CREDIT SUISSE

Thematic Insights: Robotik, Schutz und Sicherheit

Die zunehmend fragilere Sicherheit im Internet – Gibt es Investitionsopportunitäten für Anleger?

Dr. Patrick Kolb, Fondsmanager, Credit Suisse

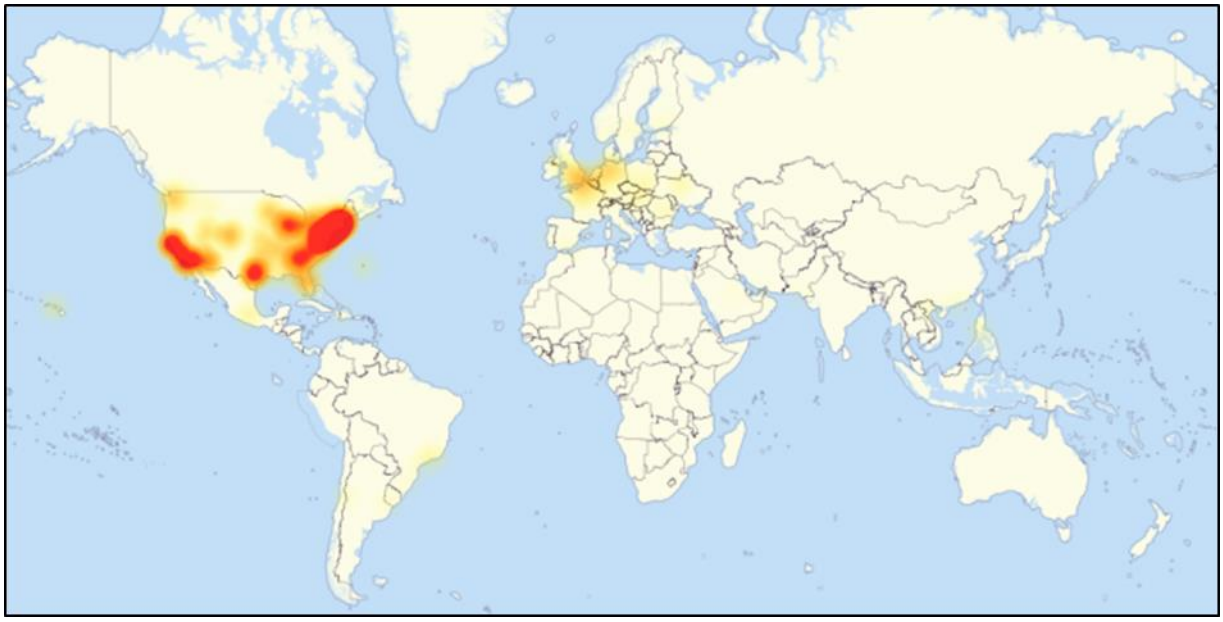
> ***„IT-Sicherheit muss an der Spitze einer Organisation ihren Anfang nehmen. Sie ist ein Führungsthema und Firmenchefs müssen mit gutem Beispiel vorangehen."***
>
> ***Zitat während einer IT-Sicherheitskonferenz***

Die Bedrohung durch „Distributed Denial of Service"-Attacken (DDoS) im Internet nimmt laufend zu und greift weiter um sich. Am Freitag, dem 23. Oktober 2016, störte eine massive Cyberattacke den Internetverkehr auf Hunderten von Websites, darunter Twitter, Financial Times, Airbnb, PayPal, Spotify. Besonders an der Ost- und Westküste der USA konnten Millionen von Nutzern nicht mehr auf diese Websites zugreifen (siehe Abb. 1). Auch Nutzer in Europa und Asien waren betroffen. Diese DDoS-Attacke historischen Ausmaßes wurde über ein „Botnet" gestartet, ein Netzwerk aus PCs und anderen mit dem Internet verbundenen Geräten. Hunderttausende internetfähige Geräte wie Kameras, Babyphones und Home-Router waren mit Schadsoftware infiziert und für die Attacke verwendet worden, ohne dass ihre Besitzer etwas davon mitbekommen hatten. Sobald das Botnet eingerichtet ist, kann der Hacker es nutzen, um die Zielwebsite mit einer überdimensionalen Flut von Anfragen zu überschwemmen.[1] Im aktuellen Fall richtete sich der Angriff nicht gegen eine einzelne Website, sondern gegen das in den USA beheimatete Unternehmen Dyn Inc., dessen Dienstleistungen für das Internet von wesentlicher Bedeutung sind. Durch den gezielten Angriff auf die Server von Dyn Inc. konnte diese Attacke einen weitaus größeren Schaden anrichten als beim Angriff auf einzelne Websites, da es sich bei Dyn Inc. um einen „Domain Name System"-Anbieter (DNS) handelt, also im Grunde um den Betreiber einer Internet-Vermittlungszentrale. Mithilfe des DNS werden benutzerfreundliche Webadressen wie www.credit-suisse.com in „IP-Adressen" umgewandelt – numerische Adressen, die Computer nutzen, um miteinander zu kommunizieren. Die Überschwemmung der DNS-Server von Dyn Inc. mit Datenverkehr bewirkte im Endeffekt den Ausfall weiter Teile

[1] Quelle: The New York Times (2016): Hackers Used New Weapons to Disrupt Major Websites Across U.S., in: The New York Times, 21. Oktober 2016, URL: http://www.nytimes.com/2016/10/22/business/internet-problems-attack.html?_r=0, 30.10.2016.

des Internets. Der Angriff verursachte massive Kollateralschäden. Experten gehen von einem Verlust von mehr als USD 100 Millionen aus.[2]

Abb. 1: Von der DDoS-Attacke am 23. Oktober 2016 verursachte Internetausfälle.



Quelle: Downdetector.com

Was ist DDoS?

Bei einer „Distributed Denial-of-Service"-Attacke (DDoS-Attacke) handelt es sich um eine Cyberattacke mit dem Ziel, die Verfügbarkeit eines Netzwerkservers für seine Benutzer zu stören. Dazu unterbricht oder sperrt der Verursacher der Attacke die von einem mit dem Internet verbundenen Host zur Verfügung gestellten Services zeitweise oder sogar dauerhaft. In der Regel wird dabei versucht, ein Zielgerät mit überflüssigen Anfragen zu überhäufen, sodass die Server überlasten und ernsthafte Anfragen nicht länger bearbeiten können.[3] Die Verursacher von DDoS-Attacken nehmen häufig namhafte Websites oder Services ins Visier, die von Banken oder Kreditkarten-Zahlungsportalen betrieben werden. Ihre Motive reichen von Aktivismus über Rache bis hin zur Erpressung.[4]

DDoS-Attacken waren bereits in den vergangenen Jahren nichts Ungewöhnliches gewesen, aber nun steht fest, dass sie wirkungsvoller und komplexer werden und sich zunehmend gegen wichtige Internet-Infrastrukturanbieter richten. Laut Imperva Inc., einem im Bereich des Rechenzentrenschutzes aktiven IT-Sicherheitsunternehmen, erreicht ein Drittel aller DDoS-Attacken ein Datenvolumen von über 20 Gbit/s. Da DDoS-Angriffe sich stetig weiterentwickeln, benötigen Organisationen im gleichen Maße immer mehr zusätzliche Netzwerkressourcen, um sich gegen sie zu verteidigen. Sogar Unternehmen mit umfangreicher Internetbandbreite und hoher Konnektivität könnten der Überflutung ihrer Kapazitäten durch diese Attacken zum Opfer fallen – und der Zukauf weiterer Bandbreite kann extrem kostspielig sein.[5]

Abb. 2 zeigt, dass 52 % aller DDoS-Attacken aus nur zehn Ländern stammen. Die Angriffe erfolgen häufig über gekaperte Hosting-Umgebungen oder mit dem Internet verbundene Geräte in Regionen mit unsicherer Sicherheits-Infrastruktur. Obwohl eine Attacke ihren Ursprung möglicherweise in einem anderen Land hat, kann der Verursacher sie durch IT-Infrastrukturen in Ländern mit schwächeren Sicherheitsvorkehrungen leiten.

---

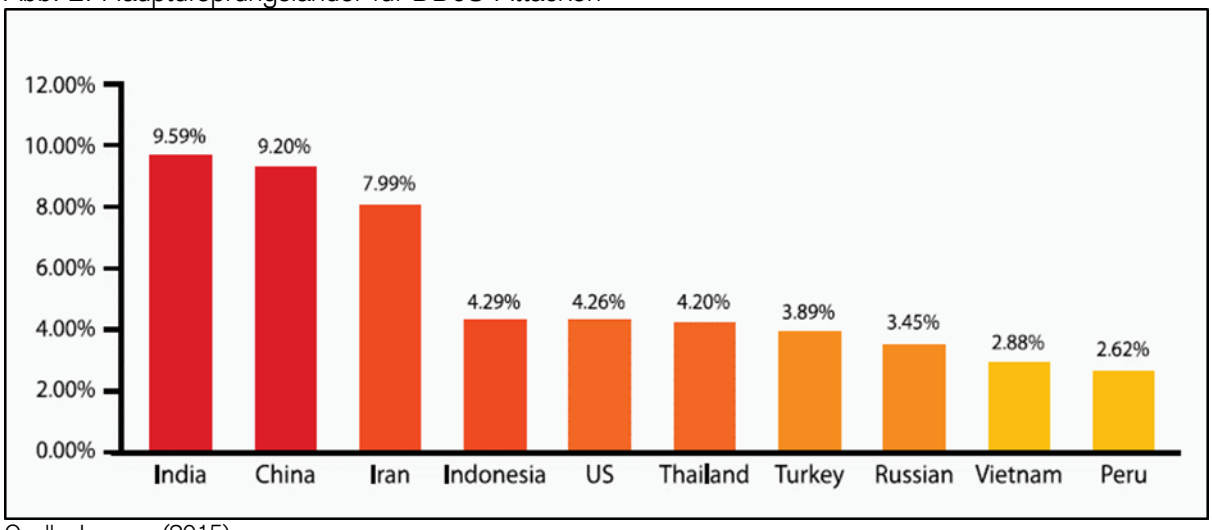
[2] Quelle: CNN Money (2016): 'Unprecedented' cyberattack involved tens of millions of IP addresses, 22. Oktober 2016, URL: http://money.cnn.com/2016/10/22/technology/dyn-cyberattack/index.html, 30.10.2016.

[3] Quelle: US-CERT (2016): Understanding Denial of Service Attacks, URL: https://www.us-cert.gov/ncas/tips/ST04-015, 30.10.2016.

[4] Quelle: Cloudflare (2016): Empty DDoS Threats: Meet the Armada Collective, URL: https://blog.cloudflare.com/empty-ddos-threats-meet-the-armada-collective/, 30.10.2016.

[5] Quelle: Imperva (2015): The Top 10 DDoS Attack Trends, S. 3, White Paper, URL: https://www.imperva.com/docs/DS_Incapsula_The_Top_10_DDoS_Attack_Trends_ebook.pdf, 30.10.2016.

Abb. 2: Hauptursprungsländer für DDoS-Attacken



Quelle: Imperva (2015)

Mirai: Eine simple Schadsoftware, aber beunruhigend effektiv

Im Rausch der Begeisterung über die Aussicht, das Eigenheim oder das Büro per Smartphone fernzusteuern (z. B. um die Heizungstemperatur anzupassen, das Garagentor zu schließen oder Einbrecher aufzuspüren), haben zahlreiche Hersteller mit geringer Erfahrung im Bereich der Cybersicherheit ihre Produkte bedenkenlos internetfähig gemacht. Das riesige Botnet, das für die DDoS-Attacke im Oktober verwendet wurde, kaperte Computer, Smartphones und andere internetfähige Geräte mithilfe eines Programms namens „Mirai". Diese Schadsoftware macht Computersysteme zu ferngesteuerten „Bots", die dann als Teil einer groß angelegten DDoS-Attacke verwendet (oder missbraucht) werden. Mirai scannt das Internet nach Geräten mit schlechten IT-Sicherheitseigenschaften (z. B. verwendete Passwörter wie „admin", „passwort" oder „12345")[6], welche miteinander über das so genannte „Internet der Dinge" („Internet of Things", IoT) vernetzt sind. IT-Sicherheitsexperten zufolge wird dieser Code, welcher der Mirai-Schadsoftware zugrunde liegt, sogar als „dilettantisch" beurteilt. Umso überraschender ist es, dass ein solch einfacher Code für eine derart große und erfolgreiche DDoS-Attacke verantwortlich sein konnte. Dieser Umstand spricht Bände darüber, wie schlecht es derzeit um die Sicherheit von IoT-Geräten bestellt ist.[7] Der Financial Times zufolge hinkt die IT-Sicherheit in der Hardware-Industrie dem Stand der Software-Industrie um ein gutes Jahrzehnt hinterher.[8]

Das Technologieforschungsunternehmen Gartner sagt voraus, dass 2020 mehr als 20 Milliarden elektrische Geräte mit dem Internet verbunden sein werden. Die Konsumenten sowie die Unternehmen würden demnach je rund USD 1.500 Milliarden für IoT-Geräte ausgeben.[9] Zudem prognostiziert das Forschungsunternehmen, dass per 2020 an rund einem Viertel aller Computerangriffe IoT-Geräte beteiligt sein werden, die betroffenen Unternehmen jedoch nur etwa 20 % ihres IT-Sicherheitsbudgets für den Schutz gegen derlei Angriffe aufwenden würden. Es wird daher erwartet, dass die Bemühungen zum Schutz des Internets der Dinge sich zusehends auf die Verwaltung, Analyse und vorsorgliche Absicherung der Geräte und ihrer Daten richten werden. Mit Sicherheit wird ein skalierbares, automatisiertes System erforderlich sein, das dynamisch mit den Überwachungs-, Erkennungs-, Zugriffskontroll- und sonstigen Sicherheitsanforderungen Schritt halten kann. In der Tat sind wir der Ansicht, dass die dem IoT zugrunde liegenden Stärken bezüglich der Weitläufigkeit und Verfügbarkeit der Vernetzung vermutlich

[6] Quelle: NZZ (2016): Quellcode von Mirai im Netz zu haben, 12.10.2016, URL: http://www.nzz.ch/digital/it-sicherheit-quellcode-von-mirai-im-netz-zu-haben-ld.121578, 30.10.2016.
[7] Quelle: NZZ (2016): Wie Kaffeemaschinen die Meinungsfreiheit gefährden – Sicherheit im Internet der Dinge, URL: http://www.nzz.ch/digital/sicherheit-im-internet-der-dinge-wie-kaffeemaschinen-die-meinungsfreiheit-gefaehrden-ld.120436, 30.10.2016.
[8] Quelle: Financial Times (2016): Connected devices create security weak spots, in: The Financial Times, 24. Oktober 2016, S. 14.
[9] Quelle: Gartner (2015): Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015, URL: http://www.gartner.com/newsroom/id/3165317, 30.10.2016.

erst dann vollständig genutzt werden können, wenn automatische Sicherheitssysteme vorhanden sind, die dynamische und kostengünstige Sicherheitslösungen ermöglichen.[10]

Automatisierte IT-Sicherheit: Eine Lösung zur Minimierung von Cyber-Risiken?

Die Überschwemmung des Internets mit Millionen billiger Allzweckcomputer stellt ein gewaltiges Sicherheitsrisiko dar. Deshalb muss die Industrie bei der Sicherheit dieser Geräte bessere Arbeit leisten. Bisher steht das Thema IT-Sicherheit im Bereich IoT noch nicht auf der Agenda. Zu beachten ist, dass dies ein „bewegliches Ziel" darstellt. Selbst die Absicherung der anspruchsvollsten und teuersten Computer dürfte weiterhin ein ständiger Kampf bleiben: Baut man eine bessere Mausefalle, so züchten Hacker einfach eine raffiniertere Maus. Doch die Sicherung der IT-Risiken aller in Millionen von Geräten verbauten, billigen Mikrocomputer in den Haushalten und Büros der Verbraucher könnte nahezu unmöglich sein.

Für Anleger verspricht das Thema IT-Sicherheit eine bedeutende langfristige Anlagechance zu bleiben, da Hacker ständig neue Möglichkeiten finden, in Netzwerke einzudringen und neue Systemarten ins Visier zu nehmen. Wir sind überzeugt, dass die Anzahl der internetfähigen Geräte, von IoT-Geräten über Drohnen und Smartphones bis hin zu Konsumartikeln mit der Zeit deutlich wachsen wird. Diese neuen Systeme werden den Fokus der Cybersicherheit erweitern, da bisher wenig in ihre Sicherung investiert wurde. Neue Prozesse und Technologien werden benötigt, um diesen Herausforderungen zu begegnen. Wir gehen davon aus, dass die Automatisierung der IT-Sicherheit zu diesem Zweck verstärkt an Bedeutung gewinnen wird. Beispielsweise ist selbst die beste Cybersicherheitslösung nutzlos, wenn ein Techniker eine Firewall falsch konfiguriert oder vergisst, auf einem neuen Server einen Patch zu installieren, um eine Sicherheitslücke zu schließen. Manuelle Arbeit ist per se mit Risiken verbunden, und unserer Ansicht nach ist bei der manuellen Behebung von IT-Sicherheitsproblemen die Katastrophe schon vorprogrammiert. Kluge Geschäftsführer müssen die Wahrscheinlichkeit menschlichen Versagens verringern – und hier stellt die Automatisierung der IT-Sicherheit eine effektive Lösung zur Risikominimierung dar.

Zusammengefasst vertreten wir die Ansicht, dass Formen künstlicher Intelligenz wie Bild- und Mustererkennung (Klassifizierung von Daten oder Objekten auf Basis von Gemeinsamkeiten), Verarbeitung natürlicher Sprache (die Fähigkeit eines Computers, menschliche Sprache zu verstehen und entsprechend zu reagieren) und maschinelles Lernen (Software, die lernt, etwas zu tun, ohne dafür programmiert worden zu sein) bald in größerem Umfang in vielen Produkten und Dienstleistungen Verwendung finden werden. Wir glauben, dass manuelle IT-Sicherheit angesichts der kommenden Datenexplosion und der zunehmenden Verbreitung hybrider Systeme in wenigen Jahren nicht mehr effektiv sein wird. Unternehmen werden für ihre IT-Sicherheit entweder eigene Automatisierungslösungen entwickeln oder diesen Prozess auslagern. Es kann Monate oder gar Jahre dauern, bis ein Unternehmen in einer hybriden Umgebung End-to-End-Prozessautomatisierung erreicht hat, doch langfristig wird die Automatisierung sich immer mehr lohnen.

Wir sind der Meinung, dass Schutz und Sicherheit sowie Robotik und Automatisierung für langfristig orientierte Anleger äußerst reizvolle Anlagethemen darstellen und sich derzeit noch in der Frühphase eines attraktiven langfristigen Wachstumszyklus befinden. Anlagen in diesen Bereichen dürften aufgrund ihres strukturellen Charakters in Zukunft zunehmen. Aus diesem Grund halten wir Beteiligungen an führenden Unternehmen dieser beiden Anlagethemen.

Weitere Informationen (wie aktuelle Fonds-Factsheets, Performanceberichte oder Quartalskommentare) finden Sie hier (Sicherheit und Schutz) oder hier (Robotik).

[10] Quelle: Gartner (2016): Gartner Says Worldwide IoT Security Spending to Reach $348 Million in 2016, URL: http://www.gartner.com/newsroom/id/3291817, 30.10.2016.

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.

CREDIT SUISSE (DEUTSCHLAND) AKTIENGESELLSCHAFT

Taunustor 1

D-60310 Frankfurt am Main