

Asset Management Equity Business

Thematische Aktien: Sicherheit und Schutz



Ist „IT Insecurity“ die neue Normalität? Dr. Patrick Kolb, Fund Manager, Credit Suisse

„Es gibt zwei Arten von Unternehmen: diejenigen, die gehackt wurden, und diejenigen, die noch nicht wissen, dass sie gehackt wurden.“¹

John Chambers, CEO von Cisco

Liebe Leserinnen und Leser, aufgrund der weltweit steigenden Anzahl von Hacker-Angriffen stellt die IT-Sicherheit ein zentrales gesellschaftliches und ökonomisches Problem dar. Die zuletzt in den Nachrichten diskutierten Datenschutzverletzungen wie etwa bei JP Morgan, dem US Office of Personnel Management (OPM, Amt für Personalverwaltung der Vereinigten Staaten), Sony Pictures, Target oder Ashley Madison zeigen, dass derartige Vorfälle gravierende Konsequenzen haben können. Wir vertreten die Auffassung, dass neue IT-Strategien entwickelt werden müssen, um den potenziellen Schaden solcher Vorfälle vermeiden zu können.

In diesem Artikel möchten wir kurz die derzeitige Situation im Bereich IT-Sicherheit analysieren und die Frage stellen, was Unternehmen zur Neutralisierung

dieser Bedrohung tun können. Abschließend werden wir ein kurzes Fazit ziehen.

Projekt Einstein 3: Noch vor zwei Jahren war es hochmodern ...

Als die US-Regierung im Jahr 2012 mit der Einführung des Projekts Einstein 3 begann, war es auf dem neuesten Stand der damaligen IT-Sicherheitstechnik: Das Einstein-Programm wurde 2003 ursprünglich als „Intrusion Detection System“, ein Einbruchmeldesystem, von der US-Regierung entwickelt. Das Ziel war die Überwachung der Netzwerke von US-Regierungsstellen und -behörden im Hinblick auf unbefugten Datenverkehr.² Laut Bloomberg war dieses System darauf ausgelegt, Angriffe zu stoppen, bevor Regierungscomputer überhaupt erreicht werden konnten. Die fünf größten Internetprovider nutzen dieses Tool zur Überprüfung des enormen Datenvolumens im Zusammenhang mit sensiblen Netzwerken und verwenden digitale Signaturen zur Erkennung und Löschung von Hacker-Tools. Es scheint jedoch, als ob Hacker dieses System bereits erfolgreich umgehen können. Mittlerweile hinterlassen sie keine digitalen Signaturen mehr, die vom Einstein-System aufgedeckt werden könnten.³

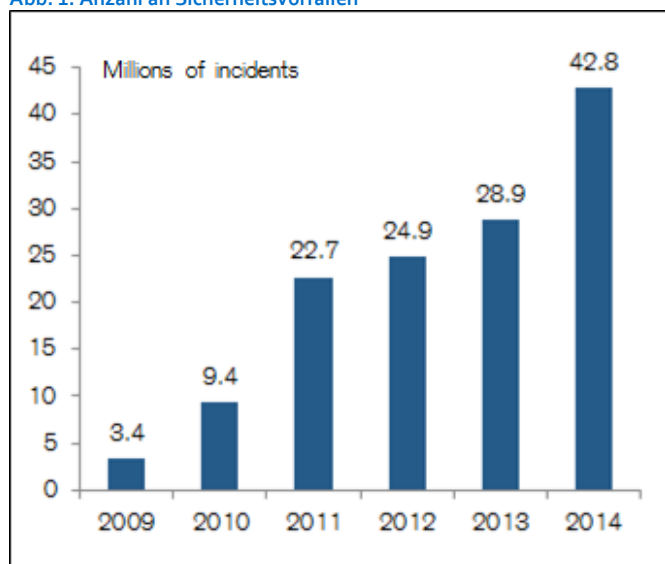
¹ Quelle: Chambers (2015): What does the Internet of Everything mean for security?, in: World Economic Forum Blog, Jan. 21st 2015, URL: <https://agenda.weforum.org/2015/01/companies-fighting-cyber-crime/>, 3.9.2015.

² Quelle: Department of Homeland Security (2004): Privacy Impact Assessment EINSTEIN Program, Sept. 2004, p. 4, URL: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein.pdf, 31.8.2015.

³ Quelle: Bloomberg (2015): China Hackers Got Past Costly U.S. Computer Security with Ease, in: Bloomberg, June 6th 2015, URL:

Ein weiterer besorgniserregender Trend ist die Beobachtung, dass Cyberkriminelle sich schneller technologisch weiterentwickeln, als die betroffenen Unternehmen sich verteidigen können. Laut der Financial Times ist beispielsweise die kryptische Ransomware eines der bei Hackern beliebtesten neuen Tools. Mit dieser Anwendung werden Dateien, Fotos und andere digitale Medien eines Opfers solange zur Erpressung genutzt, bis ein Lösegeld bezahlt wird (normalerweise zwischen USD 300 und USD 500).⁴ Der von Symantec veröffentlichte Internet Security Threat Report 2015 zeigt, dass Ransomware-Angriffe sprunghaft angestiegen sind, von 11000 Angriffen pro Tag im Jahr 2013 auf über 24000 Angriffen täglich im Jahr 2014 (+ 113 %).⁵

Abb. 1: Anzahl an Sicherheitsvorfällen



Quelle: PwC (2015)

PricewaterhouseCoopers (PwC) stellte in seiner diesjährigen Umfrage unter 9700 Branchenteilnehmern fest, dass es im Jahr 2014 geschätzt 42,8 Millionen Sicherheitsvorfälle gab. Wie Abb. 1 zeigt, ist dies ein Anstieg um 48 % im Vergleich

<http://www.bloomberg.com/news/articles/2015-06-06/china-hackers-got-past-costly-u-s-computer-security-with-ease>, 31.8.2015.

⁴ Quelle: The Financial Times (2015): Cyber criminals lead race to innovate, in: The Financial Times, April 14th 2015, URL: <http://www.ft.com/intl/cms/s/0/94dcee3a-e21a-11e4-9995-00144feab7de.html#axzz3ceNx2Hz4>, 31.8.2015.

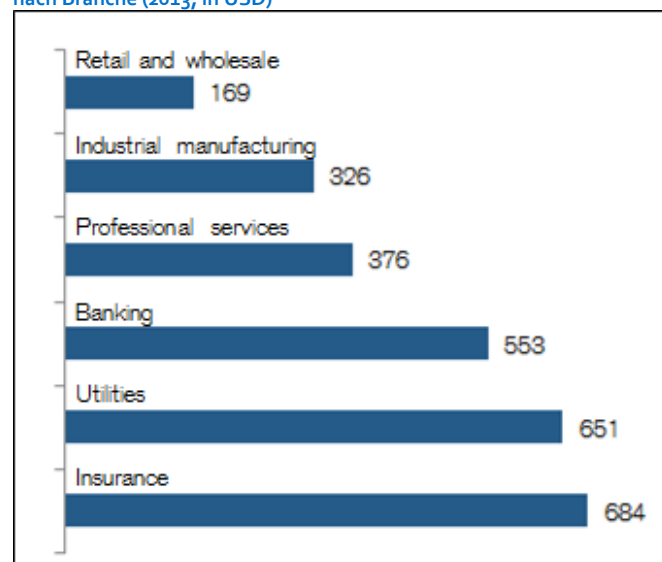
⁵ Quelle: Symantec (2015): Internet Security Threat Report 2015, Vol. 20, p. 93, URL: https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf, 1.9.2015.

zu 2013, was eine Beschleunigung gegenüber den Vorjahren zeigt.⁶

... daher sind wir der Meinung, dass IT-Sicherheit immer wichtiger wird

Wir sind davon überzeugt, dass die IT-Sicherheit zum Dreh- und Angelpunkt für den Geschäftserfolg werden wird, da Kunden unter Umständen ihr Vertrauen in Unternehmen, die nicht sorgfältig mit Daten umgehen, verlieren werden. Besonders die Finanzindustrie hat Hunderte von Millionen Dollar in die Sicherheit ihrer Netzwerke investiert und Tausende der klügsten Köpfe im Technologiebereich eingestellt. Und trotzdem ereignen sich immer noch schwerwiegende Sicherheitsverletzungen, wie kürzlich aufgetretene Vorfälle zeigen.⁷

Abb. 2: Weltweite Ausgaben für Informationssicherheit pro Mitarbeiter nach Branche (2013, in USD)



Quelle: The Wall Street Journal (2014)

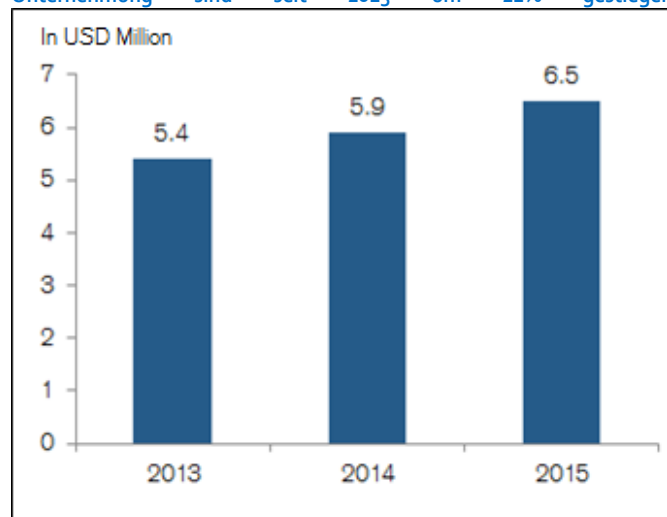
Laut dem Wall Street Journal planen Finanzdienstleistungsunternehmen in den nächsten zwei Jahren, ihre Budgets für Cybersicherheit um bis zu USD 2 Mrd. zu erhöhen. Abb. 2 zeigt die weltweiten Ausgaben für IT-Sicherheit pro Mitarbeiter nach Branche. Deutlich zu sehen ist, dass die Banken- und

⁶ Quelle: PricewaterhouseCoopers (2014): Managing cyber risks in an interconnected world, Sept. 30th 2014, p. 7, URL: <http://www.dol.gov/ebsa/pdf/erisaadvisorycouncil2015security3.pdf>, 31.8.2015.

⁷ Quelle: Reuters (2014): JP Morgan hack exposed data of 83 million, among biggest breaches in history, in: Reuters, Oct. 2nd 2014, URL: <http://www.reuters.com/article/2014/10/03/us-jpmorgan-cybersecurity-idUSKCN0HR23T20141003>, 2.9.2015.

Versicherungsbranche mehr als USD 550 pro Mitarbeiter ausgeben. Insgesamt belaufen sich die Ausgaben der Banken und Versicherungen auf ca. USD 4,1 Mrd.⁸ Trotzdem steigt die Anzahl der Hacks und die damit verbundenen Kosten immer weiter an. Abb. 3 zeigt, dass die Kosten von Datenschutzlecks in den USA von USD 5,4 Mio. im Jahr 2013 auf mittlerweile USD 6,5 Mio. angestiegen sind.⁹ Die durchschnittliche Anzahl aufgedeckter Vorfälle stieg von 4628 (2013) auf knapp 5000 im letzten Jahr.¹⁰ Obwohl der finanzielle Schaden für diese Unternehmen im Vergleich zu ihrem Konzernumsatz derzeit relativ gering ist, leidet – vor allem bei großen Unternehmen – ihre Reputation.

Abb. 3: Die durchschnittlichen Kosten eines Datenlecks pro Unternehmung sind seit 2013 um 21% gestiegen



Quelle: The Ponemon Institute (2015)

Ein weiteres Problem ist, dass viele globale Banken aufgrund der Fusionen über tendenziell veraltete und inkompatibel zusammengetragene Technologien verfügen. Oder sie haben andere Handelsplattformen, die nicht einfach oder kostengünstig auf neue Systeme übertragen werden können. Und schließlich sind Investitionen in IT-Sicherheitstechnologien bereits für große Banken sehr teuer. Für ihre kleinen oder mittelgroßen Mitbewerber sind sie jedoch beinahe unbezahlbar. Laut der Financial Times setzt diese

⁸ Quelle: Wall Street Journal (2014): Financial Firms Bolster Cybersecurity Budgets, in: The Wall Street Journal, Nov. 17th 2014, URL: <http://www.wsj.com/articles/financial-firms-bolster-cybersecurity-budgets-1416182536>, 31.8.2015.

⁹ Quelle: Ponemon Institute (2015): 2015 Cost of Data Breach Study: Global Analysis, May 2015, p. 7.

¹⁰ Quelle: PricewaterhouseCoopers (2014): Managing cyber risks in an interconnected world, Sept. 30th 2014, URL: <http://www.doi.gov/ebsa/pdf/erisaadvisorycouncil2015security3.pdf>, 31.8.2015.

Entwicklung die Banken größeren Risiken aus und belässt sie unvorbereitet für den Umgang mit diesen Bedrohungen.¹¹

Neuartige IT-Sicherheitsstrategien

Wir sind der Meinung, dass Unternehmen zunehmend zur Umsetzung einer „aktiven Verteidigungsstrategie“ übergehen sollten. Laut der Financial Times ist es daher beim Management erforderlich, die IT-Sicherheit als eine Schlüsselfunktion zu sehen. Bei einer aktiven Verteidigung werden Taktiken genutzt, um Hacker in Fallen zu locken oder ihre Schritte bis zum Ursprung eines Angriffs zurückzuverfolgen. Die wichtigsten Taktiken einer aktiven Verteidigung werden als Verzögerung (Annoyance), Attribution und Angriff kategorisiert. Dabei sind nur die ersten beiden Taktiken legal.

Bei der Verzögerungstaktik wird ein Hacker verfolgt und zu einem nicht-relevanten Server weitergeleitet. So verschwendet der Hacker seine Zeit und kann einfacher entdeckt werden. Bei der zweiten Taktik, Attribution, werden Tools zur Zurückverfolgung der Angriffsquelle bis zu einem bestimmten Ort (oder einem einzelnen Hacker) verwendet. Zwei beliebte Zuordnungstools sind der „Honey Badger“, der die Angriffsquelle orten kann, und „Beacons“, die in Dokumenten platziert werden, um festzustellen, wann und von wo auf Daten von außerhalb eines Benutzersystems zugegriffen wird. Die dritte Option, der Angriff, ist umstritten und beinhaltet einen „Hack Back“, in dessen Rahmen ein Unternehmen auf den Computer eines vermuteten Hackers zugreift, um dessen Daten zu löschen oder sogar einen Gegenangriff durchzuführen. Diese Kategorie ist illegal.¹²

Fazit

Unserer Meinung nach ist die derzeitige Eskalation der IT-Risiken ein Vorbote der neuen Normalität. Die Lösung des Problems besteht nicht darin, beispielsweise einfach seine Türen abzuschließen. In einer typischen IT-Infrastrukturmgebung können Schlösser geknackt werden oder Türen müssen manchmal offen gelassen werden. Zudem ist es fast unmöglich, jederzeit zu wissen, wo die Eindringlinge sind. Oder noch schlimmer: Der Eindringling kann ein

¹¹ Quelle: Financial Times (2015): The Big read, FT Series: Cyber insecurity: When 95% isn't good enough, in: The Financial Times, July 29th 2015, p. 5.

¹² Quelle: Financial Times (2015): Hacking back, in: The Financial Times, The Big Read, FT Series: Cyber Insecurity, July 28th 2015, p. 7.

Mitarbeiter sein. Daher kommen wir zu dem Schluss, dass zukünftig sowohl Cyberangriffe als auch ihre Kosten zunehmen werden. Unserer Auffassung nach ist dies eine nachvollziehbare Entwicklung, da immer mehr Daten in digitaler Form vorliegen und daher tendenziell stärker gefährdet sind.

In Anbetracht dieser Möglichkeiten glauben wir, dass das Anlagethema IT-Sicherheit für langfristig orientierte Anleger weiterhin sehr attraktiv ist. Unserer Meinung nach stellt der jüngste Aktienkursrückgang des IT-Sicherheitssektors eine attraktive Kaufgelegenheit dar. Wir bevorzugen daher Unternehmen, die sich in Marktnischen als Marktführer etabliert haben und von denen wir glauben, dass sie dort ihren jeweiligen Marktanteil steigern können. Aus diesem Grund halten wir langfristig Aktien von führenden Unternehmen in Bereichen wie Firewalls, Cloud- und Datacenter-Security, Sandboxing, Vulnerability Management, URL-Filterung und Verschlüsselung.

CREDIT SUISSE AG
credit-suisse.com

DISCLAIMER

The information provided herein was produced by Credit Suisse AG and/or its affiliates (hereafter "CS") with the greatest of care and to the best of its knowledge and belief.

The information and views expressed herein are those of CS at the time of writing and are subject to change at any time without notice. They are derived from sources believed to be reliable.

CS provides no guarantee with regard to the content and completeness of the information and does not accept any liability for losses that might arise from making use of the information. If nothing is indicated to the contrary, all figures are unaudited. The information provided herein is for the exclusive use of the recipient.

Neither this information nor any copy thereof may be sent, taken into or distributed in the United States or to any U. S. person (within the meaning of Regulation S under the US Securities Act of 1933, as amended).

It may not be reproduced, neither in part nor in full, without the written permission of CS.

Equities are subject to market forces and hence fluctuations in value, which are not entirely predictable.

Copyright © 2015 Credit Suisse Group AG and/or its affiliates. All rights reserved.

Luxembourg

This document is distributed by CREDIT SUISSE (LUXEMBOURG) S.A. ("CSLux"), which is authorized as a credit institution in the Grand Duchy of Luxembourg and under the prudential supervision of the Luxembourg supervisory authority of the financial sector, the Commission de Surveillance du Secteur Financier (CSSF), 110, route d'Arlon, L-2991 and part of the Credit Suisse group. This document has been prepared by CS AG and not by CSLux.

CSLux was not involved in the production of this document. CSLux provides no guarantee with regard to its content and completeness and does not accept any liability for losses which might arise from making use of this information.

This document constitutes marketing material. It does not constitute investment research. It has not been prepared in accordance with legal requirements designed to promote the independence of investment research and it is not subject to any prohibition on dealing ahead of the dissemination of investment research.

This document is intended only to provide general and preliminary information and shall not be construed as the basis for any investment decision nor as an offer or a solicitation to conclude a transaction in financial instruments or to subscribe to banking services. The liability of CSLux may not be engaged as regards any investment, divestment or retention decision taken by an investor/recipient on the basis of this document. Each investor/recipient shall make his/her own appraisal of the tax, legal, accounting and other financial merits and risks of his/her investment regardless of the opinion expressed in the document. An investor must particularly ensure the suitability of his/her investment as regards his/her financial and fiscal situation, his knowledge and experience in financial instruments and his/her investment objectives. The investor bears all the risks of losses in connection with his/her investment.

This document shall not be construed as a personal recommendation as regards the financial instruments/investment strategies mentioned in the material. This document does not constitute an investment advice, it does not take into account the recipient's economic situation, his/her current assets or liabilities, his/her knowledge and experience in financial instruments and markets, his/her investment purposes, investment horizon, risk profile and preferences.

This document is addressed to the recipient on the basis of the recipient's explicit request. This document is for the exclusive use of the recipient. Any use of this information by the recipient is under the sole responsibility of the recipient. This document may not be reproduced or disseminated either in part or in full without the written permission of CSLux. This document is not intended for persons who, due to their nationality or place of residence, are not permitted to receive such information under local law. Neither this document nor any copy thereof may be sent, taken into or distributed in the United States or to any U. S. person (within the meaning of Regulation S under the US Securities Act of 1933, as amended).

Copyright © 2015 CREDIT SUISSE (LUXEMBOURG) S.A., registered office: 5, rue Jean Monnet, L-2180 Luxembourg, Grand Duchy of Luxembourg, R.C.S. Luxembourg n° B 11756. All rights reserved.

Liechtenstein:

For institutional investors only.

The shares offered are exclusively offered to a limited group of investors, in all cases and under all circumstances designed to preclude a public solicitation in Liechtenstein. This document may not be reproduced or used for any other purpose, nor be furnished to any other person other than those to whom copies have personally been sent. This offer is a private offer, this material and the transactions described therein are therefore not nor have been subject to the review and supervision of the Liechtenstein Financial Market Authority.

Für Liechtenstein:

Nur für institutionelle Anleger. Das Zeichnungsangebot ist einer begrenzten Anlegergruppe vorbehalten. Ein öffentliches Angebot in Liechtenstein ist in allen Fällen und unter allen Umständen ausgeschlossen. Das vorliegende Dokument darf nicht zu anderen Zwecken verwendet oder vervielfältigt werden und ist ausschliesslich für Personen bestimmt, denen das Dokument persönlich zugesendet wurde. Bei diesem Angebot handelt es sich um ein privates Zeichnungsangebot. Die vorliegenden Unterlagen und die darin beschriebenen Transaktionen unterliegen deshalb nicht der Aufsicht und Überprüfung durch die Finanzmarktaufsicht Liechtenstein.

Italy

Performance indications do not consider commissions levied at subscription and/or redemption. Furthermore, no guarantee can be given that the performance of the benchmark will be reached or outperformed.

PERFORMANCE OBTAINED IN THE PAST DOES NOT CONSTITUTE ANY WARRANTY FOR FUTURE. BEFORE THE SUBSCRIPTIONS READ THE PROSPECTUS.

CREDIT SUISSE (ITALY) S.P.A. - Via Santa Margherita, 3 - 20121 Milano – italy.csam@credit-suisse.com - www.credit-suisse.com/it

Spain

For institutional clients only

When distributed in Spain is distributed by CREDIT SUISSE (ITALY) S.P.A. - Via Santa Margherita, 3 - 20121 Milano – italy.csam@credit-suisse.com - www.credit-suisse.com/it

UK

For Qualified Investors/Institutional Clients Only.

When distributed from the United Kingdom, this is distributed by Credit Suisse Asset Management Limited which is authorized and regulated by the Financial Conduct Authority.

France

This document can only be offered to professional clients and to eligible counterparties. This document is distributed by Credit Suisse (Luxembourg) S.A., Succursale en France

When distributed in France, this is distributed by Credit Suisse (Luxembourg) S.A., Succursale en France which is authorized and regulated by Autorité de Contrôle Prudentiel et de Résolution (ACPR) and l'Autorité des Marchés Financiers (AMF).

Dubai

This presentation can only be offered to Professional Clients. This material is personal to each offeree and may only be used by those persons to whom it has been handed out.

Sweden/Denmark/Norway/Netherlands

For Qualified Investors/Institutional Clients Only

Germany and Austria

Wichtige Hinweise

Dieses Dokument wurde von der Division Private Banking & Wealth Management von Credit Suisse („Credit Suisse“) und nicht von der Research-Abteilung von Credit Suisse erstellt. Es stellt **keine Finanzanalyse** dar und **genügt deshalb nicht allen gesetzlichen Anforderungen zur Gewährleistung der Unvoreingenommenheit von Finanzanalysen** und unterliegt keinem Verbot des Handels vor der Veröffentlichung von Finanzanalysen.

Bei diesem Dokument handelt es sich um eine **Werbemitteilung**, die ausschließlich zu Werbezwecken verbreitet wird. Dieses Dokument dient ausschliesslich zur Information und Veranschaulichung sowie zur Nutzung durch den Empfänger. Es stellt **weder eine Aufforderung noch ein Angebot zur Zeichnung oder zum Erwerb der darin erwähnten Produkte und Dienstleistungen** dar. Bei den darin enthaltenen Informationen handelt es sich lediglich um **allgemeine Marktkommentare** und in keiner Weise um regulierte Finanzberatung bzw. Rechts-, Steuer- oder andere regulierte Finanzdienstleistungen. Den finanziellen Zielen, Verhältnissen und Bedürfnissen einzelner Personen wird keine Rechnung getragen. Diese müssen indes berücksichtigt werden, bevor eine Anlageentscheidung getroffen wird. Die hierin enthaltenen Informationen sind nicht ausreichend, um eine Anlageentscheidung zu treffen, und stellen **keine persönliche Empfehlung oder Anlageberatung** dar. Sie bringen lediglich die Einschätzungen und Meinungen der betreffenden einzelnen Mitarbeiter von Private Banking & Wealth Management zum Zeitpunkt der Erstellung des Dokuments zum Ausdruck und beziehen sich nicht auf das Datum, an dem der Leser die Informationen erhält oder darauf zugreift.

Die Einschätzungen und Meinungen der Mitarbeiter von Private Banking & Wealth Management können von den Einschätzungen und Meinungen der Analysten von Credit Suisse oder von anderen Mitarbeitern von Credit Suisse Private Banking & Wealth Management oder den Eigenpositionen von Credit Suisse abweichen oder können diesen widersprechen. Sie können sich zudem **jederzeit ohne Benachrichtigung ändern** und es besteht keine Verpflichtung, die Angaben zu aktualisieren. Sofern dieses Dokument Aussagen über künftige Wertentwicklungen enthält, sind diese Aussagen zukunftsgerichtet und bergen daher diverse Risiken und Ungewissheiten.

Die in diesem Dokument enthaltenen Informationen und Meinungen stammen aus oder basieren auf Quellen, die von Credit Suisse als zuverlässig erachtet werden; dennoch **garantiert Credit Suisse weder deren Richtigkeit noch deren Vollständigkeit**. Credit Suisse lehnt jede Haftung für Verluste ab, die aufgrund der Verwendung dieses Dokuments entstehen. Ist nichts anderes vermerkt, sind alle Zahlen ungeprüft. Sämtliche hierin erwähnten Bewertungen unterliegen den Bewertungsrichtlinien und -prozessen von Credit Suisse. Zu beachten ist, dass **historische Wertentwicklungen und Finanzmarktszenarien kein verlässlicher Indikator für laufende und zukünftige Ergebnisse** sind.

Mit jeder Anlage sind **Risiken** verbunden und unter volatilen oder unsicheren Marktbedingungen **können der Wert und die Rendite der Anlage stark fluktuieren**. Bei Anlagen in ausländischen Wertschriften oder Fremdwährungen besteht zusätzlich das Risiko, dass die ausländische Wertschrift oder die Fremdwährung gegenüber der Referenzwährung des Anlegers an Wert verliert. Alternative Anlageprodukte und -strategien (wie Hedge Fonds und Private Equity) können komplex sein und höhere Risiken beinhalten. Diese Risiken können sich aus dem ausgedehnten Einsatz von Leerverkäufen, Derivaten und Leverage ergeben. Zudem kann der Mindestanlagezeitraum für solche Anlagen länger sein als bei traditionellen Anlageprodukten. Alternative Anlagestrategien (wie Hedge Fonds) sind nur für Anleger bestimmt, welche die mit diesen Anlagen verbundenen Risiken verstehen und akzeptieren.

Dieses Dokument ist nicht für die Verbreitung an oder die Nutzung durch natürliche oder juristische Personen bestimmt, die Bürger eines Landes sind oder die in einem Land ihren Wohnsitz bzw. ihren Gesellschaftssitz haben, in dem die Verbreitung, Veröffentlichung, Bereitstellung oder Nutzung geltende Gesetze oder Vorschriften verletzen würde oder in dem Credit Suisse und/oder ihre Tochtergesellschaften oder verbundenen Unternehmen Registrierungs- oder Zulassungspflichten erfüllen müssten. Die Unterlagen wurden dem Empfänger zur Verfügung gestellt und dürfen nicht ohne die ausdrückliche schriftliche Genehmigung von Credit Suisse weitergegeben werden. In Deutschland wird das vorliegende Dokument von der Credit Suisse (Deutschland) AG verteilt bzw. bereitgestellt, die von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) zugelassen ist und von ihr beaufsichtigt wird.

Copyright © 2015. CREDIT SUISSE GROUP AG und/oder verbundene Unternehmen. Alle Rechte vorbehalten.

CREDIT SUISSE (DEUTSCHLAND) AKTIENGESELLSCHAFT

Junghofstraße 16

D-60311 Frankfurt am Main