Ausgabe 1/2021

Advisory Inside

Unsere Themen: Ausblick 2021 • Datensicherheit • Cybersecurity • Anlageidee • Interview Oliver Münchow – Lucy Security • Wissens-Corner FTSE MIB • Chart-Corner S&P 500

Ausblick 2021

Für ein vermeintlich erfolgreiches Anlagejahr gibt es Prognosen wie Sand am Meer.

Fast jede Bank und jeder Broker gibt sich da ein Stelldichein. Leider haben aber auch wir keine Kristallkugel. Dennoch zeigen wir mögliche Leitplanken und erwartete Trends auf. Gewisse Grundregeln wie die Börsenpsychologie gelten immer und können bei Bedarf ruhig auch aus dem Ausblick vom letzten Jahr nochmals verinnerlicht werden:
https://www.akb.ch/-/advisory-inside-201912

Kurzer Rückblick

Im März 2020 kamen auch die Crash-Propheten nach einer Ewigkeit wieder einmal auf ihre Kosten, konnten sie doch wegen der Corona-Pandemie und dem folgenden Kurstaucher triumphieren. Doch der Markt kam mit einer unglaublichen Wucht zurück und viele Hauptbörsen beendeten das Jahr ausgeglichen oder sogar positiv. Wir hatten die für viele kaum plausible V-Bewegung als mögliches Szenario hingegen auf dem Plan und so relativ früh wieder die ersten Investitionen tätigen können.

Damit aber genug zurückgeschaut. Erstens ist dies an der Börse eher langweilig und hilft zweitens nur bedingt für zukünftige Investitionen. Der Blick nach vorne, also in die Zukunft, bietet da deutlich spannendere Lektüre. Ein Zukunftsthema, nämlich die Informationssicherheit (Cybersecurity), beleuchten wir deshalb in dieser Ausgabe ausführlich.

Am richtigen Ort.ch
Aargauische Kantonalbank

Mögliche Marktprognosen

Ob nach einem über 10 Jahre dauernden Anstieg der Bullenmarkt wirklich in die Jahre gekommen ist, also der Crash bereits vor der Türe wartet, steht nirgendwo geschrieben. Vielleicht spricht sogar immer noch mehr dafür, dass getrieben von der Liquidität der Geldpolitik und der Innovation, der übergeordnete Bullenmarkt am Leben bleibt.

Schauen wir also zuerst einmal optimistisch ins neue Jahr. Wir gehen von einem guten, aber schwierigen Anlagejahr 2021 aus. Deshalb anspruchsvoller, weil die von sinkenden Zinsen getriebenen gleichmässigen Anstiegsphasen langsam vorbei sein dürften. Auch ist die Anlegerstimmung seit der Bekanntgabe der Impfungen (zu) positiv. So ist ziemlich sicher mit zerhackten, wilder schwankenden und damit weniger berechenbaren Marktphasen zu rechnen. Dennoch stehen die Chancen gut, dass wir Ende 2021 in den Indizes wieder höher stehen.

Stimmen zum Anlagejahr 2021

- Der Konsens der Investoren ist verdächtig gleich. Der Dollar wird schwach bleiben, Asien wird besser als der Rest der Welt abschneiden, Value wird Wachstumsaktien schlagen, Rohstoffe steigen weiter, der Reflations-Zyklus kommt (leicht steigende Zinsen) und generell weiter steigende Aktienmärkte.
- Aber eine Tatsache ist, die meisten Sektoren sind aktuell eher heissgelaufen. Seien dies die Wachstumsaktien, Technologie aber auch die zyklischen Titel. Die Extreme werden angeführt von «Clean-Energie/Green-Tech» mit heissen Themen wie Solar und Wasserstoff. Einen gewissen Aufholbedarf haben eigentlich nur Sektoren aus dem Telekombereich, Öl- und Gaswerte sowie Rohstoffe.
- Deshalb ist von einer sich mehrfach im Jahr wiederholenden Rotation dieser Sektoren auszugehen. Es wird Phasen geben, wenn der Markt weniger Risiko nimmt, wo sich defensive Titel wie die Pharmawerte besser schlagen, dann werden wieder Rohstofftitel gefragt sein, wenn an eine Konjunkturerholung geglaubt wird.
- Richtet sich der Blick aber auf die fernere Zukunft, werden Firmen und Sektoren, die Wachstum in sich selber tragen, weniger vom Börsenzyklus abhängig sein. So wird kein Weg daran vorbeiführen, diese Megatrendthemen wie Digitalisierung, Nachhaltigkeit, Ressourcenknappheit und Klimawandel, Datensicherheit, demografischer Wandel mit Gesundheitsthemen, Robotik etc. im Auge zu behalten.

Wir werden Sie, liebe Kundinnen und Kunden, auf diesem möglicherweise eher wilderen Ritt im 2021 begleiten und mit Ihnen die wichtigsten Zukunftsthemen besprechen.

Bis und mit heute gilt aber Folgendes: Wir starten mit grün, sprich bullish, bis das Gegenteil bewiesen ist. Wann dies sein könnte, dazu halten wir Sie auf dem Laufenden.

Newsletter

Unsere Experten geben dazu mit dem quartalsweise publizierten AKB Investment Strategie-Newsletter und den monatlichen AKB Portfolio Management sowie den Anlage-News die Leitplanken vor, wie die Anlagepolitik den aktuellen Gegebenheiten angepasst werden kann.

Alle Publikationen sind kostenlos erhältlich unter
akb.ch/newsletter

Datensicherheit
Ein Thema fürs nächste Jahrzehnt.

Wieso die Datensicherheit so wichtig ist

Es bringt als Laie nichts, auf der technischen IT-Ebene alle möglichen Angriffsoptionen und Löcher verstehen zu wollen. Wichtiger ist es, das Bewusstsein zu erlangen, was die rasante Digitalisierung alles für Möglichkeiten, aber auch welche Gefahren entstehen lässt.

Ein besonderes Augenmerk gilt der digitalen Revolution, wenn sie sich mit der kommenden biologischen und gesundheitlichen verbindet.

Denn die Vergleichbarkeit von biologischen und digitalen Daten ist in vielen Punkten erstaunlich. Die Genetik ist mit ihren riesigen Datensätzen zu einer weitgehend digitalen Wissenschaft geworden. So sind die Modellreihen bei dem aktuell prominenten Corona-Virus meist digital.
Diese Big-Data-Auswertungen mithilfe von künstlicher Intelligenz (KI) werden das Wissen über unseren Körper massiv verbessern.

Und wir liefern die Daten bereits – häufig ohne unser Bewusstsein
Die digitale Selbstvermessung ist über den Sport bei Millionen von Menschen bereits angekommen. So werden Strecke, Puls, Kalorienverbrauch gemessen. Und mit dem Smartphone sind viele weitere Sensoren dazugekommen. Dazu gehören Atmung, Schnarchlautstärke, Blutdruck, Schlafphasen, Zuckerspiegel, Blutsauerstoffsättigung, Hirnaktivität und viele weitere. Und diese heute meist mehrfach im Handy steckenden Sensoren lassen viele Rückschlüsse zu. So ist z.B. aus dem Bewegungsmuster und der Atmung gut ablesbar, ob der Träger bald an einer Grippe erkrankt oder nicht. Mit anderen Worten weiss Apple bereits vor dem iPhone-Besitzer, dass er bald das Bett wegen einer Grippe hüten muss. So werden bereits heute die Daten von Sportlern aus der Smart-Watch ausgelesen, wenn sie z.B. mit Herzproblemen ins Spital eingeliefert werden.

Nicht nur körperliche Daten können mit anderen verknüpft werden und viel über unsere Gesundheit aussagen
Die Algorithmen sind auch scharf auf mögliche Indizes unserer psychologischen Gesundheit. Und im Universum von Social-Media lässt sich da viel aufstöbern. So hat z.B. Facebook bereits einen «Selbstmord-Frühwarn-Algorithmus» am Laufen. Dieser kann durchaus Leben retten oder aber auch grosse Probleme bereiten – dazu später.

So arbeiten alle grossen Digitalkonzerne an Gesundheitsthemen/-produkten
Google hat es auf den 50-Milliarden-Markt Human-Insulin abgesehen. Dort ist sie an der Entwicklung von umfassenden Lösungen, die Geräte, Software, Medizin und professionelle Pflege kombinieren, um ein einfaches und intelligentes Krankheitsmanagement für Menschen mit Diabetes zu ermöglichen. **Samsung** ist daran mit seiner Sensorik-Expertise und einer App die Verabreichung von Medikamenten zu revolutionieren. Und **Apple** hat mit der fix installierten App «Health» eine Datenzentrale für Gesundheit aufgebaut. Sie lässt sich nicht löschen und hat das Ziel, im Verbund mit allen «Schnarch»- und Fitness-Apps den digitalen Körper ganzheitlich zu erfassen. Diese Daten stellt Apple bereits heute anonymisiert der Wissenschaft zur Verfügung. Der Clou liegt darin, dass die Forschung damit nicht nur an gewaltige Daten von «Kranken», sondern auch von «Gesunden» gelangt. Damit lassen sich ganz andere Schlüsse ziehen, als wenn nur Krankenakten zum Studium zur Verfügung stehen.

Alles bestens, oder?

Das tönt auf den ersten Blick alles sehr positiv. Aber der Titel dieser Ausgabe ist ja Datensicherheit. Und was passiert, sollten die Bewerbungsunterlagen zusammen mit dem psychologischen «Fussabdruck» des Bewerbers beim zukünftigen Arbeitgeber landen? Speziell wenn nach einem schweren Schicksalsschlag der Selbstmord-Algo dies gemeldet hätte? Dieser Bewerber wird kaum mehr einen Job finden. Oder wenn die digitale Datenzentrale Ihre nicht sehr sportlichen Records an alle Versicherungen weitergibt? Ist nicht so schlimm, ausser ggf. ein paar Franken höhere Krankenkassen-Prämien, vermutet man auf die Schnelle. Leider falsch. Denn diese Algorithmen geben auch Prognose-Modelle ab und das kann z.B. dann heissen, dass Ihre Lebenserwartung nur noch paar Jahre beträgt. Somit keine neue Arbeitsstelle und kaum die Möglichkeit, eine neue Lebensversicherung abzuschliessen.

Schock-Diagnosen per Link

So gab es schon vor einigen Jahren die ersten Fälle in diese Richtung. Die Frau eines Google-Gründers hatte die Firma 23andme ins Leben gerufen. Wie es der Name sagt, geht es um das Erbmaterial der 23 Chromosomenpaare oder einfacher um die genetische DNA-Analyse. Die Idee ist, dass mit einer Speichelprobe per Internet die Herkunft, also der Stammbaum angefordert werden kann. Das Resultat lautet dann zum Beispiel Sie sind zu 65% Skandinavier und 3% Neandertaler. Quasi als Add-On ist für diejenigen zusätzlich noch ein Link drin, die mehr über ihre Gesundheit wissen möchten. Ein Kunde hat da draufgedrückt und es ziemlich schnell bereut. Denn er bekam folgendes Ergebnis locker-flockig mitgeteilt: Er habe zwei Genmutationen und werde an einer vererbten Gliedergürteldystrophie leiden. Geschockt von dieser am Ende tödlichen Muskelschwund-Diagnose forderte der äusserst begabte Programmierer die Daten an. Nach langem Studium fand er einen Programmierfehler seitens 23andme und im Umkehrschluss, dass er eigentlich gesund sei. Man stelle sich vor, diese Daten gelangten vorher in die falschen Hände. Sind solche Daten einmal im Netz, wird es wie bei einem falschen Bonitätscheck ein Ding der schieren Unmöglichkeit, sie wieder loszuwerden. Nur dürften die Konsequenzen verheerender sein, als wenn die Wohnwandbestellung im Online-Shop ärgerlicherweise wegen schlechter Bonität abgeblockt wurde.

Cybersecurity
Im Homeoffice noch wichtiger.

Mit einer Smartphone-App oder «Alexa» seinen Hund zu Hause überwachen und bei tadellosem Verhalten (Briefträger in Ruhe gelassen) aus der Entfernung ein Leckerli zuschmeissen? Mit dem Fitness-Tracker-Armband bei der Versicherung Prämien sparen? Mit einer Smart-Home-Anwendung, die mit all ihren Kameras und Sensoren den Garten automatisch bewässert, je nachdem welche Wetterprognose «Meteo-Bucheli» gerade auf SRF abgegeben hat?

Das ist die neue, tolle vernetzte Welt! Doch mit der Digitalisierung jedes einzelnen Lebensaspektes steigt auch die Gefahr für Lücken im System. Denn jährlich fallen Millionen von Datensätzen durch verletzliche Sicherheitssysteme und Leaks in unerwünschte Hände. Dies mit drastischen Folgen für Unternehmen und Privatpersonen.

Der erste Hacker wurde MIT-Professor

Ganz neu ist das Phänomen von Computer-Angriffen natürlich nicht. So war bereits 1988 die erste IT-Attacke im Umlauf. Die Ambition dieses Hackers war allerdings «nur», dass er abzuschätzen versuchte, wie gross das Internet sei. Er war die erste Person, die nach dem US-Gesetz über Computerbetrug und -missbrauch verurteilt wurde. Heute arbeitet er als angesehener Professor am MIT. Unterdessen gab es natürlich Dutzende von weiteren Cyberattacken. So waren in den letzten Jahren auch viele grosse Industriekonzerne betroffen. Konkret legte der Angriff direkt ihre (Produktions-)Maschinen und Computer lahm. Die Täter bei solchen Ransomware-Attacken wollen dann Geld (immer häufiger Kryptowährungen), damit sie nach Bezahlung den ordentlichen Betrieb wieder freigeben. Davon können renommierte Firmen wie Norsk Hydro, Porsche, Siemens und viele weitere ein Lied singen.

Benutzerdaten klauen ist lukrativ

Eine weitere Variante ist der Datenklau. Da haben es die Betrüger auf die Userdaten abgesehen. Mit Vorliebe wird der Fokus auf Kreditkarten oder Bankkonten-Daten gerichtet.

Da wurde schon bei vielen Grosskonzernen zugeschlagen. So zählen z.B. JP Morgan, LinkedIn, eBay, Target und Ashley Madison zu den grössten Opfern. So wurden bei letzterem über 35 Millionen User und ihre Daten von der Hacker-Gruppe «The Impact Team» geklaut und veröffentlicht.

Dass sich die Daten einer Dating-Plattform natürlich auch für eine finanzielle Erpressung der Nutzer eignen, versteht sich von selbst. Ein Trend, der anhalten dürfte; getrieben von der Dynamik steigender Mobilfunk-Nutzung, des Internets der Dinge und des Cloud-Computing gewinnt die digitale Sicherheit laufend an Bedeutung. Mit der zweiten Covid-Welle wird es noch offensichtlicher, dass die Leute vermehrt von zu Hause aus arbeiten werden. Hier müssen die Unternehmen künftig noch viel stärker in die IT-Sicherheit, sprich im Bereich Cybersecurity investieren.

95%

aller Vorfälle sind auf menschliches Fehlverhalten zurückzuführen

Anlageidee

iShares Digital Security UCITS ETF (USD, thesaurierend)
Valor: 41860931, **ISIN:** IE00BG0J4C88

Wie einleitend aufzuzeigen versucht wurde, ist die Digital Security ein komplexes Thema. Es müssen die Daten bei den Firmen, aber auch im Privaten geschützt werden. So gibt es auch unzählige IT-Security-Firmen, die sich eines Teils dieses Puzzles angenommen haben. Als Anleger tut man gut daran, in mehrere dieser Gebiete zu investieren. Am einfachsten geht dies mit einem Fonds.

Wieso den iShares Digital Security UCITS ETF kaufen?

- Zukünftiges Wachstumspotenzial durch Engagement im starken Trend zur digitalen Sicherheit.
- Diversifizierung durch eine breite Palette von Unternehmen, die weltweit an verschiedenen Aspekten der Bereitstellung von Datensicherheit beteiligt sind und nach ESG-Kriterien überprüft werden.

Interview
Mit Oliver Münchow von Lucy Security.

Aktuell wird vermehrt im Homeoffice gearbeitet. Dies bedeutet mehr Datenverkehr ausserhalb der Firma und deren Sicherheitsvorkehrungen. Das schreit förmlich nach Sicherheitsproblemen oder schöner gesagt nach Cyber-Security-Herausforderungen. Einer, der sich in diesem Metier sehr gut auskennt, ist Oliver Münchow mit seiner Firma Lucy Security.

Oliver, kannst du mir Genaueres zu euren Dienstleistungen sagen?
Wir bieten hauptsächlich ein Produkt (Software) an und ergänzen das bei Bedarf mit Dienstleistungen (dir wir direkt oder mit Partnern anbieten). Es ist ganz einfach: Hacker attackieren leider sehr oft ahnungslose Mitarbeiter. Das kann ein Phishing-E-Mail sein oder auch etwas anderes. Das Problem dabei: Auf der einen Seite wurde in vielen Betrieben sehr viel in die Informatik-Infrastruktur investiert, aber solange sich die ganze Sicherheit mit einer E-Mail oder SMS an einen Mitarbeiter aushebeln lässt, ist das natürlich nicht so gut. Das zeigen die vielen Pressemitteilungen zu erfolgreichen Attacken (Ransomware & Co. lassen grüssen). Unsere Software setzt da an. Mit interaktiven, webbasierten Schulungsmodulen sensibilisiert man die Mitarbeiter auf diese Risiken. Und wenn man Lust hat, kann man mit Phishingsimulationen dann gleich auch testen, ob die Mitarbeiter die Gefahr auch wirklich verstehen. Wer dann auf einen Link klickt oder sein Passwort auf einer Phishingseite eingibt, muss nochmals nachsitzen und ein Zusatztraining machen. Der IT-Leiter kann dann sehen, wie viele «riskante» Endbenutzer er in seinem Betrieb hat und schafft es mit unserer Lösung dann hoffentlich auch, dieses Risiko über die Zeit etwas abzubauen.

Welche Dienstleistungen sind besonders gefragt?
Primär Schulungen zu allen Themen (Passwortsicherheit, Cloudsicherheit, Phishing etc.). Meistens mischt man diese webbasierten Schulungen mit ganz spezifischen Tipps, die auf die Firma zugeschnitten sind. Phishingsimulationen sind natürlich auch ganz interessant. Und manche Kunden fragen uns auch mal, ob wir nachschauen können, was denn alles bereits schon so im Internet oder Darknet von einem Betrieb zu finden ist. Viele vermuten da wohl zu Recht, dass sich Mitarbeiter in der Vergangenheit nicht immer ganz perfekt verhalten haben. Zu dem Thema haben wir eine weitere Firma gegründet, die solche Recherchen durchführt.

In welchen Branchen und Ländern sind eure Kunden tätig?
Eigentlich in allen Branchen und auf allen Kontinenten. Von der kleinen Arztpraxis bis zu Firmen mit rund 400 000 Mitarbeitern ist alles dabei.

Wie viele Mitarbeitende hat Lucy? In welchen Berufen?
Ich würde sagen Dreiviertel haben bei uns einen technischen Hintergrund (Programmierer, IT Support, Consulting etc.). Am Projekt LUCY sind mittlerweile viele Leute beteiligt. Weil wir Kurse in teils über 30 Sprachen anbieten, haben wir natürlich sehr viele Freelancer, die uns helfen. Wenn ich nur die Fixangestellten zähle, sind das rund 45 Mitarbeiter.

Welche Ausbildung brauchen gute Leute bei dir? Müssen sie Diplome haben, oder wie bei Elon Musk einfach das Handwerk beherrschen?
Ich setze die menschlichen Qualitäten über technische Fachkenntnisse, schliesslich kann man fast alles lernen.

Wir bei der AKB wurden auch schon mit Mails getestet, ob wir irgendwelche gefährlichen Links oder Attachments öffnen. Ist das nicht etwas gar trivial?
Es ist trivial. Aber selbst bei den trivialen E-Mails werden Links geklickt und Attachments geöffnet. Und solange das der Fall ist, muss man die Mitarbeiter auch auf diese Risiken hinweisen.

Was denkst du, würde über die AKB rauskommen, wenn im Darknet recherchiert würde?
Das Übliche – ich hatte ja schon mal einen Blick darauf geworfen. Einige Mitarbeiter registrieren sich mit AKB-Konten auf Webseiten, die eventuell gar keinen Geschäftsbezug haben. Diese Webseiten werden dann gehackt und plötzlich taucht der Mitarbeiter dann im Darknet auf. Meist haben die geleakten Daten aber wenig Relevanz – es sei denn, der Mitarbeiter verwendet überall das gleiche oder ein ähnliches Passwort.

Glaubst du als IT-Security-Spezialist daran, dass irgendwann ein Supergau passiert, weil im Internet of Things (IoT) ein AKW, Staudamm oder Chemielabor sabotiert wird?
In Friedenszeiten nicht.

Wenn ich einen Cyber-Security-Report anschaue, glaube ich mich in einem Kriegsgebiet zu befinden. Denn es wimmelt da von Attacks, Targets, Destabilisierung, Storm, Knocks, Terroristen, Cyber Kill Chain, Hunting und vielem mehr. Ist es so schlimm und gefährlich in der Cyber-Welt?
Es ist vor allem eines: lukrativ. Und solange man so einfach Geld machen kann, wird es nicht besser.

Ist Datenhosting (z.B. Rechenzentrum in den Bergen) für die neutrale Schweiz eine Chance?
Ich denke der physische Sicherheitsaspekt beim Datenhosting wird überschätzt. Daher: nein.

Aber was kann den Schweizer Banken helfen, wenn nicht der Standortvorteil? Gibt es trotzdem Möglichkeiten, einen Vorteil wie früher mit dem Bankkundengeheimnis zu erlangen?
Ich habe viele Banken in verschiedenen Ländern erlebt. Schweizer Banken haben bereits heute einen der höchsten Sicherheitsstandards und sind auch bei den Dienstleistungen, die ja auf einer gut funktionierenden IT beruhen, ganz vorne dabei. Das Bankgeheimnis gibt es nicht mehr. Die Kunden sind aber geblieben. Ich sehe den Vorteil schon heute.

Und die letzte Frage an den Fachmann: Hat dir auch schon jemand mit einer fiesen IT-Attacke ein paar Viren in den PC gelegt?
Nein! Beziehungsweise nicht, dass ich wüsste…

Vielen Dank Oli fürs Interview! Und ich hoffe natürlich, dass wenn Lucy Security einmal den Köder nach mir auswirft, ich nicht darauf hereinfalle.

Abonnieren Sie Ihr persönliches AKB Advisory Inside: akb.ch/newsletter

Wissens-Corner

An dieser Stelle berichtet unser Lernender, an welchem Thema er aktuell arbeitet. Sein Input heute:

FTSE MIB

Dass Italien vom Corona-Virus stark betroffen war und ist, ist uns allen bekannt. Weniger hingegen, wie der italienische Markt, sprich dessen Aktienindex darunter zu leiden hat.
Die *Financial Times Stock Exchange und Milano Italia Borsa*, abgekürzt FTSE MIB, ist einer der italienischen Leitindizes.
Der Index startete 1992 unter dem Namen COMIT 30. Schon 1994 wurde er von der Borsa Italiana übernommen und auf den Namen MIB 30 umbenannt. Dieser wiederum wurde am 3. November vom FTSE MIB als Leitindex abgelöst. Am 1. Juni 2009 trat Standard & Poor's den Index an die FTSE Group ab, die zu 50% der London Stock Exchange Group gehört.
Im Index sind 40 verschiedene Titel untergebracht, von denen auch in der Schweiz einige sehr bekannt sind. Damit ein Unternehmen in den Index aufgenommen werden kann, muss es finanziell handlungsfähig sein sowie eine hohe Liquidität aufweisen können. Erstaunlicherweise ist der Index trotz einiger berühmter Titel wie zum Beispiel Ferrari, Fiat, Moncler oder Generali Versicherungen bei uns eher unbekannt.

Ein sehr spannender Titel ist die Enel S.P.A. Der prozentuale Anteil dieses Titels ist sehr hoch, er beträgt 12% des Gesamtvolumens. Enel ist der grösste Stromversorger in Italien und ausserdem in weiteren 32 Ländern tätig. Das Unternehmen ist 1999 in den Index eingetreten.
Auch Ferrari ist interessant anzusehen; der Konzern ist noch nicht sehr lange in diesem Index zu finden, da er sich erst vor Kurzem von Fiat getrennt hat. Das genaue Eintrittsjahr war 2016.

Ebenso lohnt es sich, einen Blick auf CNH Industrials zu werfen, denn dieses Unternehmen ist ein angesehener Hersteller von Investitionsgütern wie z.B. Nutzfahrzeugen. Bekannte Marken aus dem Produktportfolio sind Iveco oder New Holland. Der Konzern besteht aus 12 Unternehmen. Der prozentuale Anteil ist trotz der Grösse der Firma nur 2,57%, was verhältnismässig wenig ist.

Der Wert des Index ist in der Pandemie stark gesunken. Seitdem befindet er sich in einer Erholungsphase, hat aber immer noch gut 10% Potenzial auf die alten Höchststände.

Nicola Läubli mit Praxisausbilder

Chart-Corner
Analyse vom S&P 500.

Die Fakten

- Mit einem unerwarteten Plus von über 16% hat der wichtigste Index der Welt das Corona-Jahr gemeistert.
- Er vereint die 500 grössten Unternehmen der US-Märkte. So sind Unternehmen aus dem Dow Jones, der NYSE Composite aber eben auch Apple, Amazon, Facebook und Co. aus dem Technologie-Index der Nasdaq vertreten.
- Am Gängelband des S&P 500 hängen viele der Weltmärkte. Eine völlige Abkoppelung ist schwer möglich.

Wie sieht der S&P 500 Index mit Sicht auf die nächsten Monate aus? Ist mit dem Ende der Hausse zu rechnen?

Monatschart (1 Kerze = 1 Monat)

Der über 11 Jahre dauernde Säkulartrend ist immer noch intakt. Erst Kurse unter 3200 Punkten in den nächsten Monaten würden berechtigte Zweifel über das Ende dieser mehrjährigen Aufwärtsbewegung aufkommen lassen. Erwähnt werden muss aber auch, dass vom aktuellen Kursniveau jederzeit eine Korrektur von mind. 15% auftreten kann, ohne den Langfristtrend zu beenden. Die auf höherem Niveau verharrende Volatilität lässt auf eine Schaukelbörse fürs 2021 schliessen. Die immer noch hohe Liquidität kann den Bullenmarkt noch bis ins 1. Halbjahr 2022 mit einem Kursziel von ca. 4250 befeuern, bevor eine mehrjährige Korrektur folgen dürfte.

Tageschart (1 Kerze = 1 Tag)

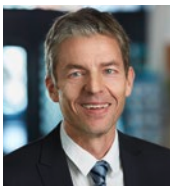
Erste Schwächesignale (Divergenzen) sind sichtbar. Ein kleiner Rücksetzer Richtung 3600 ist in den nächsten Wochen gut möglich. Geht der Support bei 3600 verloren, sind anschliessend mehrere Monate mit erhöhter Volatilität durchaus im Bereich zwischen 3200 und 4000 einzuplanen.

Konklusion

Die Chancen stehen gut, dass wir das Ende des Bullenmarktes noch nicht gesehen haben. Auch wird das Jahr 2021 bei den zu erwartenden Korrekturen somit höchstwahrscheinlich nochmals eine Einstiegschance bieten. Auf der anderen Seite dürfen im ruppiger zu erwartenden Umfeld aber auch Kurse abgesichert und noch besser Teilgewinne an sehr positiven Tagen realisiert werden.

Das Produkt ist keine Kollektivanlage im Sinne des Kollektivanlagegesetzes (KAG) und untersteht keiner Genehmigungspflicht und keiner Aufsicht der Eidgenössischen Finanzmarktaufsicht (FINMA). Dieses Dokument enthält Werbung für Finanzdienstleistungen. Die detaillierten Angaben und Bedingungen entnehmen Sie dem Termsheet. Dieses Dokument stellt keinen Prospekt dar. Alle Angaben sind ohne Gewähr.

Diese Publikation richtet sich an Personen mit Wohnsitz in der Schweiz. Sie richtet sich nicht an Bürger oder Niedergelassene in den USA, CAN oder UK sowie nicht an andere Personen, die Restriktionen (z.B. bezüglich Nationalität, Wohnsitz) unterliegen. Sie enthält Ansichten ohne Offertcharakter. Unsere Quellen sind in der Regel zuverlässig; für Richtigkeit und Vollständigkeit garantieren wir nicht. Alle Angaben sind deshalb ohne Gewähr. Dieses Dokument berücksichtigt weder die spezifischen oder künftigen Anlageziele noch die finanzielle Lage oder individuellen Bedürfnisse des einzelnen Empfängers und ist keine individuelle Beratung. Vor einer Investition muss sich der potenzielle Anleger über die Anlagepolitik, das Anlageziel, Chancen, Risiken sowie Kosten informieren. Eine Investition erfolgt auf eigenes Risiko. Die Aargauische Kantonalbank lehnt jegliche Haftung im Zusammenhang mit möglichen Steuerfolgen ab. Stand Januar 2021. Änderungen sind jederzeit möglich.



Andi Binder
Produktmanagement Anlagen
Aargauische Kantonalbank
advisory@akb.ch