Ein genauerer Blick auf wichtige IT-Sicherheitstrends: Welche Auswirkungen haben sie?

Liebe Leserinnen und Leser,

2014 nahm nicht nur die Zahl der Datenschutzverletzungen zu, sondern es wurde auch vermehrt in den Medien über derartige Vorfälle berichtet. Schlagzeilen machten zum Beispiel die Datenlecks bei Target, Home Depot, JP Morgan, dem US Postal Service und kürzlich bei Sony. Diese Ereignisse erregten in den USA und Europa viel mediale Aufmerksamkeit, was wiederum die Unternehmen anspornte, ihre Datenschutzrisiken zu verringern, um nicht selbst negativ in die Schlagzeilen zu geraten. Folglich hat das Thema IT-Sicherheit inzwischen eine hohe Priorität bei den Management-Teams eingenommen. Der Vorfall bei Sony hat dazu geführt, dass nun sogar ein Eingreifen der Regierung denkbar ist. Die jüngste Datenschutzverletzung bei Anthem Inc., einem führenden US-Krankenversicherer, unterstrich die potenziellen Risiken, mit denen sich Gesundheitseinrichtungen konfrontiert sehen.[1]

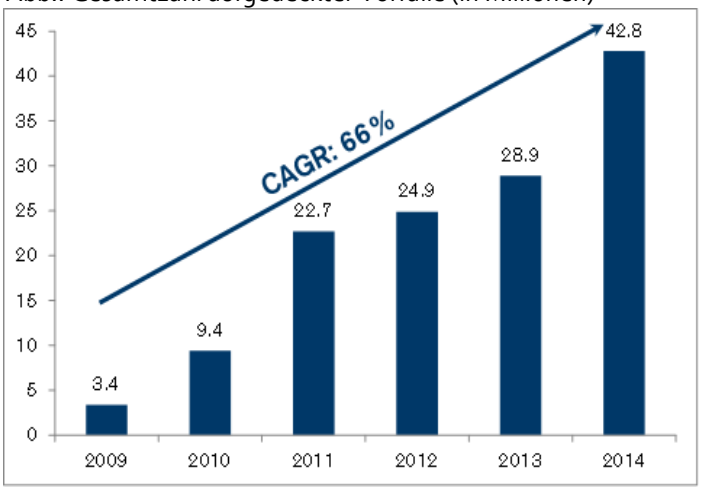
Aufgrund der fortschreitenden Digitalisierung der Weltwirtschaft und der neuen Qualität bei Cyber-Angriffen werden Cyber-Kriminelle voraussichtlich bald in jeden Bereich unseres Lebens eindringen. Wir sehen neue Schwachstellen, wie zum Beispiel bei Krankenhäusern und medizinischen Geräten, mobilen Zahlungssystemen, Unterwasser-Telekommunikationsverbindungen oder Funksensoren für das Internet der Dinge.

Im Folgenden beschreiben wir zunächst die Gegebenheiten in der IT-Sicherheitsbranche. Anschließend zeigen wir auf, dass sich Regierungen zunehmend mit dem Thema Cyber-Sicherheit befassen. Abschließend erörtern wir mögliche Bereiche, in denen wir die IT-Sicherheit als niedrig erachten.

Ein sich veränderndes Umfeld

Laut einer Umfrage von Pricewaterhouse-Coopers (PwC) ist bei mehr als 74% der befragten Unternehmen in den vergangenen 12 Monaten ein sicherheitsrelevanter Vorfall aufgetreten. In der gleichen Umfrage gab PwC an, dass die durchschnittliche jährliche Wachstumsrate (CAGR) der aufgedeckten Vorfälle zwischen 2009 und 2014 bei 66% lag. Dabei gab es 2014 einen Zuwachs um 48% gegenüber dem Vorjahr auf 42,8 Millionen Vorfälle oder 117 339 Angriffe pro Tag (vgl. Abb.). Der

Abb.: Gesamtzahl aufgedeckter Vorfälle (in Millionen)



Quelle: PwC (2014): Managing cyber risks in an interconnected world: Key findings from The Global State of Information Security® Survey 2015, 30.9.2014, S. 7.

[1] Quelle: Wall Street Journal (2015): Health Insurer Anthem Hit by Hackers: Breach Gets Away with Names, Social Security Numbers of Customers, Employees, in: The Wall Street Journal, 4.2.2015, URL: http://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720, 10.2.2015.

geschätzte jährliche finanzielle Schaden in Verbindung mit Cyber-Sicherheit betrug USD 2,7 Mio. und stellt damit eine Zunahme von 34% gegenüber 2013 dar.[2] Obgleich dieser Anstieg beeindruckend erscheint, könnte dies unseres Erachtens eine eher konservative Schätzung sein, da viele Datenverletzungen nicht gemeldet oder sogar überhaupt nicht entdeckt werden, sodass die Zahl der „unbekannten Vorfälle" deutlich höher sein könnte. Trustwave Holdings meldete kürzlich, dass nach Ansicht des Unternehmens bis zu 71% der Vorfälle nicht entdeckt würden.[3]
Laut der Financial Times wird für die weltweiten Ausgaben für Informationssicherheit für 2015 ein Anstieg von 8,2% auf USD 76,9 Mrd. prognostiziert.[4] In den letzten Jahren haben sich auch das allgemeine Profil und die Motive der Hacker verändert. Wir leben nicht länger in einer Welt, in der es 16-jährigen Teenagern um Ruhm und Aufmerksamkeit geht, und wir wissen auch nicht mehr, wer der wahre „Gegner" ist. Die neuen Hacker haben ganz neue, höchst unterschiedliche Motive. Um das Ganze noch komplizierter zu machen, gibt es zudem einige ganz neue Teilnehmer: Viele von ihnen werden von Staaten unterstützt und viele sind sehr gut ausgebildet.[5]

Regierungen nehmen sich des Themas Cyber-Sicherheit immer mehr an

„Keine ausländische Nation, kein Hacker sollte in der Lage sein, unsere Netzwerke stillzulegen, unsere Industriegeheimnisse zu stehlen oder in die Privatsphäre von amerikanischen Familien, vor allem die unserer Kinder, einzudringen."

US-Präsident Barack Obama[6]

2013 gab das FBI bekannt, es habe 3 000 Unternehmen davon in Kenntnis gesetzt, dass sie Opfer eines Cyber-Angriffs geworden seien.[7] Im Frühjahr 2014 erhob das US-Justizministerium Anklage gegen fünf chinesische Militärangehörige. Ihnen wurde vorgeworfen, die Rechner von Atomkraftwerken und Metallproduzenten in den USA gehackt zu haben. Es ist eher unwahrscheinlich, dass die Verdächtigen jemals in den USA vor Gericht stehen werden, denn zwischen den USA und China gibt es kein Auslieferungsabkommen. Der Vorfall war jedoch insofern bedeutend, als die USA zum ersten Mal Vertreter eines anderen Staates eines Cyber-Verbrechens unter dem Economic Espionage Act (Wirtschaftsspionagegesetz) anklagten.[8]
Unserer Einschätzung nach ist es wahrscheinlich, dass in den USA ein IT-Sicherheitsgesetz verabschiedet wird. Dieses würde den Aufsichtsräten und der obersten Geschäftsführung von Unternehmen die Verantwortung für den Datenschutz übertragen. In der Regel ist die Gesetzgebung deutlich langsamer als die sich schnell weiterentwickelnde Technologie. Doch angesichts der zunehmenden Zahl hochkarätiger Datenschutzverletzungen könnten schon bald neue und strengere Standards gelten: Am 8. Juli 2014 verabschiedete das Senate Intelligence Committee einen

[2] Quelle: PricewaterhouseCoopers (2014): Managing cyber risks in an interconnected world: Key findings from The Global State of Information Security® Survey 2015, 30.9.2014, S. 7, URL: http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf, 9.2.2015.
[3] Quelle: Trustwave Holdings (2014): 2014 Trustwave Global Security Report, Mai 2014, S. 14, URL: https://www2.trustwave.com/rs/trustwave/images/2014_Trustwave_Global_Security_Report.pdf, 9.2.2015.
[4] Quelle: Financial Times (2015): Israeli cyber security "foundry" launched, in: The Financial Times, 11.2.2015, S. 17.
[5] Quelle: PricewaterhouseCoopers (2014): Managing cyber risks in an interconnected world: Key findings from The Global State of Information Security® Survey 2015, 30.9.2014, S. 13, URL: http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf, 9.2.2015.
[6] Quelle: The White House (2015): Auszüge aus der Rede des US-Präsidenten zur Lage der Nation, URL: http://www.whitehouse.gov/the-press-office/2015/01/20/excerpts-president-s-state-union-address, 10.2.2015.
[7] Quelle: The Washington Post (2014): U.S. notified 3,000 companies in 2013 about cyberattacks, 24.3.2014, URL: http://www.washingtonpost.com/world/national-security/2014/03/24/74aff686-aed9-11e3-96dc-d6ea14c099f9_story.html, 10.2.2015.
[8] Quelle: The Wall Street Journal (2014): U.S. Charges Five in Chinese Army with Hacking: First Time Washington Has Charged Foreign State Employees with Hacking, in: The Wall Street Journal, 19.5.2014, URL: http://www.wsj.com/articles/SB10001424052702304422704579571604060696532, 10.2.2015.

Gesetzesentwurf zur Cyber-Sicherheit, in dessen Rahmen mehr Informationen zu Cyber-Sicherheitsrisiken zwischen dem öffentlichen und privaten Sektor ausgetauscht werden dürfen.[9] Am 13. Februar 2015 kündigte Präsident Barack Obama als Reaktion auf Vorfälle wie den Angriff auf Sony eine Durchführungsverordnung an, nach der die Regierung und Unternehmen angewiesen werden, mehr Informationen über Bedrohungen in Verbindung mit Cyber-Sicherheit auszutauschen.[10]
In der EU könnten ähnliche Trends aufkommen. Gegen Unternehmen, die die vorgeschlagene Verordnung nicht befolgen, könnten Geldstrafen von bis zu 5% ihres Jahresumsatzes oder EUR 100 Mio. verhängt werden, je nachdem, welcher Betrag höher ist.[11]
Unserer Einschätzung nach unterstreicht das wachsende staatliche Engagement für Cyber-Sicherheit nachdrücklich die zunehmende Bedeutung dieses Bereichs. Diese Entwicklungen können auch als Vorbild für zukünftige staatliche Eingriffe im privaten Sektor dienen, sollte dies im Interesse des Datenschutzes sein. Wir wären nicht überrascht, wenn dies den Boden für weitere staatliche Eingriffe oder einen Informationsaustausch bereiten würde.

Mögliche neue, aus unserer Sicht höchst anfällige IT-Sicherheitsbereiche
Unserer Einschätzung nach werden Cyber-Kriminelle ihre Aufmerksamkeit auf neue Bereiche richten, in denen die Sicherheitsvorkehrungen tendenziell gering sind. Zu diesen Schwachstellen gehören zum Beispiel:

- **Medizinische Unterlagen:** In den USA sind medizinische Unterlagen attraktive Ziele, denn sie enthalten oft sowohl sensitive Informationen wie zum Beispiel die Sozialversicherungsnummer, aber auch finanzielle Informationen. Das Ponemon Institute, ein im Bereich Datenschutz aktiver US-amerikanischer Think Tank, stellte fest, dass im Jahr 2013 insgesamt 1,84 Millionen erwachsene Amerikaner oder enge Familienangehörige einmal Opfer eines medizinischen Identitätsdiebstahls geworden waren. Ein Jahr zuvor waren es noch 1,52 Millionen.[12]
  Die jüngste Datenschutzverletzung bei Anthem Inc. unterstreicht, dass verstärkt Unternehmen und Organisationen im Gesundheitswesen ins Visier geraten. Hacker verschafften sich Zugriff auf Daten von Millionen von aktuellen und früheren Kunden und Mitarbeitenden, darunter Namen, Geburtsdaten, Sozialversicherungsnummern, Anschriften, E-Mail-Adressen und Einkommen.[13]
- **Medizinische Geräte:** Experten warnen schon seit einiger Zeit vor der Gefahr, dass Hacker bei medizinischen Geräten Daten manipulieren und die Geräte per Fernzugriff steuern können. Zu anfälligen Geräten gehören Herzschrittmacher, Defibrillatoren, Insulinpumpen und Geräte für

[9] Quelle: The Washington Post (2014): Senate intelligence panel advances cybersecurity bill, in: The Washington Post, 8.7.2014, URL: http://www.washingtonpost.com/blogs/the-switch/wp/2014/07/08/senate-intelligence-panel-advances-cybersecurity-bill/, 10.2.2015.
[10] Quelle: Neue Zürcher Zeitung (2015): Bedrohung aus dem Cyberspace wird zur Chefsache, in: Neue Zürcher Zeitung, 16.2.2015, S. 5.
[11] Am 12. März 2014 stimmte das Europäische Parlament in einer Plenarsitzung für die vollständige Unterstützung der vorgeschlagenen Verordnung. Damit die vorgeschlagene Verordnung Gesetzeskraft erlangen kann, muss sie vom EU-Ministerrat und der Europäischen Kommission verabschiedet werden. Das wird voraussichtlich 2015 erfolgen (Quelle: Long (2014): Significant impact of new EU data protection regulation on financial services, URL: http://www.globalbankingandfinance.com/significant-impact-of-new-eu-data-protection-regulation-on-financial-services/, 11.2.2015, Long (2014): EU Data Protection Regulation: fines up to €100m proposed, in: Computer Weekly, http://www.computerweekly.com/opinion/EU-Data-Protection-Regulation-fines-up-to-100m-proposed, 11.2.2015).
[12] Quelle: Ponemon Institute (2013): 2013 Survey on Medical Identity Theft, September 2013, S. 4, URL: https://clearwatercompliance.com/wp-content/uploads/2013/10/2013-Medical-Identity-Theft-Report-FINAL.pdf, 12.2.2015.
[13] Quelle: Wall Street Journal (2015): Health Insurer Anthem Hit by Hackers Breach Gets Away With Names, Social Security Numbers of Customers, Employees, in: The Wall Street Journal, 4.2.2015, URL: http://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720, 12.2.2015.

die kontinuierliche Blutzuckermessung. Diese tragbaren Geräte sind oft über Wi-Fi mit dem Internet verbunden, damit die Daten an Kliniken gesendet werden können. Allerdings haben Experten gezeigt, dass sie sich Kontrolle über ein Gerät verschaffen oder die gesendeten Daten abfangen können. Anders als Smartphone und Computer werden medizinische Geräte keinem regelmäßigen Sicherheits-Update unterzogen, denn Software-Änderungen könnten eine erneute Zertifizierung durch staatliche Aufsichtsbehörden wie die FDA erforderlich machen.[14] Das U.S. Department of Homeland Security untersucht rund zwei Dutzend Fälle von vermuteten Cyber-Sicherheitslücken bei medizinischen Geräten und Krankenhausausstattung, bei denen offizielle Stellen einen Hacker-Angriff befürchten.[15]

- **Unterwasser-Telekommunikationskabel:** Laut Foreign Affairs werden rund 95% der interkontinentalen Kommunikation – E-Mails, Telefongespräche, Geldüberweisungen usw. – nicht via Funk oder Satellit, sondern per Unterwasserkabel mit einer Länge von insgesamt mehr als 965 600 Kilometern übertragen. Größtenteils mangelt es diesen kritischen Kommunikationswegen an grundlegendsten Schutzmechanismen, und zwar sowohl auf dem Meeresboden als auch bei den Anschlusspunkten. Der Schutz physischer IT-Infrastruktur wurde bisher von staatlichen Behörden weitgehend ignoriert. Eine mögliche Manipulation wäre ebenfalls relativ einfach, da viele Kabeltrassen der Öffentlichkeit zugänglich sind.[16]
- **Funksensoren / Internet der Dinge (Internet of Things, IoT):** Laut Cisco wird das „Internet der Dinge" bis 2022 ein Umsatzpotenzial von USD 14 Bio. erreichen. Über 50 Milliarden Funksensoren könnten mit dem Internet verbunden sein.[17] Allerdings wird der Erfolg oder Misserfolg des Internet of Things weitgehend von Sicherheitsaspekten abhängen. In Verbindung mit diesem Technologietrend wurden drei Risiken identifiziert[18]: Erstens könnte ein gehacktes Gerät nicht richtig funktionieren und je nach Gerät eine Gefahr darstellen. Zweitens könnte eine Geräte-Schwachstelle den unerwünschten Zugang auf ein größeres „Smart Home" oder Firmennetzwerk ermöglichen. Drittens könnten Funksensoren und IoT-Geräte, die nicht durch eine robuste IT-Sicherheitsumgebung geschützt sind, Ausgangspunkt für Angriffe werden, zum Beispiel über „Distributed Denial of Service"-Angriffe oder Attacken anderer Netzwerke. In diesen Fällen drohen neben dem Schaden durch das ursprünglich gehackte Gerät noch viele andere schwerwiegende Gefahren.[19]
- **Mobile Zahlungssysteme:** Laut Deloitte werden 2015 rund 5% der 600–650 Millionen mit Nahfeldkommunikation (NFC) ausgestatteten Telefone mindestens einmal im Monat genutzt, um kontaktlose Zahlungen zu tätigen. Dies ist deutlich mehr als 2014. Damals wurden

[14] Quelle: FDA (2014): The FDA takes steps to strengthen cybersecurity of medical devices, press release, 1.10.2014, URL: http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm416809.htm, 12.2.2015, siehe auch Credit Suisse (2014): „Internet of Things": A new disruptive technology … and really without any security issues?, Newsletter Security, Safety & Protection Industry, Februar 2014, S. 4.

[15] Quelle: Reuters (2014): U.S. government probes medical devices for possible cyber flaws, 22.10.2014, URL: http://www.reuters.com/article/2014/10/22/us-cybersecurity-medicaldevices-insight-idUSKCN0IB0DQ20141022, 12.2.2015.

[16] Quelle: Foreign Affairs (2015): Under the Sea: The Vulnerability of the Commons, in: Foreign Affairs, Januar/Februar 2015, URL: http://www.foreignaffairs.com/articles/142491/robert-martinage/under-the-sea, 13.2.2015.

[17] Quelle: Cisco (2013): Embracing the Internet of Everything To Capture Your Share of USD 14.4 Trillion, White Paper, S. 4, URL: http://internetofeverything.cisco.com/learn/value-stake-analysis, 13.2.2015.

[18] Quelle: McSweeney (2015): Security Is a Must for the Internet of Things, in: re/code, 27.1.2015, URL: http://recode.net/2015/01/27/security-is-a-must-for-the-internet-of-things/, 13.2.2015.

[19] Autos sind unserer Einschätzung nach in erheblichem Umfang von Hackerangriffen bedroht, denn sie sind zunehmend computerisiert und mit dem Internet verbunden. Vor Kurzem musste BMW eine Sicherheitslücke beheben, die es Hackern ermöglicht hätte, die Türen von bis zu 2,2 Millionen Fahrzeugen der Marken Rolls-Royce, Mini und BMW zu öffnen (Quelle: Chip (2015): Schwachstelle in BMW ConnectedDrive: ADAC knackt Autos per Mobilfunkverbindung, in: Chip, 30.1.2015, URL: http://www.chip.de/news/Schwachstelle-in-BMW-ConnectedDrive-ADAC-knackt-Autos-per-Mobilfunkverbindung_76134061.html, 13.2.2015.

weltweit weniger als 0,5% der 450 Millionen Smartphones für mobile Zahlungen eingesetzt.[20] Aktuell werden mobile Bezahlsysteme wie Apple Pay und ähnliche Systeme als sicher vermarktet. Doch mit steigender Verbreitung werden auch Cyber-Kriminelle auf diesen Zug aufspringen. Laut der Washington Post ist es nur noch eine Frage der Zeit, bis Hacker herausfinden, wie sie die Sicherheitsvorkehrungen manipulieren können.[21]

Fazit

Unserer Einschätzung nach ist es nicht mehr nur eine Frage der Zeit, bis Cyber-Gefahren nicht mehr nur Kreditkarten, Bankkonten und Filmstudios, sondern ganze Computersysteme betreffen, welche die wesentlichen Infrastruktureinrichtungen eines Landes steuern. Beispielsweise haben sich Hacker bereits erfolgreich Zugang zu Computersystemen in einem südkoreanischen Atomkraftwerk verschafft.[22] Zudem sind Hacker nach einem Bericht des deutschen Bundesamts für Sicherheit in der Informationstechnik in das Netzwerk eines nicht genannten Stahlwerks in Deutschland eingedrungen und haben Steuerungssysteme dermaßen manipuliert, dass ein Hochofen nicht mehr ordnungsgemäß heruntergefahren werden konnte. Die Schäden seien „massiv" gewesen.[23]
Daher sind unserer Meinung nach robuste IT-Sicherheitssysteme erforderlich. Als langfristig orientierte Anleger investieren wir deshalb in IT-Sicherheitsunternehmen, welche in attraktiven Marktnischen eine führende Position innehaben und von zahlreichen Opportunitäten profitieren können.

Service
Bei allfälligen Fragen stehe ich Ihnen gerne unter der Telefonnummer +41 (0)44 334 69 90 oder der folgenden E-Mail-Adresse zur Verfügung: Dr. Patrick Kolb: patrick.kolb@credit-suisse.com

[20] Quelle: Deloitte (2015): Technology, Media & Telecommunications Predictions 2015, S. 51, URL: http://www2.deloitte.com/lu/en/pages/technology-media-and-telecommunications/articles/tmt-predictions.html, 13.2.2015.
[21] Quelle: The Washington Post (2015): The time a major financial institution was hacked in under 15 minutes, in: The Washington Post, 14.1.2015, URL: http://www.washingtonpost.com/blogs/the-switch/wp/2015/01/14/the-time-a-major-financial-institution-was-hacked-in-under-15-minutes/, 23.2.2015.
[22] Quelle: Reuters (2014): South Korea nuclear plant operator says hacked, raising alarm, in: Reuters, 22. Dezember 2014, URL: http://www.reuters.com/article/2014/12/22/us-southkorea-nuclear-idUSKBN0K008E20141222, 13.2.2015.
[23] Quelle: Bundesamt für Sicherheit in der Informationstechnik (2014): Die Lage der IT-Sicherheit in Deutschland 2014, S. 31, URL: https://www.bsi.bund.de/DE/Publikationen/Lageberichte/bsi-lageberichte.html, 13.2.2015.

andere Konsequenzen zu prüfen. Dieses Dokument darf ohne schriftliche Genehmigung der CS weder auszugsweise noch vollständig vervielfältigt werden. Es richtet sich ausdrücklich nicht an Personen, deren Nationalität oder Wohnsitz den Zugang zu solchen Informationen aufgrund der geltenden Gesetzgebung verbietet. Weder das vorliegende Dokument noch Kopien davon dürfen in die Vereinigten Staaten von Amerika versandt, dorthin mitgenommen oder in den Vereinigten Staaten von Amerika verteilt oder an eine US-Person (im Sinne von Regulation S des US Securities Act von 1933 in dessen jeweils gültiger Fassung) abgegeben werden. 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. Zu beachten ist, dass historische Renditeangaben und Finanzmarktszenarien keine verlässlichen Indikatoren für zukünftige Ergebnisse sind.

Liechtenstein

Nur für qualifizierte/professionelle Anleger.

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.

Australien

Nur für Wholesale Clients.

Wird dieses Dokument in Australien verbreitet oder wird von dort darauf zugegriffen, so erfolgt seine Herausgabe in Australien durch die CREDIT SUISSE INVESTMENT SERVICES (AUSTRALIA) LIMITED ABN 26 144 592 183 AFSL 370450. Es wurde erstellt und wird ausschließlich zur Verfügung gestellt für zulässige Empfänger, die Großkunden („Wholesale Clients") im Sinne von Section 761G(7) des Corporations Act 2001 (Cth.) (das „Gesetz") und sachkundige oder professionelle Anleger („Sophisticated or Professional Investors") im Sinne von Section 708(8) bzw. (11) des Gesetzes sind, bei denen ein Angebot keine Offenlegung gemäß Part 7.9 oder Chapter 6D des Gesetzes erfordern würde.

GB

Nur für qualifizierte/institutionelle Anleger.

Die Verbreitung von Großbritannien aus erfolgt durch die Credit Suisse Asset Management Limited, die von der Financial Conduct Authority zugelassen und reguliert wird.

Dubai

Diese Präsentation darf nur professionellen Kunden angeboten werden. Diese Unterlagen sind für den Angebotsempfänger persönlich bestimmt und dürfen nur von den Personen genutzt werden, denen sie ausgehändigt wurden.

Singapur

In Singapur nur an institutionelle Anleger. Keinesfalls zur Weiterverbreitung.

Dieses Dokument ist kein Prospekt („Prospectus") im Sinne des singapurischen Securities and Futures Act, Chapter 289 („SFA") und wurde bei der Monetary Authority of Singapore nicht als Prospekt registriert. Daher würde die gesetzliche Haftung im Rahmen des SFA für den Inhalt von Prospekten nicht gelten, und dieses Dokument ist in keiner Weise als Aufforderung oder Angebot zum Kauf oder Verkauf einer darin genannten Beteiligung oder Anlage auszulegen. Sie sollten sorgfältig prüfen, ob sich die Anlage für Sie eignet. Das in diesem Dokument genannte Produkt ist nicht von der Monetary Authority of Singapore („MAS") zugelassen oder anerkannt, und die Beteiligungen/Aktien/Anteile dürfen Kleinanlegern in Singapur nicht angeboten werden.

Hongkong/Taiwan/Südkorea

Nur für professionelle/institutionelle Anleger

Kanada

Diese Informationen werden in Kanada von der Credit Suisse Securities (Canada), Inc. oder einer mit ihr verbundenen Gesellschaft (gemeinsam die „Credit Suisse") verbreitet. Die hierin enthaltenen Beobachtungen und Erwartungen können sich von den Beobachtungen und Erwartungen der Credit Suisse unterscheiden oder zu diesen im Widerspruch stehen. Die hierin enthaltenen Informationen dienen ausschließlich zu Informationszwecken. Sie stellen keinen Prospekt, keine Werbung, kein öffentliches Angebot, kein Angebot zum Verkauf von hierin beschriebenen Wertpapieren und keine Empfehlung zum Kauf von hier beschriebenen Wertpapieren in Kanada oder dessen Provinzen oder Territorien dar und sind keinesfalls als solche auszulegen. Ein Verkaufsangebot oder -abschluss in Bezug auf die hierin beschriebenen Wertpapiere in Kanada erfolgt nur unter einer Freistellung von den Erfordernissen zur Einreichung eines Prospekts bei den betreffenden kanadischen Wertpapierregulierern und nur durch einen Händler, der ordnungsgemäß im Rahmen der geltenden Wertpapiergesetze registriert ist, oder alternativ unter einer Freistellung vom Erfordernis der Händlerregistrierung in der betreffenden Provinz oder dem betreffenden Territorium Kanadas, in der oder dem das Verkaufsangebot oder der Verkaufsabschluss erfolgt. Die hierin

enthaltenen Informationen sind keinesfalls als Anlageberatung in einer Provinz oder einem Territorium Kanadas auszulegen und nicht auf die Bedürfnisse des Empfängers zugeschnitten. Soweit die hierin enthaltenen Informationen auf Wertpapiere eines Emittenten Bezug nehmen, der nach den Gesetzen Kanadas oder einer Provinz oder eines Territoriums Kanadas eingetragen, gegründet oder errichtet wurde, müssen alle Geschäfte mit solchen Wertpapieren über einen in Kanada registrierten Händler durchgeführt werden. Diese Unterlagen, die darin enthaltenen Informationen und der Wert der darin beschriebenen Wertpapiere wurden von keiner Wertpapierkommission oder ähnlichen Regulierungsbehörde in Kanada geprüft oder in irgendeiner Weise beurteilt, und jede gegenteilige Aussage ist strafbar.

Die hierin enthaltenen Informationen können vorausblickende Informationen (Forward-Looking Information, „FLI") im Sinne von Section 1.1 des Securities Act (Ontario) enthalten. FLI sind Offenlegungen zu möglichen Ereignissen, Bedingungen oder Ergebnissen von Tätigkeiten, die auf Annahmen über künftige Wirtschaftsbedingungen und Handlungsweisen basieren, und umfassen zukunftsorientierte Finanzinformationen (Future-Oriented Financial Information, „FOFI") zu möglichen Ergebnissen von Tätigkeiten, Vermögenslagen oder Cashflows, die entweder als Vorhersage oder als Projektion präsentiert werden. „FOFI" sind FLI zu möglichen Ergebnissen von Tätigkeiten, Vermögenslagen oder Cashflows, die auf Annahmen über künftige Wirtschaftsbedingungen und Handlungsweisen basieren und in Form einer historischen Bilanz, Erfolgsrechnung oder Geldflussrechnung präsentiert werden. Entsprechend handelt es sich bei einem „finanziellen Ausblick" (Financial Outlook) um FLI zu möglichen Ergebnissen von Tätigkeiten, Vermögenslagen oder Cashflows, die auf Annahmen über künftige Wirtschaftsbedingungen und Handlungsweisen basieren und nicht in Form einer historischen Bilanz, Erfolgsrechnung oder Geldflussrechnung präsentiert werden.

Empfänger sollten sich nicht auf FLI in diesen Unterlagen verlassen, da solche Informationen verschiedenen Risiken, Unsicherheiten und anderen Faktoren unterliegen, die zu einer wesentlichen Abweichung der tatsächlichen Ergebnisse von den Erwartungen führen könnten. Bei Erhalt dieser Unterlagen erkennt jeder Empfänger hiermit an und stimmt zu, dass hierin enthaltene FLI nicht als wesentlich für die Zwecke von National Instrument 51-102 Continuous Disclosure Requirements betrachtet werden sollten und möglicherweise nicht in Übereinstimmung damit erstellt und/oder präsentiert wurden und dass der Anleger keine weiteren Informationen zur Aktualisierung dieser FLI erhalten wird, außer wenn dies im Rahmen geltender Wertpapiergesetze erforderlich ist und/oder verträglich vereinbart wurde. Empfänger sollten sich wegen zusätzlicher Informationen an ihre eigenen Rechts- und Finanzberater wenden.