »

Aussage aus dem Interview mit Ivan Bütler, Spezialist Cybersicherheit, Interview auf Seite 9

Sandro Schibli
Bereichsleiter Private Banking

Geschätzte Leserin,
geschätzter Leser

Sie in bewegten und bewegenden Zeiten mit einem kaum direkt fassbaren Thema zu konfrontieren – auch das noch, ist man geneigt zu urteilen. Das noch grössere Wagnis ist jedoch, das vorliegende Thema Cybersicherheit zu verniedlichen. Denn nicht nur die Generation Z lebt, davon umklammert, in einer technologisch geprägten und vernetzten Welt. Auch Sie und ich können unser tägliches Leben kaum noch ohne direkte oder indirekte Berührung mit dem grossen World Wide Web bewältigen. «Die Idylle des Fortschritts musste ja irgendwann ein Ende haben», so der Zyniker.

Nüchtern betrachtet geht es bei der Cybersicherheit um das Ein- und Begrenzen von Sicherheitsrisiken. So wie Sie und ich das kennen vom Sicherheitsgurt im Auto, von der Lebensversicherung, vom Feuerlöscher und vom Türschloss.

In gewohnter Manier haben unsere Spezialisten von Research & Advisory das Thema Cybersicherheit fundiert untersucht und spannend aufgearbeitet. Sie öffnen für Sie das Türschloss zum Sicherheitsverhalten in der Cyberwelt. Ich wünsche Ihnen eine spannende Lektüre!

Ein Virus der anderen Art

Das Thema Sicherheit als Grundbedürfnis des Menschen beschäftigt uns alle: Ob zu Hause, im Freien oder bei der Arbeit, wir wollen uns sicher fühlen. Doch trotz des starken Bedürfnisses befindet sich unsere Gesellschaft im Daueralarm, das Bewusstsein für Risiken und Gefahren nimmt zu. Sicherheit ist weder eine Selbstverständlichkeit noch handelt es sich um einen festen Zustand. Eine Krise jagt die nächste. Mehr denn je entwickelt sich vor diesem Hintergrund die persönliche und gesellschaftliche Sicherheit zum Gebot der Stunde. So stellt beispielsweise die Cybersicherheit eine äusserst ernst zu nehmende Herausforderung dar – für Privatpersonen, Unternehmen und Regierungen. Mit der steigenden Konnektivität unserer Geräte wird die Angriffsfläche grösser und grösser. Auch im laufenden Jahr häufen sich die Meldungen über Angriffe bereits wieder. Prävention als Schlagwort gewinnt an Bedeutung.

Grafik 1: Auszug der in der Schweiz publik gemachten Attacken im Jahr 2021:[1]

April
Hacker dringen laut «Rundschau»-Bericht ins Netzwerk der Ruag International ein. Das auf zivile Luft- und Raumfahrt spezialisierte Unternehmen dementiert die Geschehnisse, gibt aber später «ernst zu nehmende Sicherheitslücken» zu. Bereits 2016 wurde ein grosser Cyberangriff auf militärische Geheimnisse der Ruag publik.

Mai
Hacker schleusen einen Verschlüsselungstrojaner ins Unternehmensnetzwerk des Pharmazulieferers Siegfried AG in Zofingen ein. Das Unternehmen muss die Produktion, darunter auch die Abfüllung von Impfstoffen, während mehrerer Tage herunterfahren.

Juni
Die Daten tausender spanischer Kundinnen und Kunden der Zurich Versicherung werden gestohlen und ab Oktober im Darknet angeboten. Die Lücke wird rasch geschlossen.

Juli
Die Erpresserbande «Grief» dringt beim Vergleichsdienst Comparis ein, legt IT-Systeme und die Webseite lahm. Kunden- und Unternehmensdaten werden verschlüsselt und gestohlen. Comparis sagt zuerst, man habe kein Lösegeld bezahlt und werde auch keines bezahlen. Wenige Tage später werden die Daten im Darknet veröffentlicht, wie Recherchen zeigen. Ende Juli gibt Comparis zu, doch Lösegeld bezahlt zu haben, um verschlüsselte Daten wiederherzustellen.

[1] Watson, «Die unfassbar lange Opferliste», Januar 2022
* Begriffserklärung siehe Seite 11

von Alessandro Poletti

«Achtung: Virus!» Eine Meldung, die für Schweissperlen sorgt, egal ob das Virus biologischen oder digitalen Ursprungs ist. In Zeiten von Corona sind biologische Viren in der Wahrnehmung der breiten Öffentlichkeit deutlich präsenter, dennoch ist die zweite Art von Virus nicht weniger relevant und aktuell. Schliesslich tragen digitale Viren ihren Namen, weil sie ihren biologischen Pendants sehr ähnlich sind: Sie verbreiten sich rasend schnell und wachsen dabei exponentiell von einem lokalen zu einem regionalen und schliesslich zu einem globalen Problem heran.

Genauso wie ein biologisches Virus für seine Vermehrung eine menschliche Zelle braucht, so braucht ein digitales Virus dafür Daten oder vernetzte Rechner – und genau das findet es in unserer zunehmend digitalisierten Welt. Eine deutlich steigende Anzahl von Angriffen auf Daten und Systeme untermauert denn auch die Relevanz der Cybersicherheit. Kein Wunder, verzeichnet auch der Wirtschaftszweig, der sich mit der Abwehr solcher Angriffe befasst, hohe Zuwachsraten.

Weshalb betrifft die Thematik uns alle? Wie lange war die Schweizer Opferliste des vergangenen Jahres? Wie hoch wird der jährliche Schaden geschätzt? Die Antworten hierauf sowie mehr zu den geforderten Präventivmassnahmen und zur Reaktion der Schweizer Landesregierung auf die digitale Bedrohung erfahren Sie in der vorliegenden «acrevis invest»-Ausgabe. Tauchen Sie ein in das spannende Thema der digitalen Sicherheit und erfahren Sie, mit welchen Umsetzungsideen Sie als Anlegerin oder Anleger am wachsenden Wirtschaftszweig teilhaben können.

Leben in einer immer vernetzteren Welt

Die Corona-Pandemie hat der Digitalisierung in etlichen Sektoren einen deutlichen Schub verpasst. Mit dieser Entwicklung hat auch die Konnektivität, also die Vernetzung unserer Welt, signifikant zugenommen. Waren es im Jahr 1950 noch rund 5'000 Geräte, die vernetzt waren, erhöhte sich deren Zahl bis 2003 auf 500 Millionen. Mit der globalen Verbreitung von Smartphones und Tablets, des mobilen Internets sowie von

Juli
Der Haushaltsgerätehersteller V-Zug wird Ziel einer Cyberattacke. Es seien keine «Betriebsbeeinträchtigungen oder Schäden» entstanden, sagt die Firma.

August
Der Technologiekonzern Saurer wird um den 1. August herum von einer Ransomware-Attacke* getroffen, am 26. August erfolgt ein zweiter Angriff. Exceltabellen, Mitarbeiterlisten und Finanzdokumente sind im Darknet zugänglich. Die Erpresser verlangen 500'000 Dollar Lösegeld. Saurer bezahlt laut Eigenaussage nicht.

Oktober
Das Casinotheater Winterthur wird Opfer einer Ransomware-Attacke. Betroffen sind das E-Mail- und das Reservationssystem des Restaurants. In einem auf dem Server hinterlassenen Erpresserschreiben fordern die Täter Geld für die Freigabe der Daten.

November
Media Markt wird Opfer der Ransomware-Bande «Hive». Betroffen sind rund 1'000 Filialen in 13 Ländern, darunter 25 Elektronikmärkte in der Schweiz. Kreditkartenzahlungen oder das Ausstellen von Quittungen können während mehreren Tagen nur eingeschränkt ausgeführt werden. Die Erpresser verlangen angeblich 50 Millionen Dollar Lösegeld, um die verschlüsselten Daten wieder freizugeben.

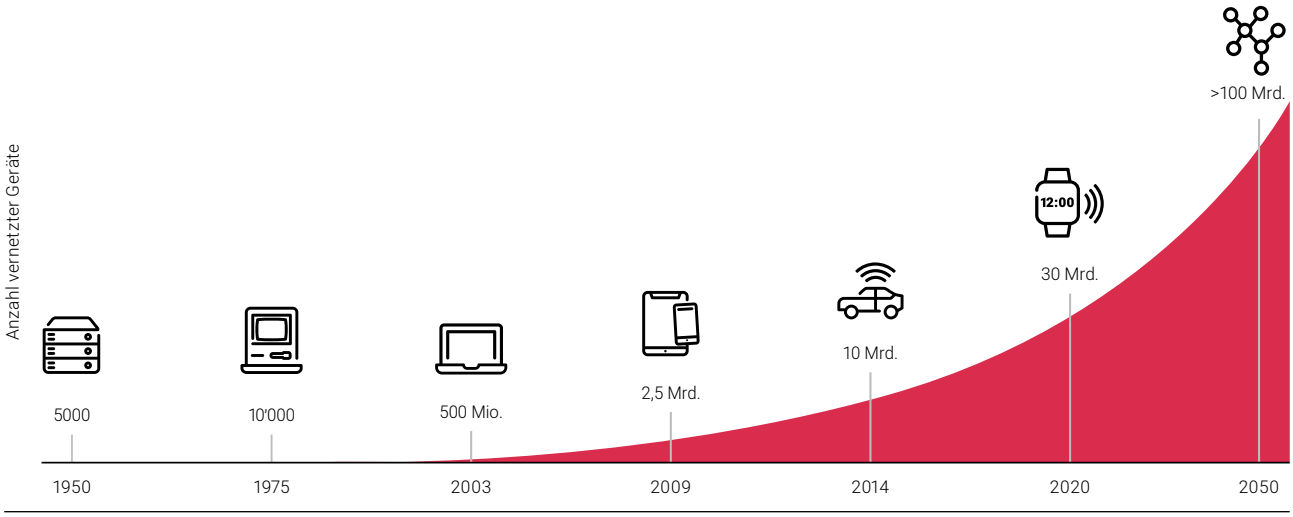
November
Ein Hackerangriff auf Bucher Industries legt die Produktion des Maschinen- und Fahrzeugbauers in elf Ländern temporär lahm.

Wearables und Smart Homes schoss die Zahl bis heute auf gut 30 Milliarden hoch.[2] Die geschätzte Anzahl vernetzter Geräte steigt jährlich um 10 Prozent. Gemäss Projektionen dürfte es im Jahr 2050 über 100 Milliarden verknüpfter Geräte auf der Welt geben.[3] Die fortschreitende Konnektivität bringt allerdings nicht nur Vorteile mit sich: Je mehr Geräte einem Netzwerk angeschlossen sind, desto grösser wird auch die Angriffsfläche für Cyberkriminalität. Hinzu kommen die ständig wachsenden Datenmengen, die täglich von den Unternehmen erzeugt und verarbeitet werden, sowie der Trend hin zu mehr Arbeiten von zu Hause aus. Daran wird deutlich, warum Cyberkriminalität ein ernst zu nehmendes Risiko darstellt – für Unternehmen, Regierungen und Privatpersonen.

Wer sind die Akteure und was sind ihre Ziele?

Die Herausforderungen im Bereich Cybersicherheit sind vielfältig und komplex. Das rührt nicht zuletzt von der Vielfalt an Akteuren und deren unterschiedlichen Zielen her: Kriminelle, Geheimdienste, unzufriedene Mitarbeitende oder Whistleblower. Während die einen sich rächen und andere (echte oder vermeintliche) Missstände aufdecken wollen, setzen Kriminelle auf Störung oder gar Zerstörung zugunsten einer illegalen Gewinnerzielung, sprich auf das schnelle Geld. Und das Geschäft boomt: Hacker haben längst erkannt, dass das skrupellose Geschäft mit Erpressungen oder dem Verkauf gestohlener Daten Gold wert ist. Sind hingegen institutionelle Angreifer wie etwa Geheimdienste am Werk, spielt Geld oft eine untergeordnete Rolle und die Motive sind politischer Natur.

Grafik 2: Anzahl vernetzter Geräte



Quelle: acrevis in Anlehnung an Pictet Asset Management

[2] Wearables sind Computertechnologien, die man am Körper trägt, etwa Smartwatches. Smart Home dient als Oberbegriff für technische Verfahren und Systeme in Wohnräumen und -häusern.
[3] Pictet Asset Management, «Pictet-Security Enabling a Safer World», Januar 2022

Wer zahlt, ist Teil des Problems

Mit dem Argument, dass Produktionsausfälle und Reputationsschäden rasch viel teurer als die Lösegeldforderung werden können, bezahlen laut Experten 30 bis 50% der Unternehmen das geforderte Lösegeld und machen sich damit zu Komplizen einer schnell wachsenden kriminellen Industrie. Das NCSC (Nationale Zentrum für Cybersicherheit des Bundes) rät in der Regel eindringlich von der Zahlung eines Lösegeldes ab. Es gibt keine Garantie, dass die Verbrecher nach der Bezahlung des Lösegelds die Daten nicht doch veröffentlichen oder anderen Profit daraus schlagen. Zudem motiviert jede erfolgreiche Erpressung die Angreifer zum Weitermachen, finanziert die Weiterentwicklung der Angriffe und fördert deren Verbreitung. Wird die Lösegeldforderung beglichen, so gilt man als lohnenswertes Ziel und kommt auf die «Kundenliste». Damit steigt die Wahrscheinlichkeit eines erneuten Angriffs drastisch.

Sind Sie als Privatperson oder als Unternehmen von einem Angriff betroffen?
Dann folgen Sie dem abgebildeten QR-Code des Nationalen Zentrums für Cybersicherheit. Hier finden Sie die wichtigsten Informationen zum empfohlenen Vorgehen.

Die lange Liste von Cyberattacken…

Werfen wir einen Blick auf die harte Realität: Im Jahr 2022 stapeln sich die Meldungen über Cyberattacken in der Schweiz bereits wieder. Gewichtige Unternehmen wie das Internationale Rote Kreuz, die Versandapotheke Zur Rose oder der Autohändler Emil Frey gehören zu den Opfern. Betrachtet man die Liste der Vorfälle aus dem vergangenen Jahr, erkennt man den Ernst der Lage: 2021 haben sich 161 Opfer von Erpresserbanden beim Bund gemeldet, rund zweieinhalb Mal mehr als im Vorjahr. Total erhielt die Meldestelle des Nationalen Zentrums für Cybersicherheit (NCSC) über 21'000 Meldungen von Cyberattacken. Dabei ist von einer hohen Dunkelziffer auszugehen, denn die Schweiz kennt bislang keine generelle Meldepflicht bei Cyberangriffen.

…und deren finanziellen Folgen

Die finanziellen Schäden, die aus solchen Attacken entstehen, sind immens: So schätzt das in der IT-Branche häufig zitierte US-Unternehmen Cybersecurity Ventures, dass die durch Cyberkriminalität verursachten weltweiten Schäden im Jahr 2021 sechs Billionen Dollar (!) erreicht haben. Bis 2025 könnte diese Summe demnach auf schwindelerregende 10,5 Billionen steigen.[4] Darin eingerechnet sind Datendiebstahl und -zerstörung, Finanzkriminalität, Produktivitätsverluste, Diebstahl geistigen Eigentums und andere Delikte ebenso wie die Kosten der Schadensbeseitigung.

Verständnis von Sicherheit

Trotz der weitreichenden Folgen von Cyberattacken sind viele Unternehmen unzureichend vorbereitet, was die steigende Anzahl an Fällen klar beweist. Dies liegt zumindest zum Teil auch an fehlendem Wissen: Gemäss einer aktuellen Studie zum Thema Cybersicherheit in Schweizer KMUs fühlt sich ein Fünftel der KMU-Geschäftsleitenden zu wenig oder sogar überhaupt nicht informiert über Cyberrisiken. Die Relevanz der Cybersicherheit ist in der Studie zu erkennen, allerdings unseres Erachtens noch zu wenig: Nur 65% der Geschäftsleitenden von Schweizer KMUs bewerten die Thematik als wichtig oder sehr wichtig.[5]

Wie gelingt die Kehrtwende? Einerseits muss die Cybersicherheit als eine strategische Angelegenheit eingestuft und somit Thema jeder Führungsetage werden. Andererseits braucht es ein verstärktes, in der Unternehmenskultur verankertes Sicherheitsbewusstsein.

Heutzutage sind Risiken komplex und dynamisch. Wie eingangs erwähnt, stellt die Sicherheit somit keine Selbstverständlichkeit oder einen festen Zustand dar, der einmal hergestellt und anschliessend einfach gehalten werden kann. Es handelt sich vielmehr um einen variablen Wert, um den man sich laufend neu bemühen muss. Dabei haben die systematischen Bestrebungen für mehr Sicherheit in den vergangenen Dekaden enorme Fortschritte gebracht. Entgegen der vielfach empfundenen Unsicherheit etwa angesichts des Krieges in der Ukraine leben wir in der Schweiz in der Tat in sehr sicheren Zeiten: Egal welche Indikatoren in puncto Sicherheit auch betrachtet werden (Armut, Bildung, Arbeitsmarkt etc.), die Entwicklung ist beinahe überall positiv. Dennoch fühlen wir uns in ständiger Gefahr – woher kommt diese Diskrepanz? Laut Psychologen ist die Kombination von menschlicher Kognition, Unterhaltungsindustrie und Journalismus dafür verantwortlich. Menschen schätzen demzufolge Risiken und Wahrscheinlichkeiten anhand von Einzelberichten, Erzählungen und Bildern ein. Weil viele Medien, insbesondere die Boulevardpresse und Social Media, sich auf plötzliche, meist negative Einzelereignisse fokussieren und intensiver über Anschläge, Kampfhandlungen oder Epidemien berichten als über positive Entwicklungen, wird unser Sicherheitsempfinden beeinflusst.[6] Daraus resultiert eine wichtige Tatsache: Der Mensch gibt immer mehr Geld für seine Sicherheit aus. Dementsprechend gewinnt auch der Wirtschaftszweig «Cybersicherheit» laufend an Bedeutung: Die weltweiten Massnahmen gegen Cyberattacken und Sicherheitsverletzungen kosten jährlich Milliarden, Tendenz steigend. Eine Studie beziffert die globalen Ausgaben für Sicherheitslösungen im vergangenen Jahr auf rund 150 Milliarden Dollar. Die Erwartungen fürs 2022 und 2023 belaufen sich auf 161 respektive 177 Milliarden, was einer Wachstumsrate von 10 Prozent entspricht.[7]

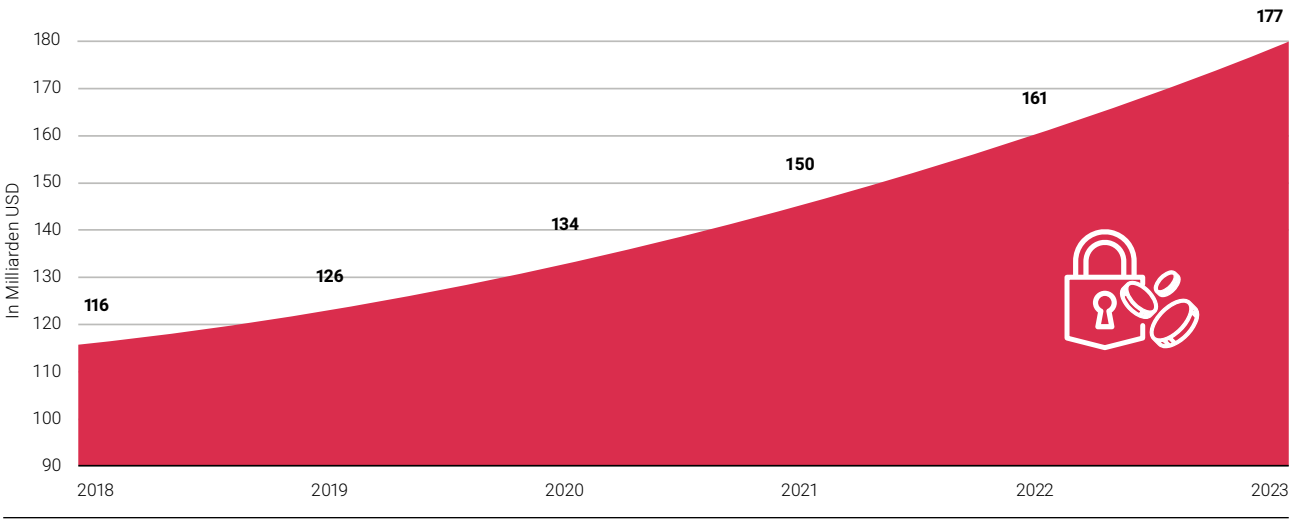
Cybersicherheit als wichtiges Zukunftsthema

Zusammengefast lässt sich festhalten, dass Cybersicherheit, also der Schutz von Daten, Informationen und IT-Strukturen, eine enorm wichtige Angelegenheit ist und zu den wichtigsten Zukunftsthemen unserer Zeit gehört, auch mit Blick auf die Privatsphäre und den Datenschutz, die vor allem in Europa ein hohes Gut darstellen und als schützenswert erachtet werden.

Entstanden sind der Begriff «Cybersicherheit» und das daraus resultierende Geschäftsfeld bereits in den 1970er- und 1980er-Jahren. Ins Bewusstsein der breiten Öffentlichkeit drang das Thema durch massive Hackerangriffe im vergangenen Jahrzehnt, bei denen Daten von mehreren Milliarden Nutzerinnen und Nutzern betroffen waren (Yahoo: 3 Mrd., eBay: 145 Mio., Marriot International: 500 Mio.). Die Cybersicherheit ist deshalb so wichtig, weil sie Unternehmen und auch die Gesamtwirtschaft vor weitreichenden Folgen wie unterbrochenen Lieferketten oder der Gefährdung der Wettbewerbsfähigkeit durch Reputations- und Vertrauensverluste bewahrt. Das Thema steht längst nicht mehr nur im Aufgabenheft eines engen Kreises von Technikexperten, sondern beschäftigt Organisationen als Ganzes.

[4] Cybersecurity Ventures Magazine, «Cybercrime to Cost the World $10,5 Trillion Annually by 2025», November 2020
[5] Die Mobiliar, digitalswitzerland, FHNW, SATW, gfs-zürich, «Homeoffice und Cybersicherheit in Schweizer KMU», November 2021
[6] ZukunftsInstitut, Artikel «Megatrend Sicherheit»
[7] Gartner, «Forecasts Worldwide Security and Risk Management Spending», Mai 2021

Grafik 3: Weltweite jährliche Ausgaben für Cybersicherheit



Quelle: acrevis in Anlehnung an Pictet Asset Management

Prävention als Gebot der Stunde

Gemäss Experten kann man sich besser oder schlechter schützen, aber niemals vollständig.[8] Es gilt: Wenden erfahrene Hacker genügend Zeit auf, so knacken sie beinahe jedes System. Mit geeigneten Massnahmen kann man es ihnen aber so schwer wie möglich machen: Gängige technische Schutzmechanismen wie etwa Anti-Virus-Scanner, Firewalls oder aufwändige Passwörter sind zwingend und richtig anzuwenden. Dies, kombiniert mit korrektem persönlichem Verhalten, erhöht die Sicherheit in der virtuellen Welt schon markant. Und für den unschönen Fall der Fälle helfen ein guter Krisenbewältigungs- und Managementplan sowie – wenn immer möglich – eine adäquate Versicherung.

Angriffsfaktor Mensch

Nebst den überwiegend komplexen technischen Massnahmen wird einem Glied in der Sicherheitskette oft zu wenig Beachtung geschenkt: dem Faktor Mensch. Er kann entweder als Bollwerk gegen oder als Eintrittstor für Cyberattacken stehen.

Es ist eine Tatsache, dass die meisten Sicherheitsvorfälle nicht der Technik geschuldet sind, sondern den Menschen. Dies unterstreicht die Wichtigkeit des Faktors Mensch bei diesem Thema. Prävention beginnt beim Sperren der Arbeitsstation beim Verlassen des Arbeitsplatzes und geht bis hin zum verantwortungsvollen Umgang mit E-Mails (Stichwort Phishingversuche*). Entsprechend entscheidend ist es, innerhalb der Organisation eine angemessene Sicherheitskultur zu schaffen. Regelmässige, obligatorische Trainings begleitet von Massnahmen wie dem Aushändigen von Checklisten oder dem Wiederholen der Verhaltensregeln sollen helfen, das Bewusstsein der Mitarbeitenden im täglichen Umgang mit Daten und Informationen zu steigern. Denn dieses Bewusstsein ist im Kampf gegen Cyberkriminalität mitentscheidend.

Eine Cybermiliz für die Schweiz

Und wie reagiert die Schweizer Regierung auf diese globale Bedrohung im digitalen Raum? Grundsätzlich hat der Staat in privaten, nichtstaatlichen Netzwerken nichts zu suchen. Er kann höchstens im Dialog und durch Partnerschaften versuchen, gemeinsam mit Unternehmen für mehr Sicherheit zu sorgen, was er in der Schweiz auch tut. Um der Gefahr von Cyberattacken als Nation entgegenzutreten, hat der Bundesrat im vergangenen Jahr die rechtlichen Grundlagen für das Kommando «Cyber» verabschiedet. Damit wird die elektronische Aufrüstung der Armee konkreter. Dazu gehört ein Miliz-Cyberbataillon, welches aus rund 600 spezialisierten Soldatinnen und Soldaten bestehen soll. Die neue Abteilung setzt sich gemäss Bundesrat aus Armeeangehörigen zusammen, die aufgrund ihrer zivilen beruflichen oder akademischen Tätigkeit über die notwendige Cybererfahrung und Qualifikation verfügen.

Schon seit 2018 können junge Talente aus dem Cyberbereich – etwa Absolventinnen und Absolventen einer Informatiklehre oder angehende Informatikstudierende – als Schwerpunkt ihrer militärischen Grundausbildung an einem 40-wöchigen Cyberlehrgang teilnehmen. Zusammen mit anderen Cyberspezialisten aus der Miliz werden diese Armeeangehörigen künftig ins Cyberbataillon eingeteilt. Laut Thomas Süssli, Chef der Armee, gibt es trotz strenger Selektion keine Rekrutierungsprobleme, es bewerben sich mehr junge Leute, als freie Plätze im Lehrgang zur Verfügung stehen.[9]

[8] ZukunftsInstitut, Interview mit M. D. Cavelty, «Der Cyberkrieg ist längst hier»
[9] NZZ, «Die Schweiz schafft eine Cybermiliz», September 2021
* Begriffserklärung siehe Seite 11

Fünf Fragen an Ivan Bütler

Compass Security ist ein Schweizer Unternehmen mit über 60 Mitarbeitenden an den Standorten in der Schweiz, in Deutschland und in Kanada. Im Jahre 1999 durch Walter Sprenger und Ivan Bütler gegründet, hat sich Compass Security zu einem technisch herausragenden und europaweit anerkannten IT-Security-Unternehmen entwickelt.

Ivan Bütler
Experte, Gründer und Board Member
bei der Firma Compass Security Network Computing AG

Compass Security bietet Penetrationstests, Trainings, Security Reviews und weitere Dienstleistungen im Zusammenhang mit Cybersicherheit an.

Erfahren Sie mehr unter folgendem QR-Code:

Herr Bütler, Sie beschäftigen sich schon seit über 20 Jahren mit dem Thema Cybersicherheit. Welche jüngsten Entwicklungen stellen Sie fest?
Im Rahmen unserer simulierten Hacker-Attacken und Cyber-Feuerwehr-Einsätze stellen wir ein hohes Mass an Ransomware-Angriffen fest. Erpresser verschlüsseln die Daten der Kunden und verlangen Lösegeld. Die Angreifer sind gut organisiert und setzen präzise und gefährliche Malware ein. Immer mehr Firmen werden gehackt, weil Mitarbeitende in Mails auf einen Link oder Anhang klicken. Die Angreifer werden immer professioneller, es wird immer schwieriger, sich adäquat zu schützen. Darüber hinaus werden Cloud-Anbieter immer bedeutender.

Haben Sie mit der enormen Beschleunigung und wachsenden Relevanz des Themas in diesem Ausmass gerechnet?
Ja, damit war leider zu rechnen. Die Digitalisierung eröffnet unglaublich viele neue Business Cases. Doch Komplexität und Vernetzung überfordern die Menschen und so schleichen sich unbemerkt viele kleine Sicherheitslücken ein, die durch Hacker ausgenutzt werden können. Security steht zwar bei vielen Unternehmen zuoberst auf der Agenda, steht aber im Spannungsfeld zu Business Opportunities oft an zweiter Stelle. Ein Unternehmen muss Geld verdienen und Security-Prozesse kosten Geld und erfordern viel Kompetenz. Der Mangel an Sicherheitskräften trägt ebenfalls dazu bei, dass in naher Zukunft keine Besserung in Sicht ist.

Die Liste der Opfer von Cyberattacken ist lang. Stimmen Sie der Aussage zu, dass sich die Unternehmen im Durchschnitt schlecht oder unzureichend mit dem Thema auseinandersetzen?
Das Wort «schlecht» scheint mir hier etwas zu umfassend. Viele Unternehmen, insbesondere die Schweizer Finanzbranche, haben schon sehr früh mit der Abwehr von Cyberattacken begonnen. Andere Branchen sind etwas im Hintertreffen, sei es, weil diese glauben, es gäbe bei ihnen nichts zu holen, oder weil es noch keine entsprechenden Vorgaben der Branchenverbände gibt. Solange der Faktor Mensch nicht umfassend in das Security-Dispositiv miteinbezogen wird, gibt es weiterhin Angriffsflächen. Es gewinnt oftmals die Benutzerfreundlichkeit vor der Sicherheit.

Wie sollte Ihrer Ansicht nach ein klassisches Schweizer KMU das Thema Cybersicherheit angehen?
Die Führungskräfte und Verwaltungsräte sollten Security auf oberster Stufe traktandieren und Prozesse und ein Risikomanagement etablieren. Darüber hinaus empfehle ich, dass man gedanklich davon ausgeht, Opfer einer Cyberattacke zu werden. Man sollte Notfallpläne wie auch Back-ups bereitstellen, um im Ereignisfall professionell reagieren zu können. Auch den Einsatz von 2-Faktor-Authentisierungen sehe ich als enorm wichtig.

Wie hoch ist die Chance, dass die nächste Pandemie digitaler Natur ist?
Glaubt man den Worten von Yuval Noah Harari, der in seinen Büchern die Entwicklung der Menschheit aufzeigt, werden wir in Kürze unseren Körper digitalisieren. Es sei in Zukunft möglich, Krebs zwei Jahre vor der Metastase zu erkennen, indem die Cloud und Artificial Intelligence mittels Algorithmen ständig beobachten und analysieren. Das geht viel weiter, als dass wir es uns heute vorstellen können. Ich erwarte einen gesellschaftlichen Diskurs hinsichtlich Ethik und Moral – wer das Wissen haben darf über unsere Ängste, Bedürfnisse und Vorlieben. Einen Cyber War als isoliertes Ereignis erachte ich als unrealistisch. Vielmehr scheint mir Cyber als Unterstützung bewaffneter Konflikte als real. Insofern wird die nächste Pandemie nicht primär digital sein, aber mit Sicherheit wird die Digitalisierung einen wichtigen Aspekt davon darstellen.

Je nach Bedarf sollen Kantone oder beispielsweise Elektrizitätswerke durch diese Kräfte bei der Cyberabwehr unterstützt werden. Die Spezialistinnen und Spezialisten des Cyberbataillons stehen sowohl der Armee als auch ihren zivilen Arbeitgebern zur Verfügung. Gerade weil moderne Konflikte nicht offen ausgetragen und mit Cybersabotageakten gegen kritische Infrastrukturen geführt werden, schafft die Schweiz damit ein flexibles System einer zivil-militärischen Zusammenarbeit.

Steigern Sie das Sicherheitsbewusstsein

Unser Fazit: Mit der fortschreitenden Vernetzung wird ein systematisches Verständnis von Sicherheit immer wichtiger. Weniger denn je kann Sicherheit als fix erreichbarer Endzustand angesehen werden. Vielmehr handelt es sich um eine dynamische und kontinuierliche Herausforderung, die man als Individuum, Gemeinschaft oder Organisation aktiv bewältigen muss.

In den Unternehmen ist ein Umdenken in der gesamten Unternehmenskultur über alle Abteilungsgrenzen hinweg nötig. Das Thema darf nicht länger auf einem Nebenschauplatz behandelt werden. Die Cybersicherheit muss unternehmensweit gewährleistet sein, denn digitale Attacken können praktisch jeden Unternehmensbereich treffen. Eine möglichst erfolgreiche Abwehrstrategie benötigt nebst den technischen Komponenten wie aktualisierten Betriebssystemen, starken Firewalls, externen Back-ups etc. auch effiziente und alltagstaugliche Sicherheitsroutinen, regelmässige Schulungen der Belegschaft und eine sicherheitsbewusste Unternehmensstruktur, die alle Mitarbeitenden miteinbezieht.

In der Summe verspricht ein erfolgreicher Mix aus moderner Technologie, einer klar kommunizierten und umgesetzten Sicherheitsstrategie sowie einer reibungslosen Zusammenarbeit zwischen der IT und den regulären Geschäftseinheiten am meisten Erfolg. Wichtig ist die gemeinsame Kultur der Achtsamkeit und des damit verbundenen Sicherheitsbewusstseins, dass Cybersicherheit ein wesentlicher Bestandteil der täglichen Arbeitsroutine ist: am Arbeitsplatz, unterwegs und im Homeoffice. Die menschliche Komponente bietet enorm viel Potenzial zur Risikominimierung – wir haben es also grösstenteils in der eigenen Hand. Privat und im Geschäftsleben.

Rundumschutz mit einer Cyberversicherung

Wie erwähnt sind Cyberattacken nie vollständig verhinderbar – doch die Folgen lassen sich mit einer Versicherungspolice abfedern. Eine Versicherung gegen Cyberrisiken ist für alle Unternehmen sinnvoll, die mit Daten arbeiten und eine Internetverbindung unterhalten – also so ziemlich jedes Unternehmen in der Schweiz. Durch die zunehmenden Angriffe schnellt die Nachfrage und damit auch das Angebot in die Höhe. In der Schweizer Versicherungslandschaft tummeln sich diverse Anbieter, die ein entsprechendes Produkt im Sortiment führen: Zurich, AXA, Baloise, Helvetia, Mobiliar und weitere.

Am Beispiel der Zurich gliedert sich das Versicherungsprodukt in drei Teile:

1) Prävention (Cyber-Sicherheitstraining und Risiko-Assessment)

2) Schutz vor finanziellen Risiken (Daten- und Systemwiederherstellung, Betriebsunterbruch, Krisenmanagement etc.)

3) Schadenmanagement (schnelle und adäquate Intervention im Ernstfall, 24/7-Hotline in Zusammenarbeit mit IT-Partner Compass Security)

Aufgrund der Tatsache, dass den Versicherern schlicht noch die langjährige Erfahrung mit Cyberattacken fehlt, dürfte das Preisschild für dieses «unbekannte Gut» noch nicht abschliessend angeheftet sein. Wie so oft bei Versicherungspolicen empfiehlt sich, mehrere individuelle Angebote einzuholen und zu vergleichen.

Spannende Investitionsmöglichkeit durch eine unelastische Nachfrage

Die publizierten Zahlen der Unternehmen aus dem Bereich Cybersicherheit zum Geschäftsjahr 2021 bestätigen den Trend: Eine Mehrheit weist signifikant höhere Umsätze und Gewinne aus. Auch die Ertragsqualität in der Cybersicherheitsbranche schneidet im Vergleich zum Gesamtmarkt besser ab. Das bringt uns zu einem wichtigen Fakt: Im Gegensatz zu gewöhnlichen Konsumentinnen und Konsumenten interessieren sich Hacker nicht für Inflation, Zinserhöhungen oder Lieferengpässe. Deshalb rechnen wir mit einer starken und unelastischen Nachfrage[10] nach Produkten und Dienstleistungen in diesem Segment. Da sich die Bedrohungslage ständig verändert, entwickelt sich auch die Cybersicherheitsbranche laufend weiter. Die steigende Nachfrage befeuert die Entwicklung innovativer Sicherheitslösungen durch spezialisierte Unternehmen und schafft spannende Investitionsmöglichkeiten. Mit welchen Umsetzungsideen Sie als Anlegerin oder Anleger langfristig an diesem stark wachsendem Wirtschaftszweig partizipieren können, erfahren Sie auf den folgenden Seiten.

Ransomware-Attacke

Ransomware (von englisch ransom für «Lösegeld»), auch Erpressungssoftware oder Verschlüsselungstrojaner genannt, sind Schadprogramme, mit deren Hilfe ein Eindringling den Zugriff des Computerinhabers auf Daten, deren Nutzung oder auf das ganze Computersystem verhindern kann. Für die Entschlüsselung oder Freigabe wird üblicherweise ein Lösegeld verlangt.

Phishing

Unter dem Begriff Phishing (von englisch fishing für «Angeln») versteht man Versuche, sich über gefälschte Webseiten, E-Mails oder Kurznachrichten als vertrauenswürdiger Kommunikationspartner auszugeben. Ziel des Betrugs ist es, zum Beispiel an persönliche Daten eines Internetbenutzers zu gelangen oder ihn zur Ausführung einer schädlichen Aktion zu bewegen.

[10] Eine unelastische Nachfrage ist dann gegeben, wenn sich der Preis einer Dienstleistung / Ware verringert oder erhöht, die Nachfrage sich dadurch aber kaum verändert.

Umsetzungsideen

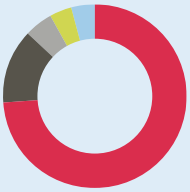
Selektiert nach den Kriterien der bewährten acrevis spektrum®-Methodik stellen wir Ihnen nachfolgend verschiedene Umsetzungsideen zum Thema vor. Zum einen handelt es sich um eine auserwählte Kollektivanlage, die global in Aktien von Unternehmen investiert, deren Geschäftstätigkeit auf die Cybersicherheit ausgerichtet ist. Zum anderen stellen wir Ihnen Unternehmen aus der Schweiz und Europa vor, die Cybersicherheit nebst anderen Aktivitäten zu ihrem Kerngeschäft erklärt haben.

L&G Cyber Security ETF

Valor	29'885'500
Währung	CHF
Kurs[11]	22,35
Kosten	0,69%
Fondsdomizil	Irland
Lancierung	2015
Performance p. a.	17,1%
Volatilität p. a. (5 J.)	22,8%
Fondsvolumen (in USD)	3 Mrd.

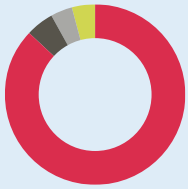
Der börsengehandelte Fonds investiert weltweit in ein konzentriertes Portfolio bestehend aus rund 45 Unternehmen, deren Geschäftsaktivitäten den Hauptfokus auf die Cybersicherheit legen. Da sich die grossen und erfahrenen Unternehmen in diesem Sektor in den Vereinigten Staaten befinden, stammen rund zwei Drittel der Positionen von dort. Ziel des Fonds ist es, das ausserordentliche Wachstumspotenzial von Produkten und Dienstleistungen für Cybersicherheit auszuschöpfen. Seit Lancierung der Strategie im Jahr 2015 ist das Fondsvolumen auf beachtenswerte 3 Milliarden US-Dollar angewachsen. Mit dieser Anlage setzen Sie das Thema breit diversifiziert und kostengünstig um. Der Fonds wird an der Schweizer Börse SIX in CHF gehandelt und eignet sich als Beimischung respektive als Satellitenanlage für langfristig orientierte Investoren.

Länder



Vereinigte Staaten 74%
Israel 13%
Japan 5%
Kanada 4%
Weitere 4%

Währungen

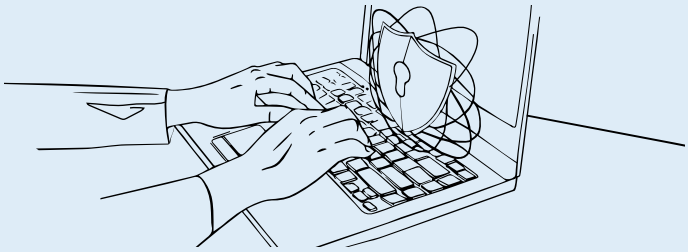


USD 87%
JPY 5%
CAD 4%
Weitere 4%

Grösste Positionen	Anteil
Splunk	5%
Mandiant	5%
Check Point Software Technologies	5%
Ping Identity Holding	4%
Palo Alto Networks	4%
CrowdStrike	4%
Trend Micro	4%
Juniper Networks	4%
Qualys	4%
NortonLifeLock	4%

Kursentwicklung

Swisscom



Valor	874’251
Währung	CHF
Branche	Telekommunikation
Kurs[11]	559,20
KGV	18,50
KBV	2,71
Dividendenrendite	3,80%

Einschätzung acrevis[12]	Rating
Fundamental	3 ↗
Verhaltensbezogen	0 ↘
Technisch	3 ↗
Gesamteinschätzung	**6 ↗**

Mit rund 19’600 Mitarbeitenden und einem jährlichen Umsatz von 11,2 Milliarden Franken ist Swisscom das führende Telekommunikationsunternehmen der Schweiz. Nebst Mobilfunk, Internet, Festnetz und TV bietet sie vor allem auch IT-Dienstleistungen für Unternehmen an. Mit einem umfassenden Angebot im Bereich Cybersicherheit gilt Swisscom in diesem Gebiet als führende Anbieterin in der Schweiz. So zählt die Sparte «Security» zu den Kernkompetenzen des Telekomkonzerns. Das Security-Management gründet auf der raffinierten Kombination von Mensch und Maschine: Dank ausgereiften Technologien und über 200 Security-Experten werden Cyberbedrohungen früh, schnell und genau erkannt. In der Schweiz vertrauen der Swisscom bereits über 1’000 Unternehmen ihre Cybersicherheit an. Bei neuartigen Cyberangriffen fliesst das neu erlangte Wissen automatisch in den Schutz aller bestehenden Kunden ein.

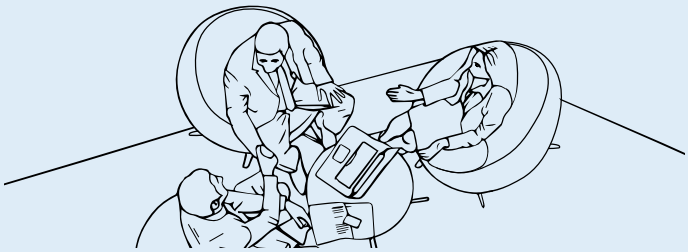
Zurich Versicherungen

Valor	1’107’539
Währung	CHF
Branche	Finanzen
Kurs[11]	443,50
KGV	10,20
KBV	1,89
Dividendenrendite	5,90%

Einschätzung acrevis	Rating
Fundamental	3 ↗
Verhaltensbezogen	1 →
Technisch	3 ↗
Gesamteinschätzung	**7 ↗**

Die Zurich Versicherung ist ein international tätiger Versicherungskonzern mit rund 54’000 Mitarbeitenden und Bruttoprämieneinnahmen von jährlich über 55 Milliarden US-Dollar. Zusätzlich zu den klassischen Versicherungen umfasst das Angebot auch Cyberversicherungen, deren globales Prämienvolumen derzeit auf 10 bis 15 Milliarden geschätzt wird. Zurich rechnet in den kommenden Jahren mit einer Zunahme von jeweils rund 25%. Die Marke von 25 Milliarden soll demnach bereits im Jahr 2025 überschritten werden. Das Zurich-Cyberversicherungskonzept hilft mittels drei Stufen (Prävention, Schutz vor finanziellen Risiken, Schadenmanagement) Privatpersonen und Unternehmen dabei, ihre Risiken zu verstehen und sich gegen Cyberattacken zu schützen. Zurich arbeitet hierfür mit hochspezialisierten Partnern zusammen.

Capgemini



Valor	488’070
Währung	EUR
Branche	Informations-technologie
Kurs[11]	189,70
KGV	13,50
KBV	3,84
Dividendenrendite	1,50%

Einschätzung acrevis	Rating
Fundamental	3 ↗
Verhaltensbezogen	1 →
Technisch	3 ↗
Gesamteinschätzung	**7 ↗**

Capgemini mit Sitz in Paris ist ein Beratungs- und Dienstleistungsunternehmen mit Schwerpunkt Informationstechnik und Spitzentechnologien. Mit weltweit rund 300’000 Mitarbeitenden erzielt das Unternehmen einen jährlichen Umsatz von 18 Milliarden Euro. Capgemini bietet unter der Servicesparte umfangreiche Cybersecurity-Services an: Cloud-Security, Cybersecurity-Beratungen, Penetrationstests, Simulationen von Cyberattacken und vieles mehr. Der grösste europäische IT-Dienstleister sorgt mit seiner breiten Produktpalette, seinem globalen Netzwerk von Security Operations Centern sowie starken Partnerschaften (mit Google Cloud, IBM, Intel oder SAP) für mehr Transparenz und eine schnelle Erkennung von Bedrohungen für Unternehmen.

[11] Kurse per 08.04.2022

[12] Beim acrevis spektrum®-Rating werden bis zu 8 Punkte vergeben – jeweils max. 3 Punkte für die Dimensionen «Fundamental» und «Technisch» sowie max. 2 Punkte für die Dimension «Verhaltensbezogen».

Makro und Märkte
Seien Sie auf der Hut

Sicherheit bleibt ein rares Gut – besonders in diesem Jahr auch beim Anlegen. Nicht nur online, sondern auch stationär drohen so viele Risiken wie schon lange nicht mehr. Geopolitik und Wirtschaft sind gefährdet: von Inflationssorgen über Konjunkturabschwächung bis hin zu Lieferkettenproblemen. Selbst die Furcht vor einer weiteren Verschärfung des Krieges mitten in Europa schwingt an den Finanzmärkten mit.

von Daniel Brunner

Die Invasion Russlands in der Ukraine verursacht nicht nur unvorstellbares menschliches Leid, sondern hat auch der Globalisierung einen herben Dämpfer verpasst. Unabhängigkeit, Selbstversorgung und eine Verkürzung der Lieferketten dürften uns noch länger beschäftigen. Dass Russland und die Ukraine gemessen am Anteil der globalen Wirtschaft keine allzu grosse Bedeutung spielen, zeigt sich, indem die Finanzmärkte in vielen Regionen wieder das Niveau vor Ausbruch des offenen Krieges erreicht haben. Trotzdem weist der Konflikt weitreichende Folgen für das globale Wirtschaftswachstum auf. Anhaltend hohe Energie- und Rohstoffpreise belasten die Konjunktur ebenso wie die gestiegene Inflation. Ungeachtet der Wachstumseinbussen definieren die westlichen Notenbanken den Kampf gegen die Inflation deshalb als ihre dringlichste Aufgabe und sind dabei, ihre Geldpolitik schrittweise restriktiver auszugestalten. Die Risiken einer Stagflation haben zugenommen, wie die flache, zeitweise sogar inverse US-Zinskurve belegt. Demgegenüber stehen jedoch ein äusserst robuster Arbeitsmarkt mit einer hohen Beschäftigungsquote sowie eine gesunde Nachfrage. Die Entwicklung verschiedener Konjunkturindikatoren, aber auch der weitere Verlauf des Ukraine-Kriegs sind von entscheidender Bedeutung für die Weltwirtschaft.

Angesichts der höheren Inflationsraten zogen die nominalen Renditen an den meisten Anleihenmärkten deutlich an und erreichten mehrjährige Höchststände. Sollten die hohen Energiepreise anhalten, dürfte eine Erholung der weltweiten Kurse bei den Anleihen noch auf sich warten lassen. In Anbetracht eines mitten in Europa stattfindenden Angriffskriegs haben sich die Aktienmärkte als überraschend robust erwiesen und wurden durch positive Unternehmensergebnisse gestützt. Doch beim wirtschaftlichen Ausblick lässt die fehlende Visibilität keine Kurseuphorie aufkommen. Die einsetzende Deglobalisierung sorgt tendenziell für steigende Kosten und spricht für tiefere Gewinnmargen der Unternehmen. Schweizer Immobilien zeigten sich trotz gestiegener Kapitalmarktzinsen erstaunlich resilient, während Gold seine Pflicht als Anker in turbulenten Phasen vollkommen erfüllte.

Politische Ereignisse vorauszusehen und sich entsprechend darauf zu positionieren ist nahezu unmöglich. Im aktuellen Umfeld geprägt von Inflation, Sanktionen und Wirtschaftsabkühlung empfiehlt sich jedoch eine vorsichtigere Positionierung.

Autoren

Sandro Schibli
Bereichsleiter Private Banking

Sandro Schibli bringt über dreissig Jahre Erfahrung in der Anlageberatung mit. Als ausgewiesener Fachmann im Asset Management ist er Mitglied des Anlagekomitees. Sandro Schibli ist diplomierter Finanzanalytiker und Vermögensverwalter.

Alessandro Poletti
Leiter Research & Advisory

Alessandro Poletti leitet bei acrevis die Abteilung Research & Advisory. Er verfügt über einen Bachelor der Zürcher Hochschule für Angewandte Wissenschaften (ZHAW) in Betriebsökonomie und ist diplomierter Finanzanalytiker und Vermögensverwalter (CIIA). Alessandro Poletti ist Mitglied des Anlagekomitees.

Daniel Brunner
Research & Advisory

Daniel Brunner ist bei acrevis als Research Analyst und Portfolio Manager tätig. Er bringt mehrere Jahre Erfahrung im Research mit und verfügt über einen Masterabschluss der Universität St. Gallen (HSG) in Quantitative Economics & Finance.

Wir sind acrevis:
Ihr verlässlicher Partner, wenn’s ums Anlegen geht.

Eine moderne Bank mit einer langen Geschichte: Seit rund einem Jahrzehnt ist die acrevis Bank für ihre Kundinnen und Kunden da – sie ist 2011 aus der Fusion der Bank CA St.Gallen und der swissregiobank entstanden. Die Wurzeln unserer Bank reichen aber über 150 Jahre zurück. Auf unsere Geschichte sind wir stolz und fühlen uns unserer Tradition auch heute noch in unserer täglichen Arbeit verpflichtet: Wir freuen uns, Ihre Bank fürs Leben zu sein.

Mit acht Standorten sind wir stark regional verankert und in St.Gallen (Hauptsitz), Gossau, Wil, Bütschwil, Wiesendangen, Rapperswil-Jona, Pfäffikon und Lachen stets nahe bei Ihnen. Unsere 170 Mitarbeitenden machen uns zur führenden Regionalbank in unserem Marktgebiet zwischen Bodensee und Zürichsee. Dabei werden wir von mehr als 10’000 regionalen Aktionärinnen und Aktionären getragen.

Verantwortungsvolles Banking im Interesse aller Anspruchsgruppen, das ist unser Ziel. Die Regelung der finanziellen Belange ist Vertrauenssache, davon sind wir überzeugt. Der Name acrevis ist an drei lateinische Wörter angelehnt, die unseren Leitsatz «Durch Vertrauen gestärkt» verkörpern: a|cre|vis (a – durch; cre – Vertrauen; vis – Stärke, Kraft).

Sie haben Fragen oder ein individuelles Anliegen? Für weitere Informationen wenden Sie sich an unsere Beraterinnen und Berater. Wir sind gerne für Sie da!

acrevis Bank AG
Marktplatz 1
9004 St.Gallen

Tel. 058 122 75 55 · info@acrevis.ch · acrevis.ch

St.Gallen · Gossau SG · Wil SG · Bütschwil · Wiesendangen · Rapperswil-Jona · Pfäffikon SZ · Lachen SZ

Gedruckt auf Refutura-Papier
FSC-Recycling-Papier/zu 100% aus Altpapier/«Blauer Engel»

«acrevis invest», das Anlegermagazin der acrevis Bank AG, wird klimaneutral produziert und hat dafür das entsprechende Gütesiegel von «swiss climate» erhalten. Diese Stiftung entwickelt und unterstützt weltweit hochwertige Klimaschutzprojekte.

Hergestellt in einem schadstofffreien, wasserlosen Druck mit konsequenter Verwendung biologischer, lebensmittelechter PURe-Druckfarben. Diese Farben enthalten anstelle von Mineralölen nur pflanzliche Öle, welche sich im Recyclingprozess rückstandsfrei herauslösen lassen.

Klimaneutral Druckprodukt ClimatePartner.com/12967-2004-1002

printing system 100% schadstofffrei

FSC www.fsc.org RECYCLED Papier aus Recyclingmaterial FSC® C011349