«Shellshock» – ein Softwarefehler, der seit Jahrzehnten besteht …
Welche Risiken drohen der gesamten IT-Infrastruktur?

Liebe Leserinnen und Leser,

in den letzten Wochen haben Sie möglicherweise in der Zeitung von einer neuen IT-Sicherheitslücke namens «Shellshock» erfahren. Diese Sicherheitslücke betrifft eine Software, die in diversen Geräten verwendet wird – von Servern, die das Rückgrat des Internet bilden, bis hin zu iPhones. Unter den bisher je entdeckten Online-Sicherheitslücken wird diese als eine der Gravierendsten eingeschätzt, deutlich schwerwiegender als der «Heartbleed»-Bug, welcher IT-Sicherheitsexperten im April 2014 tief beunruhigte.[1] Der Financial Times zufolge wurde das Ausnutzungspotenzial von Shellshock von der National Cyber Security Division des Department of Homeland Security (DHS) mit 10 auf einer Skala von 1 bis 10 eingestuft. Auch die möglichen Auswirkungen sowie der Schweregrad insgesamt wurden mit 10 von 10 veranschlagt – der höchstmöglichen Bewertung. Zum Vergleich: Heartbleed wurde insgesamt «nur» mit 5 eingestuft.[2] Die Sicherheitslücke betrifft die sogenannte «Bash Shell», ein frei verfügbares Open-Source-Softwareprogramm, das in zahlreichen Unix- und Linux-Systemen breite Anwendung findet.[3]

Was ist «Shellshock»?

Das betroffene Programm wurde 1987, lange vor dem wirtschaftlichen Durchbruch des Internet, von Brian J. Fox geschrieben, damals noch ein junger Programmierer. Heute wird diese Software in über 70 % der mit dem Internet vernetzten Geräte verwendet, darunter Server, Computer, Router, Mobiltelefone und sogar Geräte wie Kameras und Kühlschränke. Am 24. September 2014 sprachen IT-Sicherheitsexperten die Warnung aus, dass Bash einen besonders besorgniserregenden Softwarefehler namens «Shellshock» enthielt: Ein Teil des Programms könnte dazu genutzt werden, die weltweite Kontrolle über Millionen von Geräten zu erlangen, möglicherweise auch über PCs oder Smartphones. Unglücklicherweise ist das fehlerhafte Programm weit verbreitet. Viele Internetdienste wie Webserver nutzen Bash, um bestimmte Anfragen zu verarbeiten. Ein Angreifer könnte anfällige Versionen von Bash dazu veranlassen, beliebige Befehle auszuführen. Somit könnte der Angreifer die

[1] Quelle: Credit Suisse (2014): IT-Sicherheit: Konvergenz von Endpunkt- und Netzwerksicherheit?, Credit Suisse Newsletter Sicherheits- und Schutzbranche, Mai 2014, S. 1.

[2] In der Zwischenzeit wurde ein weiterer Softwarefehler namens POODLE (Paddling Oracle On Downgraded Legacy Encryption) aufgedeckt. IT-Sicherheitsexperten zufolge dürfte diese Sicherheitslücke nicht so gravierend sein wie Heartbleed oder Shellshock (Quelle: Reuters (2014): New POODLE web threat not seen as menacing as Heartbleed, Shellshock, in: Reuters, 15. Oktober 2014, URL: http://in.reuters.com/article/2014/10/15/cybersecurity-encryption-poodle-idINKCN0I401X20141015, 22.10.2014).

[3] Quelle: Financial Times (2014): Cyber attack risk heightens after global Shellshock threat to software, in: The Financial Times, 26. September 2014, S. 1.

Sicherheitslücke ausnutzen, um sich unbefugt Zugang zu einem Computersystem zu verschaffen.[4]
Der Fall Shellshock legt Vergleiche mit dem Heartbleed-Bug nahe, der im letzten Frühjahr in einer wichtigen Softwarekomponente entdeckt wurde. Shellshock hat jedoch das Potenzial, zu einer noch grösseren Bedrohung zu werden: Während Heartbleed ausgenutzt werden konnte, um zum Beispiel Passwörter auf einem Server auszuspähen, könnte mit Shellshock die Kontrolle über das gesamte System übernommen werden – auch ohne Benutzername und Passwort. Heartbleed blieb zwei Jahre lang von IT-Sicherheitsexperten unbemerkt und betraf schätzungsweise 500'000 Geräte, Shellshock hingegen wurde erst nach über 22 Jahren entdeckt.[5] Weniger als 24 Stunden nach der Aufdeckung von Shellshock begannen Hacker bereits mit entsprechenden Botnet-Angriffen.[6]

Wie gefährlich ist Shellshock?
Laut einer aktuellen Analyse des MIT Technology Review ist Shellshock wahrscheinlich der gefährlichste und älteste bekannte und nicht behobene Softwarefehler, der jemals gefunden wurde. Das Softwareprogramm Bash ist Standard auf allen Linux-Betriebssystemen und auf Mac OS X von Apple. Es wird auch von einfachen, mit dem Internet vernetzten Geräten genutzt, die als Betriebssystem häufig eine Variante von Linux verwenden.[7] Daher gehen Sicherheitsexperten davon aus, dass Shellshock das Potenzial hat, nicht nur Servers zu gefährden, sondern auch bestimmte privat genutzte Router, IP-Kameras und andere Geräte.[8]
Darüber hinaus gibt Shellshock den Hackern die Möglichkeit, aus der Ferne beliebigen Codes auf einem System auszuführen. Diese könnte dazu genutzt werden, einen selbstreplizierenden «Wurm» zu schaffen. Dadurch könnte ein geschädigtes System andere Computer angreifen, was aufgrund der Vernetzung eine rasche Vervielfältigung zur Folge hätte und würde Tausende von Systemen infiltrieren. Die sogenannte DHCP-Software beispielsweise, die zur Herstellung von Verbindungen mit einem WLAN-Netzwerk verwendet wird, kann Befehle an Bash übergeben und einen Computer mit einem anfälligen Betriebssystem bei der Verbindung zu einem WLAN-Netzwerk unter Umständen einem Angriff aussetzen. Dadurch könnte ein System mit einem anfälligen Betriebssystem bei der Verbindung zu einem nicht vertrauenswürdigen WLAN zum Angriffsziel werden.[9] Zudem erfordert die Nutzung der Schwachstelle Shellshock keine umfassende Programmierkenntnisse. Laut Greenberg (2014) ist ein darauf basierender Angriff so einfach, dass selbst ungeübte Hacker vorhandene

[4] Quelle: Selzer (2014): Shellshock makes Heartbleed look insignificant, 29. September 2014, in: ZDNet, URL: http://www.zdnet.com/shellshock-makes-heartbleed-look-insignificant-7000034143/, 20.10.2014.
[5] Es wird vermutet, dass ein Softwareentwickler um das Jahr 1992 wohl versehentlich einen Fehler in den Code einführte. Für Programmierer ist es nicht verwunderlich, dass der fehlerhafte Code über zwei Jahrzehnte lang unentdeckt blieb. Viele der kommerziell genutzten Tools, auf die Privatanwender und grosse Unternehmen angewiesen sind, wurden auf der Grundlage von Programmen entwickelt, die von wenigen unbezahlten Freiwilligen geschrieben und gepflegt werden. Sie gehören der sogenannten «Open Source Community» an. Neben grossen Unternehmen passt diese Community ältere Programme an und entwickelt auf ihrer Grundlage Neuerungen. Das Macintosh-Betriebssystem zum Beispiel wird zwar regelmässig aktualisiert, wurde aber auf Grundlage älterer Software wie Unix entwickelt (Quelle: New York Times (2014): Security Experts Expect «Shellshock» Software Bug in Bash to Be Significant, in: The New York Times, 20. September 2014, S. B1, URL: http://www.nytimes.com/ 2014/09/26/ technology/security-experts-expect-shellshock-software-bug-to-be-significant.html, 20.10.2014).
[6] Quelle: BBC (2014): Web attacks build on Shellshock bug, 26. September 2014, URL: http://www.bbc.com/news/technology-29375636, 20.10.2014.
[7] Fox wartete Bash mehrere Jahre lang, bevor er das Programm an Chet Ramey übergab, einen Freiwilligen und Programmierer, der die Software als unbezahltes Hobby weiterentwickelte (Quelle: The New York Times (2014): Security Experts Expect «Shellshock» Software Bug in Bash to Be Significant, in: The New York Times, 20. September 2014, S. B1, URL: http://www.nytimes.com/2014/09/26/technology/security-experts-expect-shellshock-software-bug-to-be-significant.html, 20.10.2014).
[8] Quelle: Cerrudo (2014): Why the Shellshock Bug Is Worse than Heartbleed, in: MIT Technology Review, 30. September 2014, URL: http://www.technologyreview.com/view/531286/why-the-shellshock-bug-is-worse-than-heartbleed/, 20.10.2014.
[9] Quelle: Cerrudo (2014): Why the Shellshock Bug Is Worse than Heartbleed, in: MIT Technology Review, 30. September 2014, URL: http://www.technologyreview.com/view/531286/why-the-shellshock-bug-is-worse-than-heartbleed/, 20.10.2014.

Codefragmente zusammenstellen können, um sich die Kontrolle über Zielgeräte zu verschaffen.[10] Unseres Erachtens werfen die Vorfälle in Zusammenhang mit Heartbleed und Shellshock ein Schlaglicht auf ein Problem, das in Zukunft erneut auftreten könnte. Das heutige Internet beruht auf Softwareprogrammen, deren Ursprünge Jahrzehnte zurückliegen. Einige von ihnen wurden nie auf potenzielle Sicherheitslücken überprüft. Wie vorhin erwähnt, geht der Softwarecode von Bash auf die späten 1980er-Jahre zurück. Der Gedanke, ihn auf seine Anfälligkeit für Internetangriffe zu prüfen, lag zum damaligen Zeitpunkt vollkommen fern. «Dass es sich um eine der am häufigsten genutzten Softwarekomponenten der Welt handelt und zum Angriffsziel werden könnte, war schlichtweg undenkbar», meint Brian Fox. «Zu dem Zeitpunkt, als dies denkbar wurde, war das Programm bereit seit 15 Jahren im Einsatz.» Heute wird das Programm Bash von allen grossen Internetfirmen verwendet – darunter Google und Facebook –, weil es sich bei dem Code um Open-Source-Software handelt.[11]

Rückläufige Budgets für IT-Sicherheit?

Ungeachtet der Verbreitung von Sicherheitslücken im Internet und in Computercodes sowie der steigenden Zahl von Zwischenfällen im Bereich Datensicherheit ist erstaunlicherweise festzuhalten, dass sich die Budgets für IT-Sicherheit in zahlreichen Unternehmen rückläufig entwickeln. Selbst angesichts der jüngsten Angriffe auf Target, Home Depot und JP Morgan,[12] die für starkes öffentliches Interesse gesorgt hatten, sind die IT-Sicherheitsbudgets weltweit laut einer Umfrage von PwC unter annähernd 10'000 Führungskräften und IT-Leitern gegenüber 2013 um 4 % zurückgegangen. Dieses Ergebnis überrascht, ist doch die Zahl der Angriffe um 48 % gestiegen, wobei sich die durchschnittlichen Kosten für die Bewältigung von Sicherheitsvorfällen und die Schadensbehebung auf USD 2,7 Mio. je Vorfall belaufen – ein Drittel mehr als im Jahr 2013. Während die Ausgaben von mittelgrossen und grossen Unternehmen um 5 % anstiegen, gingen die Sicherheitsbudgets von Firmen mit Umsätzen von unter USD 100 Mio. im Durchschnitt um 20 % zurück. David Burg von PwC warnt, dass Grossunternehmen von Prozessen bei kleineren Anbietern und Zulieferern abhängig sind. So drangen Hacker beispielsweise beim Angriff auf den Einzelhandelskonzern Target in das Computernetzwerk des Unternehmens ein, indem sie einen Zugang nutzten, der für einen Zulieferer von Kühl- und Klimaanlagen eingerichtet worden war. «Viele kleine und mittlere Unternehmen sind selbst mit grösseren Unternehmen verbunden. Die Realität ist: Das System ist in seiner Gesamtheit nicht sicherer, nur weil grosse Unternehmen mehr ausgeben», so Burg. «Es gibt keine völlig autarken Unternehmen.»[13, 14] Unseres Erachtens ist diese Studie von PwC verwirrend. Im Gegensatz dazu geht Gartner davon aus, dass die Ausgaben für IT-Sicherheit für 2014 um 7,9 % auf USD 71,1 Mia. und für

[10] Quelle: Greenberg (2014): Hackers Are Already Using the Shellshock Bug to Launch Botnet Attacks, in: Wired, 25. September 2014, URL: http://www.wired.com/2014/09/hackers-already-using-shellshock-bug-create-botnets-ddos-attacks/, 21.10.2014.

[11] Quelle: McMillan (2014): The Internet Is Broken, and Shellshock Is Just the Start of Our Woes, in: Wired, 29. September 2014, URL: http://www.wired.com/2014/09/shellshocked-bash/, 20.10.2014.

[12] JP Morgan kündigte kürzlich an, dass das Unternehmen über die nächsten fünf Jahre eine Verdopplung seiner Ausgaben für IT-Sicherheit von USD 250 Mio. auf USD 500 Mio. plane. Grund hierfür ist die Datenpanne, infolge derer die Kontaktinformationen – jedoch keine sensiblen Kontodaten – von 76 Millionen Haushalten und rund sieben Millionen kleinen und mittleren Unternehmen in falsche Hände gerieten (Quelle: The Wall Street Journal (2014): JP Morgan CEO: Cybersecurity Spending to Double, The Wall Street Journal, 12. Oktober 2014, URL: http://online.wsj.com/articles/j-p-morgans-dimon-to-speak-at-financial-conference-1412944976, 20.10.2014).

[13] Quelle: Financial Times (2014): Security budgets slide despite 48 % increase in cyber attacks, in: The Financial Times, 1. Oktober 2014, S. 18.

[14] Quelle: PWC (2014): Managing cyber risks in an interconnected world: Key findings from The Global State of Information Security® Survey 2015, S. 19, URL: http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf, 20.10.2014.

2015 um weitere 8,2 % auf USD 76,9 Mia. ansteigen werden[15].

Fazit

Die genannten Entwicklungen zeigen, dass wir uns noch in der Frühphase des Anlagethemas «Cybersicherheit» befinden. Zudem vertreten wir die Auffassung, dass die jüngst zu verzeichnende Marktkorrektur einiger führender IT-Sicherheitsunternehmen eine langfristige Kaufgelegenheit darstellt.

Unserer Meinung nach ist dieses Anlagethema für langfristig orientierte Anleger sehr reizvoll und steht erst am Anfang eines attraktiven langanhaltenden Wachstumszyklus. Wir gehen daher davon aus, dass die Investitionen in IT-Sicherheitsprodukte durch die öffentliche Hand sowie durch Unternehmen und Privatkunden künftig ansteigen werden. Aus diesem Grund halten wir Beteiligungen an Unternehmen, die auf dem Gebiet innovativer IT-Sicherheitslösungen für Datenschutz, Netzwerksicherheit, Schwachstellenmanagement und Datenspeicherung führend sind.

Service

Bei allfälligen Fragen stehe ich Ihnen gerne unter der Telefonnummer +41 44 344 69 90 oder der folgenden E-Mail-Adresse zur Verfügung: Dr. Patrick Kolb: patrick.kolb@credit-suisse.com

[15] Quelle: Wall Street Journal (2014): Global Security Spending to Grow 7.9 % in 2014, Gartner Says, in: The Wall Street Journal, 22. August 2014, URL: http://blogs.wsj.com/cio/2014/08/22/global-security-spending-to-grow-7-9-in-2014-gartner-says/, 22.10.2014.

Financial Conduct Authority) or any other Credit Suisse entities. When distributed in or accessed from Switzerland, this is distributed by Credit Suisse AG and/or its affiliates. For further information, please contact your Relationship Manager.

Liechtenstein

For qualified/professional 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.

Australia

When distributed or accessed from Australia, this document is issued in Australia by CREDIT SUISSE INVESTMENT SERVICES (AUSTRALIA) LIMITED ABN 26 144 592 183 AFSL 370450. It has been prepared for, and is made available only to, permitted recipients who are wholesale clients as that term is defined by section 761G(7) of the Corporations Act 2001 (Cth.) (the "Act") and sophisticated or professional investors as defined by sections 708(8) and (11) (respectively) of the Act, in respect of which an offer would not require disclosure under Part 7.9 or Chapter 6D of the Act.

UK

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.

Spain

This marketing material is distributed in Spain by Credit Suisse International, Sucursal en España and/or Credit Suisse AG, Sucursal en España], legal entities registered at Comisión Nacional del Mercado de Valores as distributors of the investment fund mentioned in this document

Qatar

This information has been distributed by Credit Suisse (Qatar) L.L.C, which has been authorized and is regulated by the Qatar Financial Centre Regulatory Authority (QFCRA) under QFC No. 00005. All related financial products or services will only be available to Business Customers or Market Counterparties (as defined by the Qatar Financial Centre Regulatory Authority (QFCRA) rules and regulations), including individuals, who have opted to be classified as a Business Customer, with liquid assets in excess of USD 1 million, and who have sufficient financial knowledge, experience and understanding to participate in such products and/or services.

Dubai

This information is distributed by Credit Suisse AG Dubai Branch, duly licensed and regulated by the Dubai Financial Services Authority (DFSA). Related financial products or services are only available to customers who qualify as either a Professional Client or a Market Counterparty under the DFSA rules and who have sufficient financial experience and understanding to participate in financial markets and satisfy the regulatory criteria to be a client.

Singapore

In Singapore to institutional investors only. Strictly not for redistribution.

This document is not a prospectus as defined in the Securities and Futures Act, Chapter 289 of Singapore ("SFA") and has not been registered as a prospectus with the Monetary Authority of Singapore. Accordingly, statutory liability under the SFA in relation to the content of prospectuses would not apply, and this document should not be construed in any way as a solicitation or an offer to buy or sell any interest or investment referred to in this document. You should consider carefully whether the investment is suitable for you. The product named in this document is not authorised or recognized by the Monetary Authority of Singapore (the "MAS") and none of its interests / shares / units shall be allowed to be offered to retail public in Singapore

Canada

This information is distributed in Canada by Credit Suisse Securities (Canada), Inc. or an affiliate (collectively "Credit Suisse"). The observations and views contained herein may be different from or inconsistent with the observations and views of Credit Suisse. The information contained herein is for informational purposes only and is not, and under no circumstances is to be construed as, a prospectus, an advertisement, a public offering, an offer to sell securities described herein, solicitation of an offer to buy securities described herein, in Canada or any province or territory thereof. Any offer or sale of the securities described herein in Canada will be made only under an exemption from the requirements to file a prospectus with the relevant Canadian securities regulators and only by a dealer properly registered under applicable securities laws or, alternatively, pursuant to an exemption from the dealer registration requirement in the

relevant province or territory of Canada in which such offer or sale is made. Under no circumstances is the information contained herein to be construed as investment advice in any province or territory of Canada and is not tailored to the needs of the recipient. To the extent that the information contained herein references securities of an issuer incorporated, formed or created under the laws of Canada or a province or territory of Canada, any trades in such securities must be conducted through a dealer registered in Canada. No securities commission or similar regulatory authority in Canada has reviewed or in any way passed upon these materials, the information contained herein or the merits of the securities described herein and any representation to the contrary is an offence.

The information contained herein may contain "forward-looking information" ("FLI") as such term is defined under section 1.1 of the Securities Act (Ontario). FLI is disclosure regarding possible events, conditions or results of operations that is based on assumptions about future economic conditions and courses of action and includes future-oriented financial information ("FOFI") with respect to prospective results of operations, financial position or cash flows that is presented either as a forecast or a projection. "FOFI" is FLI about prospective results of operations, financial position or cash flows, based on assumptions about future economic conditions and courses of action, and presented in the format of a historical balance sheet, income statement or cash flow statement. Similarly, a "financial outlook" is FLI about prospective results of operations, financial position or cash flows that is based on assumptions about future economic conditions and courses of action that is not presented in the format of a historical balance sheet, income statement or cash flow statement.

Recipients should not rely on any FLI that may be contained within this material as such information is subject to a variety of risks, uncertainties and other factors that could cause actual results to differ materially from expectations. Upon receipt of this material, each Recipient hereby acknowledges and agrees that any FLI included herein should not be considered material for the purposes of, and may not have been prepared and/or presented consistent with, National Instrument 51-102 Continuous Disclosure Requirements and that the investor will not receive any additional information updating any such FLI, other than as required under applicable securities laws and/or as agreed to in contract. Recipients should consult with their own legal and financial advisers for additional information.