Juli 2019

Asset Management Equity Thematic Insights: Schutz und Sicherheit

5G: Eine sichere Technologie?

Dr. Patrick Kolb, Fondsmanager, Credit Suisse Asset Management

Etwa zwei Drittel der Weltbevölkerung, also ungefähr fünf Milliarden Menschen, sind Mobilfunkteilnehmer und nutzen die drahtlosen Netzwerke der dritten (3G) oder vierten Generation (4G)[1]. Die Verbraucher können damit das volle Potenzial von Smartphones und anderen intelligenten Geräten ausschöpfen. Doch mittlerweile sorgt bereits die nächste Generation für allgemeines Aufsehen: 5G verspricht eine Revolution der Art und Weise, wie wir das Internet nutzen. Diese Technologie hat das Potenzial, durch höhere Netzwerkbandbreite, Geschwindigkeit und Reichweite Effizienzsteigerungen zu erreichen und gleichzeitig in fast allen Bereichen die Wartezeit zu reduzieren. Die Gerätehersteller und Telekommunikationsanbieter arbeiten bereits mit Hochdruck an der Einführung der nächsten Generation, die bis zu hundertmal schneller sein wird als der heutige 4G-Standard. Erwartungen zufolge werden 5G-Netzwerke die Steuerung fahrerloser Autos ebenso ermöglichen wie die Durchführung chirurgischer Operationen aus der Ferne. Bahnbrechende neue Servicedienstleistungen sind denkbar, von der Telemedizin über Notfallmassnahmen bis hin zu einem breiten Spektrum an Industrieanwendungen, die dem Internet der Dinge (Internet of Things, IoT) einen Schub nach vorne verschaffen werden. Alle diese Möglichkeiten benötigen Kommunikationsnetzwerke, und die IT-Sicherheit spielt dabei unserer Meinung nach eine Schlüsselrolle. Wir sind überzeugt, dass sich für Verbraucher, Unternehmen und Regierungen immense Chancen auftun. Die Wirtschaftlichkeit von 5G ist allerdings noch nicht geklärt, doch die Befürworter preisen bereits die enormen Opportunitäten: Unternehmen, die sich die entsprechenden Patente gesichert haben, dürften Lizenzgebühren in Milliardenhöhe einnehmen. Jene Länder mit den grössten und zuverlässigsten Netzwerken werden wahrscheinlich dank der höheren Geschwindigkeit einen wirtschaftlichen Vorsprung erringen. Und die dominanten Gerätehersteller könnten den nationalen Geheimdiensten und Streitkräften einen Vorteil beim Ausspionieren oder sogar Sabotieren der Netzwerke rivalisierender Länder verschaffen.

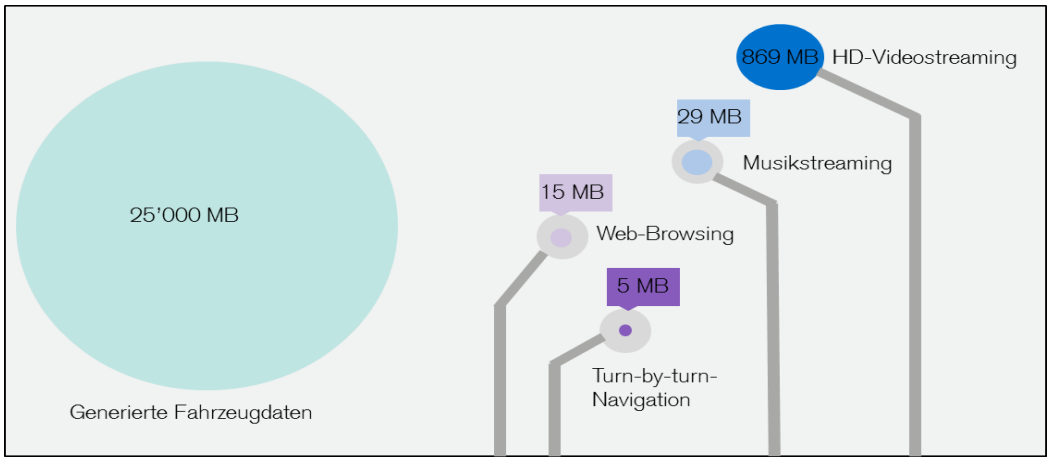
Ist 5G sicher?

Das Aufregendste an 5G ist, wie sich aufgrund seiner Geschwindigkeit das Internet verändern wird. Bislang werden im Internet lediglich Daten von A nach B transportiert. Es ist zwar heute

[1] Quelle: GSMA (2017): Global Mobile Trends 2017, URL: https://www.gsma.com/globalmobiletrends/, letzter Zugriff am 12. Juni 2019

schon möglich, mit dem Internet verbundenen Autos Fahranweisungen zuzuschicken – doch das ist im Grunde nichts anderes als der Erhalt von E-Mails, also die Weitergabe bestehender Informationen. Autonome Autos unterscheiden sich hiervon grundlegend: Durch das 5G-Netzwerk können Computer eine wahre Flut von Informationen aus zahllosen Eingangssensoren für Entscheidungsprozesse in Echtzeit nutzen. Was das bedeutet zeigt eine Studie von Richter (2017): Diese besagt, dass vernetzte Autos stündlich bis zu 25 Gigabyte an Daten erzeugen können. Wie Abbildung 1 zeigt, entspricht diese Datenmenge fast 30 Stunden HD-Videostreaming oder mehr als einem Monat Musikstreaming rund um die Uhr.

Abb. 1: Durch vernetzte Autos generierte Daten im Vergleich zur Datennutzung bei Online-Aktivitäten (pro Stunde)



Quellen: Credit Suisse, Richter (2017): Big Data on Wheels, in: Statista, 9. Feb. 2017, URL: https://www.statista.com/chart/8018/connected-car-data-generation/ , letzter Zugriff am 12. Juni 2019

Bei 5G dreht es sich nicht nur um Netzwerkaufbau, sondern auch um die Frage, ob dieses Netzwerk für die versprochenen Innovationen sicher genug sein wird. Kommen wir zurück zum Beispiel der autonomen Fahrzeuge: Wollen wir, dass dank 5G autonom fahrende Autos und Lkw zusammenstossen, nur weil jemand das Netzwerk gehackt hat? Wenn durch 5G beispielsweise ein ferngesteuerter chirurgischer Eingriff ermöglicht wird – wie kann beispielsweise vermieden werden, dass eine unbefugte Personen eine Operation manipulieren kann?

Unserer Auffassung nach wird sich das künftige Wechselspiel zwischen 5G-Netzwerken, Computing-Ressourcen und Endverbrauchern massiv auf den IT-Sicherheitsbereich auswirken. Durch den Ausbau von Verbindungen durch 5G wird sich die Zahl an Netzwerk-Endpunkten erhöhen. Hierdurch wird es auch mehr mögliche Pforten geben, über die Angreifer sich Zugang zu den Netzwerken verschaffen können. Ist den Angreifern dieser Schritt erst gelungen, können sie viel schneller und umfassender Schaden anrichten als bis anhin.

Die möglichen Gefahrenquellen reichen von mit 5G-Netzwerk verbundener kritischer Infrastruktur (einschliesslich Stromnetzen, Wassersystemen und Gasleitungen) und einem Zusammenbruch von Kommunikationssystemen über den massenhaften Ausfall der entsprechenden Dienstleistungen bis hin zum unautorisierten Zugriff auf sensible und persönliche Daten. Die Verlagerung der Rechenleistung an den Rand der Netzwerke («Edge Computing») für die Ausführung neuer, geschäftskritischer Unternehmensanwendungen[2] wird die Zahl der potenziellen Angriffspunkte drastisch erhöhen. Damit steigen auch die Sicherheitsrisiken: In den aktuellen 4G-Netzwerken können grosse Botnets für breit angelegte Distributed-Denial-of-Service-Angriffe (DDoS-Angriffe) auf Websites eingesetzt werden. In der 5G-Welt von morgen dagegen könnte dasselbe Botnet ein gesamtes Netzwerk selbstfahrender Autos lahmlegen. Die zahllosen durch globale Lieferketten verbundenen Fernsensoren und intelligenten Geräte werden die Komplexität von Sicherheitsnetzwerken drastisch erhöhen. In Kombination mit der enormen durch 5G generierten Datenmenge wird es damit noch schwerer, Anomalien aufzuspüren[3]. Aktuelle Studien haben mögliche Schwachstellen in der 5G-Netzwerkarchitektur aufgedeckt, die das Versprechen auf eine neue Ära der Innovation zu

[2] Beim Edge Computing werden Rechen-/Speicherleistungen zunehmend in Richtung des Endgerätes verlagert. Dies hilft, Wartezeiten und Transportkosten zu senken und verschiebt Anwendungen, Daten und die Rechenleistung weg von zentralen Knoten und näher an den Endverbraucher. Hauptvorteile sind Senkung von Datenvolumen, -verkehr und -übertragungsstrecke.

[3] Quelle: CPO Magazine (2019): 5G and the Future of Cybersecurity, in: CPO Magazine, 4. April 2019, URL: https://www.cpomagazine.com/cyber-security/5g-and-the-future-of-cybersecurity/, letzter Zugriff am 12. Juni 2019

untergraben drohen. In diesem Zusammenhang möchten wir auf drei wissenschaftliche Studien hinweisen:

- Laut Wissenschaftlern der ETH Zürich, der Université de Lorraine/INRIA und der University of Dundee wurde kürzlich eine neue Schwachstelle im Sicherheitsprotokoll «Authentication and Key Agreement» (AKA) entdeckt, die es Cyberkriminellen erlauben könnten, 5G-Kommunikation abzufangen und Daten zu stehlen. Darüber hinaus könnte die AKA-Lücke dazu führen, dass Benutzern zu Unrecht für die Verwendung des 5G-Netzwerks durch Dritte Gebühren berechnet werden[4].
- In einer weiteren, durch die Europäische Agentur für Netz- und Informationssicherheit (ENISA) durchgeführten Studie wurden Mängel an zwei Signalisierungsprotokollen in 2G-, 3G- und 4G-Netzwerken (sog. SS7/Diameter) festgestellt, die auch in 5G-Netzwerken auftreten könnten. Die möglichen Angriffspunkte in den Signalisierungsprotokollen könnten dazu führen, dass der Netzwerkverkehr abgehört oder Gegenstand von Spoofing-Angriffen wird, Standorte abgefangen oder Telefone vom Netzwerk getrennt werden. Darüber hinaus warnt die ENISA davor, dass die Verwendung gängiger Internetprotokolle (etwa HTTP) in 5G-Netzwerken dazu führen kann, dass entdeckte Software-Schwachstellen in diesen Protokollen auch auf mobile Netzwerke übertragen werden könnten[5].
- Positive Technologies Inc., ein globaler Anbieter von Sicherheitslösungen für Unternehmen, hat potenzielle Angriffspunkte in mobilen Netzwerken untersucht. Den Verfassern zufolge ist gegenwärtig kein mobiles Netzwerk als sicher zu bezeichnen, kein Betreiber ist in der Lage, die Sicherheit seines Netzwerks zu gewährleisten. Die Wissenschaftler haben im Rahmen ihrer Studie mehrere Cyberangriffe durchgeführt und waren bei 80% ihrer Denial-of-Service-Angriffe (die zu Betriebsstörungen führen), 77% ihrer Datenleck-Angriffe und 67% ihrer Betrugsangriffe erfolgreich gewesen[6].

Fazit und Folgerungen

5G könnte zu neuen Herausforderungen im IT Sicherheitsbereich führen. Angesichts der bevorstehenden Einführung suchen Unternehmen bereits vermehrt nach Dienstleistern, die ein stabiles Netzwerk mit robusten Cybersicherheits-Mechanismen anbieten können zwecks Gewährleistung der Sicherheit ihrer Kunden. In einer von Ericsson durchgeführten Studie, die 20 der weltweit grössten Mobilfunkanbieter einschloss, stuften 90 % der Teilnehmer IT-Sicherheit als einen wesentlichen Punkt bei der 5G-Einführung ein[7]. Sicherheitslücken stellen ein Unternehmensrisiko für Anbieter dar, die für eine verlässliche und sichere Verfügbarkeit sicherheitskritischer Verbraucheranwendungen und unternehmenskritischer Mobilfunkdienste von Unternehmen sorgen müssen. Der Aufbau einer guten Reputation wird für Mobilfunkanbieter von entscheidender Bedeutung sein. Daraus müssen Anleger unserer Auffassung nach zwei Schlüsse ziehen:

- Erstens: Das wachsende Bewusstsein für neue Sicherheitslücken im Bereich 5G wird ohne Zweifel zu verstärkten Bemühungen führen, die Kommunikationsnetzwerke zu schützen. Zu den aktuellen Gefahren zählen die nicht klar definierten Ziele im Bereich Cybersicherheit und der Mangel an Genauigkeit bei der Festlegung von Standards[8]. Unserer Meinung nach sollten die zentralen 5G-Sicherheitsinitiativen Tools auf Basis künstlicher Intelligenz (KI) beinhalten, damit Gefahren schneller erkannt werden können. Darüber hinaus gibt es Klärungsbedarf im Bereich Zugriffskontrollen und der Frage, wie eine integrierte Sicherheitsarchitektur an ein sich veränderndes Netzwerkumfeld angepasst werden kann.

---

[4] Quelle: Basin et al. (2018): A Formal Analysis of 5G Authentication, Conference Paper, in: ETH Zürich Research Collection, 15. Oktober 2018, URL: https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/300545/CCS18_finalcrc2_Fixed-Typo.pdf?sequence=1&isAllowed=y., letzter Zugriff am 12. Juni 2019

[5] Quelle: ENISA (2018): Signalling Security in Telecom SS7/Diameter/5G: EU level assessment of the current situation, März 2018, URL: https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g., letzter Zugriff am 12. Juni 2019

[6] Quelle: Positive Technologies (2016): Primary Security Threats for SS7 Cellular Networks, URL: https://www.ptsecurity.com/upload/ptcom/SS7-VULNERABILITY-2016-eng.pdf

[7] Quelle: Ericsson (2018): Exploring IoT Strategies, Paper, URL: https://www.ericsson.com/en/internet-of-things/trending/exploring-iot-strategies., letzter Zugriff am 12. Juni 2019

[8] *«… Wir denken, dass einige kritische Sicherheitsziele noch nicht erreicht wurden, sofern nicht andere Faktoren gegeben sind, die im Standard bisher nicht berücksichtigt werden»*, Quelle: Basin et al. (2018)., S.1.

- Zweitens: Sicherheit im Bereich 5G erfordert einen neuen, ganzheitlichen und transformativen Ansatz: Prävention wird wichtiger als je zuvor. Ein höheres Mass an Automatisierung im Sicherheitsbereich ist ebenso nötig wie die Integration von Big-Data-Analysen. Wir sind derzeit davon überzeugt, dass die Einführung von 5G uns in unbekanntes Terrain führen wird und unvorhergesehene Konsequenzen nicht auszuschliessen sind. Daher glauben wir, dass die auf den Bereich IT-Sicherheit spezialisierten Unternehmen unmittelbar von den neuen 5G-Sicherheitslösungen profitieren werden.

Unserer Auffassung nach ist IT-Sicherheit eine unverzichtbare Voraussetzung für 5G. Im Zuge ihrer Verbreitung werden neue Unternehmen mit führender Technologie unserer Meinung nach bestens positioniert sein, etablierten Anbietern Marktanteile abzunehmen. Die Entwicklungen machen deutlich, dass ein Best-of-Breed-Ansatz erforderlich ist. Die Anbieter solcher Produkte und Dienstleistungen sind häufig junge und innovative Unternehmen aus dem Small- und Mid-Cap-Segment. Wir sind überzeugt, dass das Thema IT-Sicherheit ein immer präsenterer Teil unseres Alltagslebens wird und als Folge der anhaltenden Digitalisierung unserer Gesellschaft immer kritischer werden.

Das übergreifende Thema Sicherheit und Schutz bietet für geduldige Investoren eine sehr attraktive langfristige Wachstumschance. Deswegen halten wir Anteile einer Reihe junger und innovativer Firmen, die neue Sicherheitslösungen im Bereich 5G und Internet der Dinge entwickeln. Unternehmen, welche die Skalierbarkeit auf dem Niveau von Cloud Computing, Prognosesicherheit und Kontrollen sowie erstklassige Schutzmechanismen für mobile Netzwerke und Firewalls der nächsten Generation bieten, sind unserer Meinung nach perfekt positioniert.

Fonds Charakteristika
Credit Suisse (Lux) Global Security Equity Fund

Fondsmanagement	Credit Suisse Fund Management S.A.
Portfoliomanager	Credit Suisse Asset Management (Schweiz) AG, Zürich Dr. Patrick Kolb
Fondsmanager seit	01. März 2007
Fondsdomizil	Luxemburg
Fondswährungen	USD, EUR, CHF
Fondsauflegung	19. Oktober 2006
Verwaltungsgebühren p.a.	Für Anlageklassen AH, B, BH und CB: 1.60%; für Anlageklasse EB und EBH: 0.90% Für Anlageklassen IB und IBH: 0.90%; für Anlageklassen UA, UB und UBH: 1.00%; für Anlageklasse MBH: 0.70%
TER (per 31.05.2018)	Klasse B 2.01%, Klasse IB 1.15%, Klasse BH in CHF 2.02%, Klasse BH in EUR 2.00%, Klasse EB[2] 1.10%, Klasse UA 1.29%, Klasse UB 1.32%, Klasse UBH in CHF 1.31%, Klasse UBH in EUR 1.32%, Klasse IBH in CHF 1.15%, Klasse IBH in EUR: 1.15%, Klasse MBH in EUR: 0.91%, Klasse EBH[2] in EUR:1.11%, Klasse EBH[2] in CHF 1.14% (geschätzt), Klasse AH in EUR 1.96%
Maximaler Ausgabeaufschlag	5% für alle Anlageklassen ausser Klassen IB, IBH, EB, EBH (maximal 3%) und MBH (maximal 1%)
Single Swinging Pricing (SSP)[1]	Ja
Benchmark	MSCI World (NR)
Anlageklassen	Klasse B, IB, UA, UB, EB in USD, Klasse BH, IBH, EBH und UBH in CHF, Klasse AH, BH, EBH, IBH, MBH und UBH in EUR
ISIN	Klasse B in USD: LU0909471251 Klasse IB in USD: LU0971623524 Klasse IBH in EUR: LU1644458793 Klasse IBH in CHF: LU1457602594 Klasse BH in EUR: LU0909472069 Klasse UBH in CHF: LU1144416515 Klasse EBH in CHF[2]: LU1886389292 Klasse UA/UB in USD: LU1557207195/LU1144416432 Klasse UBH in EUR: LU1144416606 Klasse MBH in EUR LU1692472852 Klasse EB in USD[2]: LU1042675485 Klasse BH in CHF: LU0909471681 Klasse EBH in EUR[2]: LU1575200081 Klasse AH in EUR: LU1584043118 **Wir möchten Sie darauf hinweisen, dass eventuell nicht alle Anteilklassen in Ihrem Land verfügbar sind.**

Quelle: Credit Suisse, 30. Juni 2019

[1] SSP ist ein Verfahren zur Berechnung des Nettoinventarwerts (NAV) eines Fonds. Ziel ist es, die bestehenden Anleger vor der Finanzierung indirekter Transaktionskosten zu schützen, die durch ein- und austretende Anleger verursacht werden. Bei Nettozuflüssen wird der NAV am jeweiligen Bewertungstag nach oben,

bei Nettoabflüssen hingegen nach unten angepasst. Die Anpassung des NAV kann im Hinblick auf den Nettomittelfluss einem Schwellenwert unterliegen. Weitere Informationen entnehmen Sie bitte dem Verkaufsprospekt. [2] nur für institutionelle Anleger.

Fondsrisiken

Credit Suisse (Lux) Global Security Equity Fund

- Kein Kapitalschutz: Anleger können den in dieses Produkt investierten Betrag ganz oder teilweise verlieren.
- Der Schwerpunkt auf Unternehmen im Bereich Schutz und Sicherheit kann zu signifikanten Engagements in einem bestimmten Sektor/einer bestimmten Region führen.
- Das Engagement in Small und Mid Caps kann zu einer höheren kurzfristigen Volatilität führen und Liquiditätsrisiken in sich bergen.
- Aufgrund der Möglichkeit eines erhöhten Engagements in Schwellenländern kann der Fonds durch politische und wirtschaftliche Risiken in diesen Ländern beeinträchtigt werden.
- Aktienmärkte können volatile sein, besonders kurzfristig.

CREDIT SUISSE

credit-suisse.com/assetmanagement

Generell wichtige Informationen für alle Länder

Disclaimer

Die bereitgestellten Informationen dienen Werbezwecken. Sie stellen keine Anlageberatung dar, basieren nicht auf andere Weise auf einer Berücksichtigung der persönlichen Umstände des Empfängers und sind auch nicht das Ergebnis einer objektiven oder unabhängigen Finanzanalyse. Die bereitgestellten Informationen sind nicht rechtsverbindlich und stellen weder ein Angebot noch eine Aufforderung zum Abschluss einer Finanztransaktion dar.

Diese Informationen wurden von der Credit Suisse Group AG und/oder mit ihr verbundenen Unternehmen (nachfolgend "CS") mit grösster Sorgfalt und nach bestem Wissen und Gewissen erstellt. Die in diesem Dokument enthaltenen Informationen und Meinungen repräsentieren die Sicht der CS zum Zeitpunkt der Erstellung und können sich jederzeit und ohne Mitteilung ändern. Sie stammen aus Quellen, die für zuverlässig erachtet werden. Die CS gibt keine Gewähr hinsichtlich des Inhalts und der Vollständigkeit der Informationen und lehnt, sofern rechtlich möglich, jede Haftung für Verluste ab, die sich aus der Verwendung der Informationen ergeben. Ist nichts anderes vermerkt, sind alle Zahlen ungeprüft. Die Informationen in diesem Dokument dienen der ausschliesslichen Nutzung durch den Empfänger. Weder die vorliegenden Informationen noch Kopien davon dürfen in die Vereinigten Staaten von Amerika versandt, dorthin mitgenommen oder in den Vereinigten Staaten von Amerika verteilt oder an US-Personen (im Sinne von Regulation S des US Securities Act von 1933 in dessen jeweils gültiger Fassung) abgegeben werden. Ohne schriftliche Genehmigung der CS dürfen diese Informationen weder auszugsweise noch vollständig vervielfältigt werden.

Diese Fonds sind in Luxembourg domiziliert. Vertreter in der Schweiz ist die Credit Suisse Funds AG, Zürich. Zahlstelle in der Schweiz ist die Credit Suisse (Schweiz) AG, Zürich. Der Prospekt, der vereinfachte Prospekt und/oder die wesentlichen Informationen für den Anleger sowie die jährlichen und halbjährlichen Berichte können gebührenfrei bei dem Vertreter und bei jeder Geschäftsstelle der CS in der Schweiz bezogen werden.

Ihre personenbezogenen Daten werden in Übereinstimmung mit der Datenschutzerklärung der Credit Suisse verarbeitet, die an Ihrem Wohnsitz über die offizielle Website der Credit Suisse https://www.credit-suisse.com abrufbar ist. Die Credit Suisse Group AG und ihre Tochtergesellschaften nutzen unter Umständen Ihre grundlegenden personenbezogenen Daten (z.B. Kontaktangaben wie Name und E-Mail-Adresse), um Ihnen Marketingunterlagen in Zusammenhang mit ihren Produkten und Dienstleistungen bereitzustellen. Falls Sie solche Unterlagen nicht mehr erhalten möchten, wenden Sie sich bitte jederzeit an Ihre Kundenberaterin oder Ihren Kundenberater.

Wichtige Informationen für Anleger in Österreich und Deutschland

Wichtige Hinweise

Dieses Dokument wurde von der Credit Suisse AG und / oder mit ihr verbundenen Unternehmen (nachfolgend «CS») mit größter Sorgfalt und nach bestem Wissen und Gewissen erstellt. Die in diesem Dokument geäußerten Meinungen sind diejenigen der CS zum Zeitpunkt der Redaktion und können sich jederzeit und ohne Mitteilung ändern. Ist nichts anderes vermerkt, sind alle Zahlen ungeprüft.

Das Dokument dient ausschließlich Informationszwecken und der Nutzung durch den Empfänger. Es stellt weder ein Angebot, noch eine Empfehlung zum Erwerb oder Verkauf von Finanzinstrumenten oder Bankdienstleistungen dar und entbindet den Empfänger nicht von seiner eigenen Beurteilung. Insbesondere ist dem Empfänger empfohlen, gegebenenfalls unter Einschaltung eines Beraters, die Informationen in Bezug auf die Vereinbarkeit mit seinen eigenen Verhältnissen, auf juristische, regulatorische, steuerliche, u.a. Konsequenzen zu prüfen.

Dieses Dokument darf ohne schriftliche Genehmigung der CS weder auszugsweise noch vollständig vervielfältigt werden. Das vorliegende Dokument ist ausschließlich für Anleger in Deutschland und Österreich bestimmt. Es richtet sich ausdrücklich nicht an Personen, deren Nationalität oder Wohnsitz den Zugang zu solchen Informationen aufgrund der geltenden Gesetzgebung verbieten. Weder das vorliegende Dokument noch Kopien davon dürfen in die Vereinigten Staaten versandt oder dahin mitgenommen werden oder in den Vereinigten Staaten oder an eine US-Person abgegeben werden (im Sinne von Regulation S des US Securities Act von 1933 in dessen jeweils gültigen Fassung).

Mit jeder Anlage sind Risiken, insbesondere diejenigen von Wert- und Ertragsschwankungen verbunden. Bei Fremdwährungen besteht zusätzlich das Risiko, dass die Fremdwährung gegenüber der Referenzwährung des Anlegers an Wert verliert. Historische Wertentwicklungen und Finanzmarktszenarien sind kein verlässlicher Indikator für laufende und zukünftige Ergebnisse. Es kann außerdem nicht garantiert werden, dass die Performance des Vergleichsindex erreicht oder übertroffen wird.

In Zusammenhang mit diesem Anlageprodukt bezahlt die Credit Suisse AG und/oder mit ihr verbundene Unternehmen unter Umständen Dritten oder erhält von Dritten als Teil ihres Entgelts oder sonst wie eine einmalige oder wiederkehrende Vergütung (z.B. Ausgabeaufschläge, Platzierungsprovisionen oder Vertriebsfolgeprovisionen). Für weitere Informationen wenden Sie sich bitte an Ihren Kundenberater. Zudem können im Hinblick auf das Investment Interessenkonflikte bestehen.

Bei diesem Dokument handelt es sich um Marketingmaterial, das ausschließlich zu Werbezwecken verbreitet wird. Es darf nicht als unabhängige Wertpapieranalyse gelesen werden.

Der in diesem Dokument erwähnte Anlagefonds luxemburgischen Rechts ist ein Organismus für gemeinsame Anlagen in Wertpapieren (OGAW) gemäß Richtlinie 2009/65/EG, in der geänderten Fassung.

Zeichnungen sind nur auf Basis des aktuellen Verkaufsprospekts, der wesentlichen Anlegerinformationen und des letzten Jahresberichts (bzw. Halbjahresberichts, falls dieser aktueller ist) gültig. Diese Unterlagen sowie die Vertragsbedingungen und/oder Statuten sind kostenlos in deutscher/englischer Sprache bei der Credit Suisse (Deutschland) Aktiengesellschaft, Taunustor 1, 60310 Frankfurt am Main, Deutschland und UniCredit Bank Austria AG, Schottengasse 6–8, A-1010 Wien, Österreich erhältlich.

Credit Suisse Fund Services Luxembourg S.A., 5, rue Jean Monnet, 2180 Luxemburg ist die Zentrale Verwaltungsstelle des Fonds in Deutschland.

Credit Suisse (Deutschland) AG, Taunustor 1, D–60310 Frankfurt am Main ist die Informationsstelle des Fonds in Deutschland.

UniCredit Bank Austria AG, Schottengasse 6–8, A-1010 Wien, ist die Zahlstelle des Fonds in Österreich.

CREDIT SUISSE (DEUTSCHLAND) Service-Line:
AKTIENGESELLSCHAFT Telefon: +49 (0) 69 7538 1111
Taunustor 1 Telefax: +49 (0) 69 7538 1796
D-60310 Frankfurt am Main E-Mail: investment.fonds@credit-suisse.com

Copyright © 2019 Credit Suisse Group AG und/oder mit ihr verbundene Unternehmen. Alle Rechte vorbehalten.