scip ag

Contents

1. Editorial

Ein paar Gedanken zum digitalen Geld

Rubel und Franken gehören der Vergangenheit an. Dollars sowieso. Denn die Zukunft gehöre Bitcoin, sagen die Erfinder der digitalen Währung. Der grosse Vorteil des virtuellen Gelds: Sie funktioniert dezentralisiert. Das heisst, dass die Bitcoins direkt zwischen den Usern direkt ausgetauscht werden, also nicht noch zusätzlich über eine Bank oder einen anderen Mittelmann geht. Damit werden laut Werbevideo auf der offiziellen Website, das im freundlichen Cartoon-Look daherkommt, die Gebühren niedriger. Und jeder könne auf Bitcoin zugreifen und einfach damit zahlen, vorausgesetzt er hat eine App installiert. „Bitcoin verändert die Finanzwelt in der gleichen Art, wie das Internet die Verlagsindustrie verändert hat“, sagt die jugendliche Männerstimme im Video.

Was genau das heissen soll, wird nicht erklärt. Nur so viel fügt der Sprecher an: „Wenn jeder Zugriff auf einen Markt hat, werden grosse Ideen Wirklichkeit.“ Dazu erklingt ein Engelschor und die Sonne beginnt zu scheinen. Und noch besser: Das Bitcoin-Protokoll ist Open Source. Jeder kann den Code einsehen und sichergehen, dass Bitcoin sauber ist.

Die Realität sieht aber anders aus. Anstelle von grossen Erfindungen, die die Welt revolutionieren, sind Bitcoins laut dem Wirtschaftsmagazin The Economist vor allem wegen „ihrer Rolle in zwielichtigen Geschäften“ beliebt. Statt die Welt mit einem konstanten, einfachen und hürdenfreien Geldstrom zu verbinden, verkaufte ein Mann der sich Dread Pirate Roberts nennt und im echten Leben wohl Ross Ulbricht heisst (siehe OpSec on the Silk Road: Learning from Pirates, Seite 17) Drogen und Auftragsmorde. Die Site konnte nur überleben, da sowohl Verkäufer und Käufer anonym blieben. Da half Bitcoin natürlich. Da die Kundendaten nicht in einem zentralen Server gespeichert sind – wie unter anderem bei einer Kreditkarte oder Paypal – konnte jeder so viele Drogen kaufen, wie er sich leisten konnte. Oder die Schwiegermutter umbringen lassen.

Mittlerweile, ein halbes Jahrzehnt nachdem die ersten Bitcoins generiert worden sind, steht die Währung im Rampenlicht. Nicht nur im Zuge der Affäre um Silk Road sondern auch, weil das Auktionhaus Ebay unlängst angekündigt hat, dass es darüber nachdenkt, Bitcoins allenfalls als Zahlungsmittel zuzlassen. Das, wie auch die Existenz von Bitcoin, gefällt den etablierten Finanzinstituten gar nicht. Banken sehen sich in ihrer Machtbasis bedroht, denn Bitcoins haben kein zentrales Kontrollorgan, was die Existenz einer Bank überflüssig macht. Zudem entzieht es den Banken die Kontrolle über Geld. In Bitcoins eingetauschtes Geld ist im Umlauf, ohne dass die Bank je wieder etwas davon sieht oder den Fluss regulieren kann. Angenommen Ebay springt auf den Bitcoin-Zug auf. Das wären dann potentielle 11,652 Milliarden Dollar (Stand: 2011), die nicht mehr unter Kontrolle der Banken wäre. Das ist zwar nicht besonders viel in den Augen einer Bank, doch hätte Ebays Aktion Signalwirkung.

Das bereitet den Finanzinstituten Sorgen. Zu Recht. Denn im Grunde genommen hat sich das Bankensystem in seinen Grundzügen kaum verändert. Computer sind besser geworden, die Bilanzsummen mal grösser, mal kleiner. Aber Geld, Konto, Zinsen, Investitionen und so weiter sind geblieben. Seit Jahrhunderten das selbe. Es ist lediglich grösser, einflussreicher und vor allem schneller geworden. Sollte nun Bitcoin an Bedeutung gewinnen – was bis dato zumindest theoretisch möglich ist – liegt es an den

Traditionsreichen und Altmodischen, sich neu zu erfinden und sich anzupassen. Doch am Schluss steht den Geldhändlern eine sehr schwierige Aufgabe ins Haus: Sie müssen im Konkurrenzkampf mit einem gesichtlosen, dezentralen und anonymen Gegner bestehen, dessen Kundenstamm dazu auch noch aus ihrem eigenen Kundenstamm besteht.

Doch bis zu diesem Kampf werden wohl noch viele Franken den Besitzer wechseln, genau wie Dollars und eben auch Bitcoins. Der aktuelle Stand von Bitcoin ist also dieser: Bitcoin ist weder der Untergang des Bankenwesens, noch die Erlösung der von Banken Unterjochten. Bitcoin ist vorerst einfach mal existent und ein sehr interessantes Phänomen auf sicherheitstechnischer, programmiererischer und finanzwirtschaftlicher Ebene.

Dominik Bärlocher
Zürich, 15. November 2013

Ihre Meinung interessiert uns. Wird Bitcoin zum Mainstream und somit zur Konkurrenz für Banken werden? Oder bleibt die digitale Währung eine Randerscheinung? Senden Sie uns Ihre Gedanken an doba@scip.ch.

2. scip AG Informationen

2.1 Risikoanalyse

Diskussion und Identifikation von Schwachstellen und potentiellen Sicherheitsrisiken in einem Projekt zur frühzeitigen Verhindung und Verminderung dieser.

- Vorbereitung: Definition der Ziele sowie Zusammentragen und Diskutieren des bestehenden Konzepts.
- Review: Durchsicht und Analyse zur Ermittlung von Unschönheiten und Fehlern.
- Diskussion: Dokumentation und Diskussion der identifizierten Fehler sowie der vorgeschlagenen Massnahmen.

Der Kunde erhält ein Dokument, welches die Unsicherheiten des Projekts bespricht. Die grundlegenden Diskussionen werden in Prosaform abgegeben und die einzelnen Risikoberechnungen in tabellarischer Form dargeboten.

Als Spezialisten können wir frühzeitig auf Probleme und Mängel aufmerksam machen, bevor sich diese innerhalb eines Unternehmens etablieren können. Dadurch wird die Angriffsfläche unmittelbar und längerfristig minimiert sowie die Grundlage für eine sichere Umgebung geschaffen. Dank unserer langjägrigen Erfahrung können wir zudem Vergleiche mit anderen Firmen darstellen und daher ein intelligentes Best Practice anwenden.

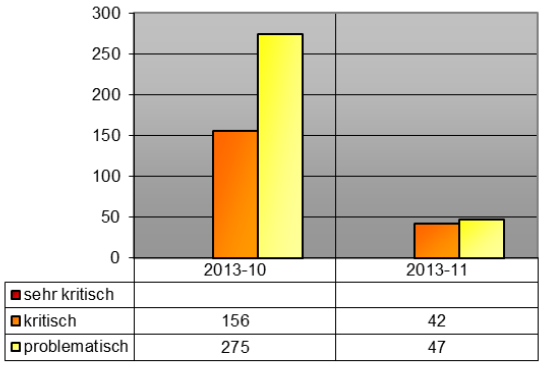
Zählen auch Sie auf uns!
http://www.scip.ch/?firma.referenzenalle

Zögern Sie nicht und kontaktieren Sie unseren Herrn Simon Zumstein unter der Telefonnummer +41 44 404 13 13 oder senden Sie ihm eine Mail an simon.zumstein@scip.ch.

3. Neue Sicherheitslücken

Die erweiterte Auflistung hier besprochener Schwachstellen sowie weitere Sicherheitslücken sind unentgeltlich in unserer Datenbank unter http://www.scip.ch/?vuldb einsehbar.

Das Dienstleistungspaket VulDB Alert System liefern Ihnen jene Informationen, die genau für Ihre Systeme relevant sind: http://www.scip.ch/?vuldb.alertsystem



	2013-10	2013-11
sehr kritisch		
kritisch	156	42
problematisch	275	47

Inhalt

11193 Google Chrome svg/properties/SVGPropertyTearOff.h Pufferüberlauf
11182 Google Chrome HTTP Parsing net/http/http_stream_parser.cc Pufferüberlauf
11179 Google Chrome Speech Input Pufferüberlauf
11150 Microsoft Windows Server Hyper-V Data Structure Value Handler erweiterte Rechte
11149 Microsoft Office WordPerfect Document Handler epsimp32.flt Pufferüberlauf
11148 Microsoft Office WordPerfect Document Handler epsimp32.flt Pufferüberlauf
11146 Microsoft Office epsimp32.flt Pufferüberlauf
11145 Microsoft Windows Graphics Device Interface Pufferüberlauf
11142 Microsoft Internet Explorer Memory Handler Pufferüberlauf
11141 Microsoft Internet Explorer Memory Handler Pufferüberlauf
11140 Microsoft Internet Explorer Memory Handler Pufferüberlauf
11139 Microsoft Internet Explorer Memory Handler Pufferüberlauf
11138 Microsoft Internet Explorer Memory Handler Pufferüberlauf
11137 Microsoft Internet Explorer Memory Handler Pufferüberlauf
11136 Microsoft Internet Explorer Memory Handler Pufferüberlauf
11130 Cisco ASA Phone Proxy Untrusted Certificate Handler Pufferüberlauf
11128 Microsoft Internet Explorer InformationCardSigninHelper icardie.dll Pufferüberlauf
11119 IBM Java erweiterte Rechte
11118 IBM Java Pufferüberlauf
11117 IBM Java Pufferüberlauf
11116 IBM Java Pufferüberlauf
11081 Microsoft Windows TIFF Image Handler Pufferüberlauf
11073 Cisco ASA CX Context-Aware Security Safe Search Enforcement Component schwache Authentisierung
11072 Cisco AnyConnect Secure Mobility Client VPN API COM Active Template Library Pufferüberlauf
11064 Cisco IOS XE TCP Packet Handler Denial of Service
11062 Cisco IOS XE Zone Based Firewall Denial of Service
11059 Mozilla Firefox/Thunderbird HTML Document Handler Pufferüberlauf
11058 Mozilla Firefox/Thunderbird Worker::SetEventListener() Pufferüberlauf
11056 Mozilla Firefox/Thunderbird Blob URL Handler nsIOService::NewChannelFromURIWith ProxyFlags() Pufferüberlauf
11055 Mozilla Firefox/Thunderbird Canvas Handler nsIPresShell::GetPresContext() Pufferüberlauf
11054 Mozilla Firefox/Firefox ESR IFRAME Handler PDF.js erweiterte Rechte
11052 Mozilla Firefox/Thunderbird Image Handler Race Condition
11051 Mozilla Firefox/Thunderbird Pufferüberlauf
11050 Mozilla Firefox/Thunderbird txXPathNodeUtils::getBaseURI() Pufferüberlauf
11048 Mozilla Firefox/Thunderbird Pufferüberlauf
11047 Mozilla Firefox/Thunderbird Input Sanitizer Pufferüberlauf
11046 Mozilla Firefox/Thunderbird Pufferüberlauf
10992 Cisco IOS Service Module schwache Authentisierung
11004 Microsoft Windows RDP Restricted Admin Mode schwache Authentisierung
10846 Google Chrome html/HTMLFormElement.cpp HTMLFormElement::submit Pufferüberlauf

3.1 Google Chrome svg/properties/SVGPropertyTearOff .h Pufferüberlauf

Risiko: kritisch
Datum: 12.11.2013
VulDB: http://www.scip.ch/?vuldb.11193

Es wurde eine Schwachstelle in Google Chrome 30.0.1599.101 ausgemacht. Sie wurde als kritisch eingestuft. Dabei betrifft es eine unbekannte Funktion der Datei svg/properties/SVGPropertyTearOff.h. Ein Aktualisieren auf die Version 31.0.1650.48 vermag dieses Problem zu lösen. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Google hat also sofort gehandelt.

3.2 Google Chrome HTTP Parsing net/http/http_stream_parser.cc Pufferüberlauf

Risiko: kritisch
Datum: 12.11.2013
VulDB: http://www.scip.ch/?vuldb.11182

In Google Chrome 30.0.1599.101 wurde eine kritische Schwachstelle gefunden. Betroffen ist eine unbekannte Funktion der Datei _net/http/http_stream_parser.cc_ der Komponente HTTP Parsing. Ein Upgrade auf die Version 31.0.1650.48 vermag dieses Problem zu beheben. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Google hat offensichtlich sofort reagiert.

3.3 Google Chrome Speech Input Pufferüberlauf

Risiko: kritisch
Datum: 12.11.2013
VulDB: http://www.scip.ch/?vuldb.11179

In Google Chrome 30.0.1599.101 wurde eine kritische Schwachstelle entdeckt. Hierbei betrifft es eine unbekannte Funktion der Komponente Speech Input. Ein Aktualisieren auf die Version 31.0.1650.48 vermag dieses Problem zu lösen. Eine neue Version kann von chrome.google.com bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Google hat demnach sofort gehandelt.

3.4 Microsoft Windows Server Hyper-V Data Structure Value Handler erweiterte Rechte

Risiko: kritisch
Datum: 12.11.2013
VulDB: http://www.scip.ch/?vuldb.11150

Eine kritische Schwachstelle wurde in Microsoft Windows Server 8/Server 2012 ausgemacht. Davon betroffen ist eine unbekannte Funktion der Komponente Hyper-V Data Structure Value Handler. Die Schwachstelle lässt sich durch das Einspielen des Patches MS13-092 beheben. Dieser kann von technet.microsoft.com bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Microsoft hat hiermit sofort reagiert.

3.5 Microsoft Office WordPerfect Document Handler epsimp32.flt Pufferüberlauf

Risiko: kritisch
Datum: 12.11.2013
VulDB: http://www.scip.ch/?vuldb.11149

In Microsoft Office 2003/2007/2010 wurde eine kritische Schwachstelle ausgemacht. Hierbei betrifft es eine unbekannte Funktion der Datei epsimp32.flt der Komponente WordPerfect Document Handler. Die Schwachstelle lässt sich durch das Einspielen des Patches MS13-091 lösen. Dieser kann von technet.microsoft.com bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Microsoft hat damit sofort gehandelt.

3.6 Microsoft Office WordPerfect Document Handler epsimp32.flt Pufferüberlauf

Risiko: kritisch
Datum: 12.11.2013
VulDB: http://www.scip.ch/?vuldb.11148

Es wurde eine kritische Schwachstelle in Microsoft Office 2003 SP3/2007 SP3 ausgemacht. Dabei betrifft es eine unbekannte Funktion der Datei epsimp32.flt der Komponente WordPerfect Document Handler. Die Schwachstelle lässt sich durch das Einspielen des Patches MS13-091 beheben. Dieser kann von technet.microsoft.com bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Microsoft hat also sofort reagiert.

3.7 Microsoft Office epsimp32.flt Pufferüberlauf

Risiko: kritisch
Datum: 12.11.2013
VulDB: http://www.scip.ch/?vuldb.11146

In Microsoft Office 2003 SP3/2007 SP3 wurde eine kritische Schwachstelle gefunden. Das betrifft eine unbekannte Funktion der Datei epsimp32.flt. Die Schwachstelle lässt sich durch das Einspielen des Patches MS13-091 beheben. Dieser kann von technet.microsoft.com bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Microsoft hat offensichtlich sofort reagiert.

3.8 Microsoft Windows Graphics Device Interface Pufferüberlauf

Risiko: kritisch
Datum: 12.11.2013
VulDB: http://www.scip.ch/?vuldb.11145

Es wurde eine kritische Schwachstelle in Microsoft Windows XP/Vista/7/8/8.1/RT/Server 2003/2008/2012, ein Betriebssystem, gefunden. Es betrifft eine unbekannte Funktion der Komponente Graphics Device Interface. Die Schwachstelle lässt sich durch das Einspielen des Patches MS13-089 lösen. Dieser kann von technet.microsoft.com bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Microsoft hat nachweislich sofort gehandelt.

3.9 Microsoft Internet Explorer Memory Handler Pufferüberlauf

Risiko: kritisch
Datum: 12.11.2013
VulDB: http://www.scip.ch/?vuldb.11142

Es wurde eine kritische Schwachstelle in Microsoft Internet Explorer bis 11, ein Webbrowser, entdeckt. Es geht dabei um eine unbekannte Funktion der Komponente Memory Handler. Die Schwachstelle lässt sich durch das Einspielen des Patches MS13-088 beheben. Dieser kann von technet.microsoft.com bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Microsoft hat sofort reagiert.

3.10 Microsoft Internet Explorer Memory Handler Pufferüberlauf

Risiko: kritisch
Datum: 12.11.2013
VulDB: http://www.scip.ch/?vuldb.11141

Eine Schwachstelle wurde in Microsoft Internet Explorer bis 11, ein Webbrowser, ausgemacht. Sie wurde als kritisch eingestuft. Es geht hierbei um eine unbekannte Funktion der Komponente Memory Handler. Die Schwachstelle lässt sich durch das Einspielen des Patches MS13-088 lösen. Dieser kann von technet.microsoft.com bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Microsoft hat hiermit sofort gehandelt.

3.11 Microsoft Internet Explorer Memory Handler Pufferüberlauf

Risiko: kritisch
Datum: 12.11.2013
VulDB: http://www.scip.ch/?vuldb.11140

In Microsoft Internet Explorer cve-2013-3917, ein Webbrowser, wurde eine Schwachstelle ausgemacht. Sie wurde als kritisch eingestuft. Es geht um eine unbekannte Funktion der Komponente Memory Handler. Die Schwachstelle lässt sich durch das Einspielen des Patches MS13-088 beheben. Dieser kann von technet.microsoft.com bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Microsoft hat damit sofort reagiert.

3.12 Microsoft Internet Explorer Memory Handler Pufferüberlauf

Risiko: kritisch
Datum: 12.11.2013
VulDB: http://www.scip.ch/?vuldb.11139

Es wurde eine Schwachstelle in Microsoft Internet Explorer bis 11, ein Webbrowser, ausgemacht. Sie wurde als kritisch eingestuft. Betroffen hiervon ist eine unbekannte Funktion der Komponente Memory Handler. Die Schwachstelle lässt sich durch das Einspielen des Patches MS13-088 lösen. Dieser kann von technet.microsoft.com bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Microsoft hat also sofort gehandelt.

3.13 Microsoft Internet Explorer Memory Handler Pufferüberlauf

Risiko: kritisch
Datum: 12.11.2013
VulDB: http://www.scip.ch/?vuldb.11138

Eine Schwachstelle wurde in Microsoft Internet Explorer bis 11, ein Webbrowser, gefunden. Sie wurde als kritisch eingestuft. Betroffen davon ist eine unbekannte Funktion der Komponente Memory Handler. Die Schwachstelle lässt sich durch das Einspielen des Patches MS13-088 beheben. Dieser kann von technet.microsoft.com bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Microsoft hat so sofort reagiert.

3.14 Microsoft Internet Explorer Memory Handler Pufferüberlauf

Risiko: kritisch
Datum: 12.11.2013
VulDB: http://www.scip.ch/?vuldb.11137

In Microsoft Internet Explorer bis 10, ein Webbrowser, wurde eine Schwachstelle gefunden. Sie wurde als kritisch eingestuft. Betroffen ist eine unbekannte Funktion der Komponente Memory Handler. Die Schwachstelle lässt sich durch das Einspielen des Patches MS13-088 lösen. Dieser kann von technet.microsoft.com bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Microsoft hat offensichtlich sofort gehandelt.

3.15 Microsoft Internet Explorer Memory Handler Pufferüberlauf

Risiko: kritisch
Datum: 12.11.2013
VulDB: http://www.scip.ch/?vuldb.11136

Es wurde eine Schwachstelle in Microsoft Internet Explorer bis 9, ein Webbrowser, gefunden. Sie wurde als kritisch eingestuft. Hiervon betroffen ist eine unbekannte Funktion der Komponente Memory Handler. Die Schwachstelle lässt sich durch das Einspielen des Patches MS13-088 beheben. Dieser kann von technet.microsoft.com bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Microsoft hat nachweislich sofort reagiert.

3.16 Cisco ASA Phone Proxy Untrusted Certificate Handler Pufferüberlauf

Risiko: kritisch
Datum: 08.11.2013
VulDB: http://www.scip.ch/?vuldb.11130

Es wurde eine kritische Schwachstelle in Cisco ASA bis 9.0.3.6 ausgemacht. Es betrifft eine unbekannte Funktion der Komponente Phone Proxy Untrusted Certificate Handler. Es sind keine Informationen bezüglich Gegenmassnahmen bekannt. Der Einsatz eines alternativen Produkts bietet sich im Zweifelsfall an.

3.17 Microsoft Internet Explorer InformationCardSigninHelper icardie.dll Pufferüberlauf

Risiko: kritisch
Datum: 08.11.2013
VulDB: http://www.scip.ch/?vuldb.11128

In Microsoft Internet Explorer 7/8/9/10, ein Webbrowser, wurde eine kritische Schwachstelle gefunden. Dabei geht es um eine unbekannte Funktionder Bibliothek icardie.dll der Komponente InformationCardSigninHelper. Die Schwachstelle lässt sich durch das Einspielen des Patches MS13-090 beheben. Dieser kann von technet.microsoft.com bezogen werden. Das Erscheinen einer Gegenmassnahme geschah 4 Tage nach der Veröffentlichung der Schwachstelle. Microsoft hat offensichtlich ziemlich schnell reagiert.

3.18 IBM Java erweiterte Rechte

Risiko: kritisch
Datum: 06.11.2013
VulDB: http://www.scip.ch/?vuldb.11119

In IBM Java bis 7SR5 wurde eine Schwachstelle gefunden. Sie wurde als kritisch eingestuft. Hierbei betrifft es eine unbekannte Funktion. Ein Aktualisieren auf die Version 5.0 SR16-FP4, 6 SR15, 6.0.1 SR7 oder 7 SR6 or higher vermag dieses Problem zu lösen. Eine neue Version kann von www-01.ibm.com bezogen werden. Das Erscheinen einer Gegenmassnahme geschah sofort nach der Veröffentlichung der Schwachstelle. IBM hat offensichtlich unmittelbar gehandelt.

3.19 IBM Java Pufferüberlauf

Risiko: kritisch
Datum: 06.11.2013
VulDB: http://www.scip.ch/?vuldb.11118

Es wurde eine Schwachstelle in IBM Java bis 7SR5 gefunden. Sie wurde als kritisch eingestuft. Dabei betrifft es eine unbekannte Funktion. Ein Upgrade auf die Version 7 SR6 or higher vermag dieses Problem zu beheben. Eine neue Version kann von www-01.ibm.com bezogen werden. Das Erscheinen einer Gegenmassnahme geschah sofort nach der Veröffentlichung der Schwachstelle. IBM hat nachweislich unmittelbar reagiert.

3.20 IBM Java Pufferüberlauf

Risiko: kritisch
Datum: 06.11.2013
VulDB: http://www.scip.ch/?vuldb.11117

Eine Schwachstelle wurde in IBM Java bis 7SR5 entdeckt. Sie wurde als kritisch eingestuft. Dies betrifft eine unbekannte Funktion. Ein Aktualisieren auf die Version 6SR15, 6.0.1 SR7 oder 7 SR6 or higher vermag dieses Problem zu lösen. Eine neue Version kann von www-01.ibm.com bezogen werden. Das Erscheinen einer Gegenmassnahme geschah sofort nach der Veröffentlichung der Schwachstelle. IBM hat entsprechend unmittelbar gehandelt.

3.21 IBM Java Pufferüberlauf

Risiko: kritisch
Datum: 06.11.2013
VulDB: http://www.scip.ch/?vuldb.11116

In IBM Java bis 7.0 wurde eine Schwachstelle entdeckt. Sie wurde als kritisch eingestuft. Das betrifft eine unbekannte Funktion. Ein Upgrade auf die Version 7 SR6 or higher vermag dieses Problem zu beheben. Eine neue Version kann von www-01.ibm.com bezogen werden. Das Erscheinen einer Gegenmassnahme geschah sofort nach der Veröffentlichung der Schwachstelle. IBM hat demnach unmittelbar reagiert.

3.22 Microsoft Windows TIFF Image Handler Pufferüberlauf

Risiko: kritisch
Datum: 05.11.2013
VulDB: http://www.scip.ch/?vuldb.11081

Eine Schwachstelle wurde in Microsoft Windows Vista/Server 2008, ein Betriebssystem, entdeckt. Sie wurde als kritisch eingestuft. Es geht hierbei um eine unbekannte Funktion der Komponente TIFF Image Handler. Die Schwachstelle lässt sich durch das Einspielen des Patches 2896666 lösen. Dieser kann von support.microsoft.com bezogen werden. Mit der Einstellung HKEY_LOCAL_MACHINESOFTWAREMicrosoft GdiplusDisableTIFFCodec = 1 kann das Problem zusätzlich adressiert werden. Als bestmögliche Massnahme wird das Installieren des jeweiligen Patches empfohlen. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Microsoft hat entsprechend sofort gehandelt.

3.23 Cisco ASA CX Context-Aware Security Safe Search Enforcement Component schwache Authentisierung

Risiko: kritisch
Datum: 01.11.2013
VulDB: http://www.scip.ch/?vuldb.11073

Es wurde eine kritische Schwachstelle in Cisco ASA CX Context-Aware Security gefunden. Dabei betrifft es eine unbekannte Funktion der Komponente Safe Search Enforcement Component. Als bestmögliche Massnahme wird das Upgrade auf eine neue Version empfohlen.

3.24 Cisco AnyConnect Secure Mobility Client VPN API COM Active Template Library Pufferüberlauf

Risiko: kritisch
Datum: 01.11.2013
VulDB: http://www.scip.ch/?vuldb.11072

Eine kritische Schwachstelle wurde in Cisco AnyConnect Secure Mobility Client entdeckt. Dies betrifft eine unbekannte Funktionder Bibliothek Active Template Library der Komponente VPN API COM. Als bestmögliche Massnahme wird das Aktualisieren auf eine neue Version empfohlen.

3.25 Cisco IOS XE TCP Packet Handler Denial of Service

Risiko: kritisch
Datum: 30.10.2013
VulDB: http://www.scip.ch/?vuldb.11064

Es wurde eine Schwachstelle in Cisco IOS XE 3.7.2S/3.8.0S gefunden. Sie wurde als kritisch eingestuft. Betroffen hiervon ist eine unbekannte Funktion der Komponente TCP Packet Handler. Ein Upgrade auf die Version 3.7.3S oder 3.8.1S

vermag dieses Problem zu beheben. Das Erscheinen einer Gegenmassnahme geschah sofort nach der Veröffentlichung der Schwachstelle. Cisco hat nachweislich unmittelbar reagiert.

3.26 Cisco IOS XE Zone Based Firewall Denial of Service

Risiko: kritisch
Datum: 30.10.2013
VulDB: http://www.scip.ch/?vuldb.11062

In Cisco IOS XE 3.4.1S/3.5.0S wurde eine Schwachstelle entdeckt. Sie wurde als kritisch eingestuft. Betroffen ist eine unbekannte Funktion der Komponente Zone Based Firewall. Ein Upgrade auf die Version 3.4.2S oder 3.5.1S vermag dieses Problem zu beheben. Das Erscheinen einer Gegenmassnahme geschah sofort nach der Veröffentlichung der Schwachstelle. Cisco hat demnach unmittelbar reagiert.

3.27 Mozilla Firefox/Thunderbird HTML Document Handler Pufferüberlauf

Risiko: kritisch
Datum: 29.10.2013
VulDB: http://www.scip.ch/?vuldb.11059

In Mozilla Firefox sowie Thunderbird 24.0 wurde eine kritische Schwachstelle ausgemacht. Hierbei betrifft es die Funktion nsContentUtils::ContentIsHostIncludingDescendantOf() der Komponente HTML Document Handler. Ein Aktualisieren auf die Version 25.0 vermag dieses Problem zu lösen. Eine neue Version kann von mozilla.org bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Mozilla hat damit sofort gehandelt.

3.28 Mozilla Firefox/Thunderbird Worker::SetEventListener() Pufferüberlauf

Risiko: kritisch
Datum: 29.10.2013
VulDB: http://www.scip.ch/?vuldb.11058

Es wurde eine kritische Schwachstelle in Mozilla Firefox sowie Thunderbird 24.0 ausgemacht. Dabei betrifft es die Funktion Worker::SetEventListener(). Ein Upgrade auf die Version 25.0 vermag dieses Problem zu beheben. Eine neue Version kann von mozilla.org bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Mozilla hat also sofort reagiert.

3.29 Mozilla Firefox/Thunderbird Blob URL Handler nsIOService::NewChannelFromURIWithProxyFlags() Pufferüberlauf

Risiko: kritisch
Datum: 29.10.2013
VulDB: http://www.scip.ch/?vuldb.11056

In Mozilla Firefox sowie Thunderbird 24.0 wurde eine kritische Schwachstelle gefunden. Das betrifft die Funktion nsIOService::NewChannelFromURIWithProxyFlags() der Komponente Blob URL Handler. Ein Upgrade auf die Version 25.0 vermag dieses Problem zu beheben. Eine neue Version kann von mozilla.org bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Mozilla hat offensichtlich sofort reagiert.

3.30 Mozilla Firefox/Thunderbird Canvas Handler nsIPresShell::GetPresContext() Pufferüberlauf

Risiko: kritisch
Datum: 29.10.2013
VulDB: http://www.scip.ch/?vuldb.11055

Es wurde eine kritische Schwachstelle in Mozilla Firefox sowie Thunderbird 24.0 gefunden. Es betrifft die Funktion nsIPresShell::GetPresContext() der Komponente Canvas Handler. Ein Aktualisieren auf die Version 25.0 vermag dieses Problem zu lösen. Eine neue Version kann von mozilla.org bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Mozilla hat nachweislich sofort gehandelt.

3.31 Mozilla Firefox/Firefox ESR IFRAME Handler PDF.js erweiterte Rechte

Risiko: kritisch
Datum: 29.10.2013
VulDB: http://www.scip.ch/?vuldb.11054

Eine kritische Schwachstelle wurde in Mozilla Firefox sowie Firefox ESR 24.0 entdeckt. Hierbei geht es um eine unbekannte Funktion der Datei PDF.js der Komponente IFRAME Handler. Ein Upgrade auf die Version 25.0 vermag dieses

Problem zu beheben. Eine neue Version kann von mozilla.org bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Mozilla hat entsprechend sofort reagiert.

3.32 Mozilla Firefox/Thunderbird Image Handler Race Condition

Risiko: kritisch
Datum: 29.10.2013
VulDB: http://www.scip.ch/?vuldb.11052

Es wurde eine kritische Schwachstelle in Mozilla Firefox sowie Thunderbird 24.0, ein Webbrowser/Mailclient, entdeckt. Es geht dabei um eine unbekannte Funktion der Komponente Image Handler. Ein Upgrade auf die Version 25.0 vermag dieses Problem zu beheben. Eine neue Version kann von mozilla.org bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Mozilla hat sofort reagiert.

3.33 Mozilla Firefox/Thunderbird Pufferüberlauf

Risiko: kritisch
Datum: 29.10.2013
VulDB: http://www.scip.ch/?vuldb.11051

Eine Schwachstelle wurde in Mozilla Firefox sowie Thunderbird 24.0, ein Webbrowser/Mailclient, ausgemacht. Sie wurde als kritisch eingestuft. Es geht hierbei um eine unbekannte Funktion. Ein Aktualisieren auf die Version 25.0 vermag dieses Problem zu lösen. Eine neue Version kann von mozilla.org bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Mozilla hat hiermit sofort gehandelt.

3.34 Mozilla Firefox/Thunderbird txXPathNodeUtils::getBaseURI() Pufferüberlauf

Risiko: kritisch
Datum: 29.10.2013
VulDB: http://www.scip.ch/?vuldb.11050

In Mozilla Firefox sowie Thunderbird 24.0, ein Webbrowser, wurde eine Schwachstelle ausgemacht. Sie wurde als kritisch eingestuft. Es geht um die Funktion txXPathNodeUtils::getBaseURI(). Ein Upgrade auf die Version 25.0 vermag dieses Problem zu beheben. Eine neue Version kann von mozilla.org bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Mozilla hat damit sofort reagiert.

3.35 Mozilla Firefox/Thunderbird Pufferüberlauf

Risiko: kritisch
Datum: 29.10.2013
VulDB: http://www.scip.ch/?vuldb.11048

Eine Schwachstelle wurde in Mozilla Firefox sowie Thunderbird 24.0, ein Webbrowser, gefunden. Sie wurde als kritisch eingestuft. Betroffen davon ist eine unbekannte Funktion. Ein Upgrade auf die Version 25.0 vermag dieses Problem zu beheben. Eine neue Version kann von mozilla.org bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Mozilla hat so sofort reagiert.

3.36 Mozilla Firefox/Thunderbird Input Sanitizer Pufferüberlauf

Risiko: kritisch
Datum: 29.10.2013
VulDB: http://www.scip.ch/?vuldb.11047

In Mozilla Firefox sowie Thunderbird 24.0, ein Webbrowser, wurde eine Schwachstelle gefunden. Sie wurde als kritisch eingestuft. Betroffen ist eine unbekannte Funktion der Komponente Input Sanitizer. Ein Aktualisieren auf die Version 25.0 vermag dieses Problem zu lösen. Eine neue Version kann von mozilla.org bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Mozilla hat offensichtlich sofort gehandelt.

3.37 Mozilla Firefox/Thunderbird Pufferüberlauf

Risiko: kritisch
Datum: 29.10.2013
VulDB: http://www.scip.ch/?vuldb.11046

Es wurde eine Schwachstelle in Mozilla Firefox sowie Thunderbird 24.0, ein Webbrowser, gefunden. Sie wurde als kritisch eingestuft. Hiervon betroffen ist eine unbekannte Funktion. Ein Upgrade auf die Version 25.0 vermag dieses Problem zu beheben. Eine neue Version kann von mozilla.org bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Mozilla hat nachweislich sofort reagiert.

3.38 Cisco IOS Service Module schwache Authentisierung

Risiko: kritisch
Datum: 24.10.2013
VulDB: http://www.scip.ch/?vuldb.10992

Es wurde eine Schwachstelle in Cisco IOS bis 15.0(2)SE1 gefunden. Sie wurde als kritisch eingestuft. Es geht dabei um eine unbekannte Funktion der Komponente Service Module. Als bestmögliche Massnahme wird Workaround empfohlen. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Cisco hat nachweislich sofort reagiert.

3.39 Microsoft Windows RDP Restricted Admin Mode schwache Authentisierung

Risiko: kritisch
Datum: 20.10.2013
VulDB: http://www.scip.ch/?vuldb.11004

Es wurde eine kritische Schwachstelle in Microsoft Windows Server 2012 R2 SP0, ein Betriebssystem, ausgemacht. Betroffen hiervon ist eine unbekannte Funktion der Komponente RDP Restricted Admin Mode. Es sind keine Informationen bezüglich Gegenmassnahmen bekannt. Der Einsatz eines alternativen Produkts bietet sich im Zweifelsfall an.

3.40 Google Chrome html/HTMLFormElement.cpp HTMLFormElement::submit Pufferüberlauf

Risiko: kritisch
Datum: 19.10.2013
VulDB: http://www.scip.ch/?vuldb.10846

In Google Chrome 30.0.1599.69 wurde eine Schwachstelle entdeckt. Sie wurde als kritisch eingestuft. Das betrifft die Funktion HTMLFormElement::submit der Datei html/HTMLFormElement.cpp. Ein Upgrade auf die Version 30.0.1599.101 vermag dieses Problem zu beheben. Das Erscheinen einer Gegenmassnahme geschah vor und nicht erst nach der Veröffentlichung der Schwachstelle. Google hat demnach vorgängig reagiert.

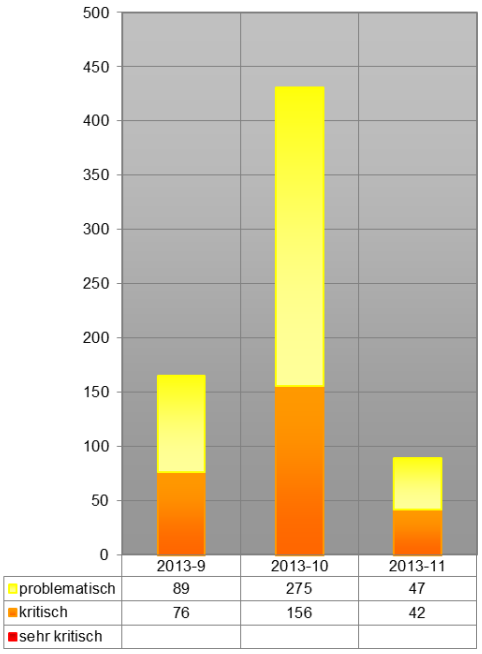
4. Statistiken Verletzbarkeiten

Die im Anschluss aufgeführten Statistiken basieren auf den Daten der deutschsprachige Verletzbarkeitsdatenbank der scip AG.

http://www.scip.ch/?vuldb

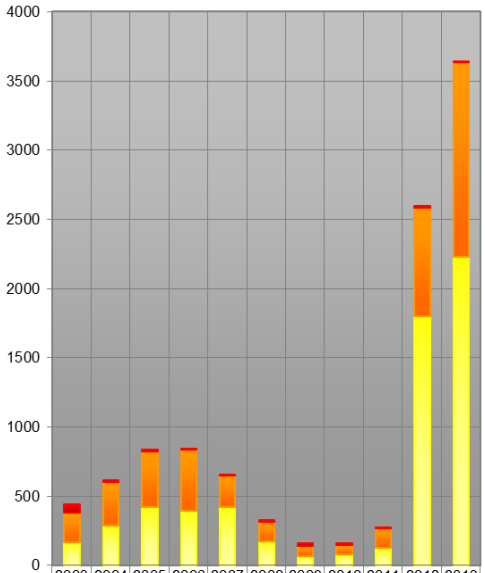
Zögern Sie nicht uns zu kontaktieren. Falls Sie spezifische Statistiken aus unserer Verletzbarkeitsdatenbank wünschen so senden Sie uns eine E-Mail an info-at-scip.ch. Gerne nehmen wir Ihre Vorschläge entgegen.

Auswertungsdatum:	18. November 2013



	2013-9	2013-10	2013-11
problematisch	89	275	47
kritisch	76	156	42
sehr kritisch			

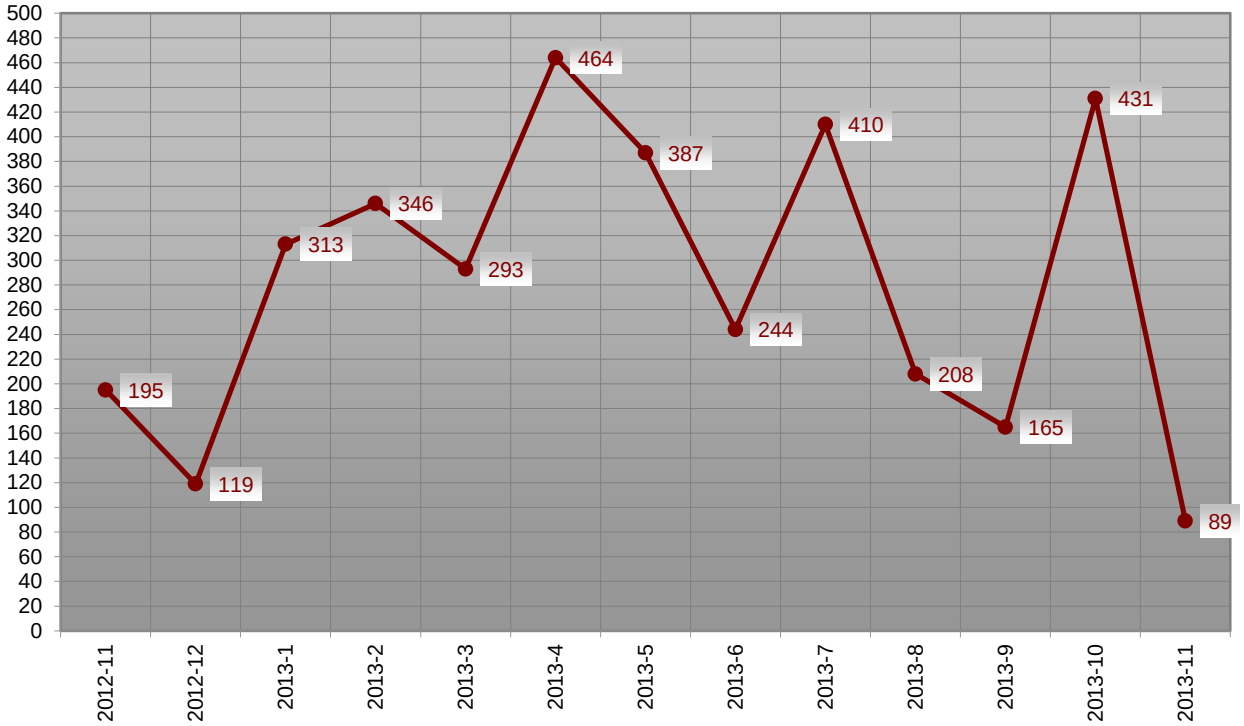
Verlauf der letzten drei Monate Schwachstelle/Schweregrad



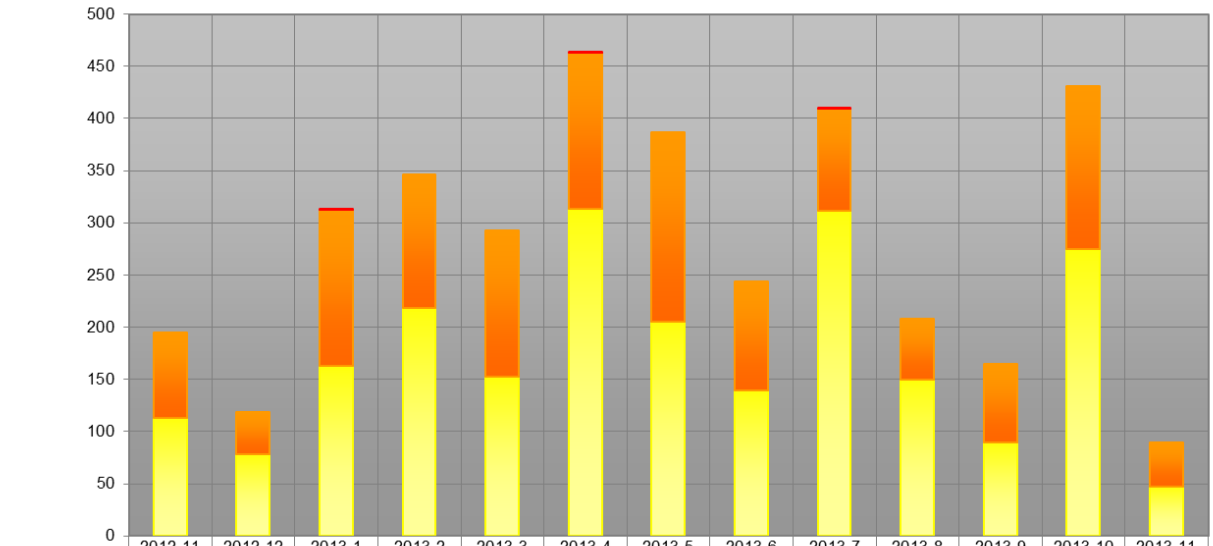
	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
sehr kritisch	56	15	15	6	11	11	21	10	8	11	3
kritisch	214	314	402	442	229	140	72	67	142	783	1403
problematisch	170	287	423	396	419	176	70	81	126	1802	2231

Verlauf der Anzahl Schwachstellen pro Jahr

Registrierte Schwachstellen by scip AG



Verlauf der Anzahl Schwachstellen pro Monat



	2012-11	2012-12	2013-1	2013-2	2013-3	2013-4	2013-5	2013-6	2013-7	2013-8	2013-9	2013-10	2013-11
sehr kritisch			1			1			1				
kritisch	82	41	149	128	141	150	182	105	98	58	76	156	42
problematisch	113	78	163	218	152	313	205	139	311	150	89	275	47

Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat

5. Labs

In unseren scip Labs werden unter http://www.scip.ch/?labs regelmässig Neuigkeiten und Forschungsberichte veröffentlicht.

5.1 Secure Mobile Data

14.11.2013 Rocco Gagliardi, roga-at-scip.ch

Everyone needs access to data, whether it is online or offline. Sometimes, there is a need to transfer data between two devices (hopefully both with encrypted storage).

Sometimes, you are an unprivileged user and cannot install software (better: you – as a security expert – always work as an unprivileged user, even on your home computer, and sometime you do not have the ability to go in privileged mode).

This is the time where the workarounds are pretty creative. In these situations, you are under pressure (you have to present something and your VGA adapter is in the office, so transfer the presentation (or, just to make sure everything will work, the whole directory) to the first computer you can attach to the projector using the first USB key you get): data exposed for a short period of time may remain as a copy on a USB key where the files were just deleted. Do you use a FIPS eraser to clean the files?

Time, urgency, pressure may lead to errors and finally to unprotected data.

In recent years, TrueCrypt has helped us to keep data secure, but still requires the user to work rigorously, requires the ability to run software on a device, expose the pass phrases to keyboard sniffing attacks and is limited to some device+OS combinations.

Protecting the Data

I have tried different solutions over the years, and – finally – last June, I spent around 160 Swiss Francs and ordered a Carbide USB Stick, a USB key with hardware encryption.

Pros

Basically, if you work rigorously, data is rather secure (note that even if you leave the data on the stick, the processing of the data is in the computer memory, swap etc. but your HD is encrypted!).

The device has following features:

- Encryption Type: AES 256CBC
- PINs: 7 to 15 digit admin and user PINs, alphanumeric keypad
- Tamper Resistant: Tamper evident construction, brute force hack resistant
- Everything Proof: Water, Dust, Shock & Tamper Resistant
- Drivers and Software Required: None
- Certification: FIPS Security 140-2 Level 3 Certified (Certificate number 1873)
- Certification: IP57 (#LVD-D120789COC), MIL-STD-810F

Unlike most encrypted drives that only work with specific combination of devices+OSs, the physical PIN code entry on the side of the drive allows for universal compatibility. You can unlock the key using the keypad and stick in the USB device port in the next 30 minutes. The computer or Android devices or television recognizes it as a normal USB key.

Remove the device (physically or virtually) and the drive is locked.

In addition to the physical and security defenses of the Carbide drive, the drive is also protected from viruses by ClevX DriveSecurity™ powered by ESET. Carbide includes a full 5-year license for DriveSecurity.

Contra

I found just one problem: the speed. If you work on Word documents, then the delay is noticeable; in this case the temptation to make a temporary copy on the desktop is irresistible.

Benchmarked Speed: 10MB/s and up, comparable to other high-end FIPS-certified hardware-encrypted drives. Random read/write of small blocks comparable to non-encrypted retail drives. Your portable apps hum along just fine!

Summary

Why so serious about data security? It is very easy to lose data. And sometime you don't know which data is lost. If you need a secure portable storage, this is the only usable solution I know. If the key is lost, you can reasonably be secure

that the data will be unreadable.

On the other side, with this device you can read data on each device reading normal USB keys.

5.2 Vorgehen und Prozesse im Falle, dass Viren in Unternehmen auftreten

7.11.2013 Flavio Gerbino, flge-at-scip.ch

Unternehmen haben Lösungen im Einsatz, die sie gegen Viren schützen: Strategien, Konzepte und nicht zuletzt intelligent implementierte Technologien, die zeitnah aktualisiert werden. Woran es aber oft mangelt, sind klare Vorgehensweisen im Zusammenhang mit Virenschutz und die explizite Vorgehensweise beim Auftreten eines akuten Virenbefalls im Unternehmen. Sogar die formale Basis d.h. Regelungen im Bereich Incident Mangement beziehungsweise CERT-Szenarien existieren, doch wenn es nun im Ernstfall darum geht, schnell, koordiniert und zielgerichtet vorzugehen, fehlt es an Prozessen, Checklisten, Tools, Kommunikationskanälen etc. die genau darauf ausgerichtet sind, das konkrete Problem eines Virenbefalls effizient zu behandeln. In diesem Artikel werden daher wichtige Hinweise zu Abläufen aufgearbeitet, die nötig sind, damit eine rationale Handhabung eines Virenbefalls gelingt.

Subjektiv gesehen, scheint es auch, dass das Thema Virenbefall in der Medienlandschaft aus dem Fokus gerückt ist, ausser im Kontext der populäreren Spionagefälle, die gerne aufgegriffen werden. Dies gibt mir auch Anlass, dieses in den Hintergrund geratene Thema wieder zu vergegenwärtigen. Denn Risiken sind dann am grössten, wenn man sich in vermeintlicher Sicherheit wiegt.

Was wird in diesem Labs- Artikel unter Viren verstanden?

Als Virenbefall wird im allgemeinen das Auftreten jeglicher Malware bezeichnet. Der Terminus Malware steht für Schadsoftware und ist bekanntlich ein Kofferwort aus den Begriff *malus* (lat. schlecht) bzw. malicious (engl. bösartig) und dem Begriff *ware*. Malware wird als Sammelbegriff verwendet, um das grosse Spektrum an feindseliger und intrusiver Software oder Programmen, die in der Lage sind, offensichtlich, getarnt oder gänzlich im Hintergrund agierend, unerwünschte und gegebenenfalls schädliche Funktionen auszuführen. Das heisst Programme, die explizit dafür entwickelt wurden, um beim Benutzer unerwünschte oder schädliche Aktionen vorzunehmen. Beispiele von Malware in einer nicht abschliessenden Aufzählung sind:

- Viren
- Würmer
- Malicious Code
- Spyware
- RootKits
- Trojaner (machen etwa 70 % aller Malware aus!)
- Backdoors

Da sich der Begriff Virus – auch wenn fachlich nicht ganz korrekt – als Synonym für Malware etabliert hat, wird dieser im weiteren Verlauf dieses Artikels zur Vereinfachung der Lesbarkeit stellvertretend für alle Formen von Malware verwendet. So ist die Rede von Virenschutz, womit viel allgemeiner der Schutz vor Schadsoftware jeglicher Art gemeint ist.

Dass sich Viren verbreiten, entspricht heute nicht mehr unbedingt der Hauptaufgabe eines typischen Virus.
Die heute gängigen Viren, meist in Struktur von Trojanischen Pferden, verfolgen viel mehr den primären Zweck, gezielt Systeme fernzusteuern, auszuspionieren oder beides.

Der Spezialfall eines Sicherheitsvorfalls – Die Vireninfektion

Sicherheitsvorfälle sind in diesem Kontext gesehen Ereignisse, welche die Sicherheit der Services, Daten oder Infrastruktur eines Unternehmens negativ beeinträchtigen. Ursachen für Sicherheitsvorfälle können gezielte Attacken oder versehentliche Fehlmanipulationen sein. Unternehmen überwachen ihre IT-Infrastruktur konstant mit dem Ziel, Sicherheitsvorfälle zu erkennen und entsprechend ihrer Kritikalität zu behandeln.

In diesem Artikel werden Anhaltspunkte für die Handhabung von Sicherheitsvorfällen der besonderen Kategorie Virenbefall vorgeschlagen. Der Fokus ist auf reaktive Aktionen im Ernstfall gerichtet. Es wird aber davon ausgegangen, dass allgemeine und grundsätzliche Regeln im Zusammenhang mit Sicherheitsvorfällen existieren und etabliert sind.

Mögliche Fälle

Das Auftreten eines Virus innerhalb eines Unternehmens sollte – nach Relevanz bezogen auf potentielle Auswirkungen und Gefahrenpotential – kategorisiert werden. Die folgende Tabelle gibt einen Überblick der sinnvollen Szenarien:

	Malware	Innerhalb	Auswirkung	Risiko	Aktion	Vorgehen
1	Neu	Nein	Informationsquelle (Medien, Vulnerability Database, Newsletter, ...)	Gering	Patternupdate erforderlich	Aktiv: Aktives intiieren eines Patternupdates
2	Neu	Ja	Ein unbekannter Virus tritt im Unternehmen auf, kein Patternfile vorhanden, AV-Konsole/Scanner wirft keinen Alarm, Schadwirkung/Verbreitung in Gang	Akut	Schadwirkung, Verbreitung begrenzen	Reaktiv: Akutmassnahmen gemäss Beschreibung im Artikel
3	Bekannt	Ja	AV-Konsole/Scanner schlägt Alarm, infiziertes File wird automatisch in Quarantäne verschoben	Gering	Schadwirkung/ Verbreitung gestoppt	Aktiv: AV Tools gemäss den in den Teams festgelegten Abläufen
4	Bekannt	Ja	AV-Konsole/Scanner schlägt Alarm, infiziertes File kann nicht in Quarantäne verschoben werden	Akut	Schadwirkung/ Verbreitung begrenzen, Patternverteilung kontrollieren	Reaktiv: Akutmassnahmen gemäss Beschreibung im Artikel
5	Bekannt	Ja	False Positive, harmloses File wird als Virus erkannt und automatisch in Quarantäne verschoben	Mittel	evtl. Exception definieren, Patternupdate erforderlich, sodann Quarantäne aufheben	Reaktiv: AV Tools gemäss den in den Teams festgelegten Abläufen

Jene Fälle aus der Tabelle, die akute Massnahmen erfordern (Nr. 2 und 4), werden in diesem Dokument weiter beschrieben. Die Fälle mit geringem oder mittleren Risiko würden im Unternehmen an interne Teams zur Bearbeitung mittels Standardverfahren weitergeleitet.

Vorgehensweise:

Der Ablauf zur Einschätzung und weiteren Beantwortung von Vorfällen im Kontext eines Virenbefalles wird folgendermassen Strukturiert:

Echtzeit
- Erkennung / Beurteilung
- Alarmierung
- Sofortmassnahmen / Isolation

Aufarbeitung
- Intervention / Analyse
- Postvention / Nachbearbeitung

Die Vorgehensweise gliedert sich offensichtlich in zwei Phasen, entsprechend der durch die Dringlichkeit des Vorfalles gebotenen zeitlichen Komponente: In einer ersten Echtzeit Phase werden Schritte hinsichtlich Erkennung, Beurteilung und allenfalls Alarmierung sowie Sofortmassnahmen gesetzt. Diese Aktionen werden, um eine potentielle Verbreitung und Schadenswirkung zu minimieren, innerhalb kürzest möglicher Frist abgeschlossen. Danach folgt eine zeitlich minder kritische Reaktion in der zweiten Phase der Aufarbeitung.

Schritt 1: Erkennung / Beurteilung

Die zentrale Bedeutung kommt bereits dem ersten Schritt zu: Dem Erkennen, dass ein Vorfall gegeben ist und *Abschätzung* der Relevanz desselben.

Es obliegt den Systemverantwortlichen des betreffenden Bereichs, sicher zu stellen, dass die Meldefunktionen der automatisierten Überwachungssysteme (unter anderem Malware/Antivirus-Tools und -Konsolen) so eingerichtet sind, dass diese die von ihnen generierten Meldungen automatisch an die entsprechenden Instanzen im Betrieb/Operations weiterleiten. Jede von einem eigenständigen Viren-Überwachungssystem generierte Meldung sollte einer zentralen Instanz zugeführt werden, wo eine umfangreiche Korrelation aller empfangenen Mitteilungen erfolgen kann. Geeignete Schwellwerte zur Erhöhung der Treffsicherheit der Überwachung sind durch die adäquaten Teams an die jeweilige Umgebung zu definieren.

Hat ein Systemverantwortlicher Kenntnis vom Auftreten eines Virus erhalten, so nimmt er eine erste Beurteilung vor. Diese liegt im Ermessen des Systemverantwortlichen, der auf Grund der ihm zu diesem Zeitpunkt vorliegenden Informationen eine Einschätzung vornimmt. Als Basis für die Beurteilung wird die Dringlichkeit aus der Wahrscheinlichkeit des Eintretens sowie dem Schadensausmass beim Eintreten abgeleitet. Eine detaillierte Analyse sollte aus zeitlichen Gründen erst zu einem späteren Zeitpunkt erfolgen. Unter Umständen wird dann dabei die initiale Beurteilung revidiert. In jedem Fall ist aber der Präventionsgedanke massgebend. Das heisst: Im Zweifelsfall besser zu hoch als zu gering einstufen.

Schritt 2: Alarmierung

Noch bevor weitere Massnahmen angegangen werden, sind vordefinierte Stakeholders und Teams zu informieren/involvieren: Dies sind üblicherweise:

- Betrieb
- Incident Management
- IT-Security
- Applicationverantwortliche
- Businessverantwortliche

Die Alarmierung erfolgt mittels direkten Kommunikationskanälen (am einfachsten Telefon oder direktes Gespräch), zum Zwecke der unmittelbaren Bestätigung, dass die Information platziert werden konnte. Mit der rückbestätigten Alarmie-

rung übergibt der Systemverantwortliche die Koordination der weiteren Vorgehensweise an die definierten Stellen. Bis zum offiziellen Handover bleibt die Verantwortung weiterhin beim Systemverantwortlichen.

Schritt 3: Sofortmassnahmen / Isolation

Abhängig von der Dringlichkeit des Vorfalles entscheidet der vordefinierte Verantwortliche einer entsprechenden Arbeitsgruppe, ob und in welchem Mass die Behandlung des Gefahrenpotentials forciert oder beschleunigt werden muss. Er entscheidet, ob Sofortmassnahmen – in der Regel auf Vorschlag der Systemverantwortlichen – eingeleitet werden müssen und/oder ob eine weiter Eskalation nötig ist. Entscheidet er sich für bestimmte Sofortmassnahmen, so spricht er diese mit den betroffenen Betriebs- und Teams, dem Applikations- und Businessverantwortlichen und dem Incident Management ab.

Bei besonders kritischen Vorfällen (grosse Schäden innerhalb des Unternehmens) kann via *Incident Management* und allfälligen *BCM Prozessen* ein *Notfallstab* mit entsprechenden Teams einberufen werden. Der Verantwortliche für diese Arbeitsgruppe entscheidet auch in Absprache mit dem Incident Management, ob weitere Ansprechstellen innerhalb des Unternehmens informiert bzw. invoviert werden müssen.

Die Zielsetzung besteht darin, den Impact zu begrenzen und einer weiteren Ausbreitung Einhalt zu bieten, so dass die akuten negativen Auswirkungen auf ein Minimum reduziert sind. Kann dies nicht erreicht werden, so sind weitere Sofortmassnahmen, etwa im Kontext der Isolation, in Absprache mit der betroffenen Betriebsgruppe und Teams und natürlich dem Security Officer, den Business Ownern und dem Incident Management zu erläutern.

Schritt 4: Intervention / Analyse

Sind die akuten negativen Auswirkungen mit adäquaten Massnahmen adressiert, wird der Vorfall einer eingehenden Analyse unterzogen. Zielsetzung ist hierbei die Aufarbeitung von:

- Ursache
- Hintergründe
- genauen Verlauf

Basierend auf diesen Informationen werden Lösungsvorschläge ausgearbeitet, um den Vorfall nachhaltig zu bereinigen. Im Gremium der im Laufe der Bearbeitung des Vorfalles involvierten Personen wird die Lösungsvariante ausgewählt, die in weiterer Folge zu Umsetzung kommen wird.

Die Dokumentation sämtlicher Aktionen erfolgt ab diesem Schritt sowohl im Incident Management als auch in Form von *Lessons-Learned*. Verantwortlich für die Vollständigkeit der Dokumentation sind die zuständigen Systemverantwortlichen.

Schritt 5: Postvention / Nachbearbeitung

Zur nachhaltigen Bereinigung des Vorfalles wird die unter Schritt 4 ausgewählte Lösungsvariante zur Umsetzung gebracht. Es sollte sichergestellt werden, dass ein erneutes Auftreten unterbunden wird, bei gleichzeitiger Wiederherstellung des Betriebszustandes.

Die Erkenntnisse aus dem Verlauf des Falles werden sinngemäss in einem *Lessons-Learned* Verfahren weiter verwertet. Abschliessend ist die Dokumentation zu aktualisieren und sämtliche im Laufe der Bearbeitung involvierten Personen sind vom Abschluss des Vorfalles und den Erkenntnissen daraus zu informieren.

Unterstützende Mittel:

Die Definition der Hilfsmittel ist weitgehend System- und Malware- spezifisch. In jedem relevanten Bereich sollten klare Checklisten und Toolboxen definiert werden, die im Ernstfall sukzessive abgearbeitet werden können. Es sollte dem Systemverantwortlichen obliegen, an ihren Bereich angepasste, spezifische Definitionen zu erstellen und aktuell zu halten.

Standardverfahren und Checklisten

Basierend auf den hier erörterten Hinweisen sollten Unternehmen konkrete Handlungsanweisungen (Checklisten etc.) separat und angepasst an die jeweiligen Bereiche und Themenkreise, die von den zuständigen Systemverantwortlichen definiert werden. Diese Listen/Factsheets haben in der gebotenen Kürze spezifisch eine Wegleitung zu bieten, um in Krisensituationen fokussiert vorzugehen – vorzugsweise als klare Schritt-für-Schritt Kurzanleitung. Im Sinne einer intuitiven Verständlichkeit minimal, textbasiert und primär visuell darstellend.

Diese Listen/Factsheets sollten regelmässig auf ihre Relevanz und Aktualität hin überprüft werden und zwar periodisch wie nach jeder signifikanten Anpassung der Sytemlandschaft. Es sollte auch für diese Dokumentenart eine formale Abnahme geben.

Tools

Pro betroffenem Bereich sollte eine Toolbox zur Bewältigung eines Malware-Vorfalles zusammengestellt werden. Diese beinhalten Hilfsmittel, Ressourcen und Werkzeuge:

- **Produktspezifische Knowledgebase**: Sammlung von Informationen (Artikel, Prozesse, White Papers, Benutzerhandbücher, erfahrungsberichte) zu einem Produkt
- **Malware-Scanner**: Freie Dienste zur Online Analyse von verdächtigen Dateien und URLs auf Viren, Würmer, Trojaner und andere Arten von Malware, identifiziert von Antivirus-Software und Web-Analyzer.

Zusammenfassende Übersicht:

Phase	Aktion	Detail/Hilfsmittel
1. Erkennen und Beurteilen	1. Erkennen	Malware-Konsolen, AV, Anomalien. Einordnen.
	2. Beurteilen	
	3. Kategorisieren	
2. Alarmieren	1. Empfänger bestimmen	Vordefinierte Points-of-Contact, Liste von Verantwortlichen. Arbeitsgruppenleiter, Teams, Security Officer, Business Owner. Synchrone Medien nutzen (Telefon, direktes Gespräch).
	2. Alarmieren	
	3. Bestätigung einholen	
3. Sofort handeln und isolieren	1. Dringlichkeit einschätzen	Vordefinierte Points-of-Contact, Liste von Verantwortlichen. Arbeitsgruppenleiter, Teams, Security Officer, Business Owner. Abstimmungen, weiteres Vorgehen erörtern.
	2. Sind Sofortmassnahmen nötig?	
	3. Ist die Ausbreitung gestoppt?	
4. Analysieren und Lösungen umsetzen	1. Prüfen, ob Status Quo wiederhergestellt ist	Check ob Status Quo vor dem Vorfall wiederhergestellt ist. Bestätigung von Business-Ownern und Operations einholen. Alle Phasen im Case nachvollziehbar dokumentieren.
	2. Sicherstellen, dass der Betrieb okay ist.	
	3. Case aktualisieren	

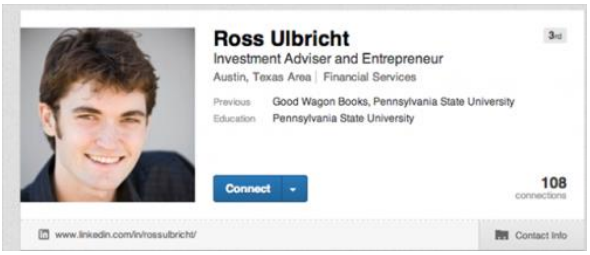
Fazit

Es ist von grosser Bedeutung, sich nicht nur mit der Technik rund um Malware und Antivirus auseinanderzusetzen, sondern auch klare Strukturen für die Handhabung dieser besonderen Art eines Vorfalls zu definieren. Besonders sollte man sich davor hüten, sich in Sicherheit zu wiegen, nur weil man extensive Anti-Malware Technologien im Einsatz hat und das klassiche Virenthema keine besondere mediale Präsenz mehr geniesst. Es genügt nicht, sich etwas einfach wegzuwünschen, mit dessen negativen Begleiterscheinungen man sich nicht auseinandersetzen möchte. Besser scheint es, sich planerisch mit möglichen Szenarien zu konfrontieren und basierend darauf Methoden und Abläufe mit den entsprechenden Verantwortlichen und Teams zu vereinbaren. Diese bieten im Ernstfall systematische Anhaltspunkte und Orientierung.

5.3 OpSec on the Silk Road: Learning from Pirates

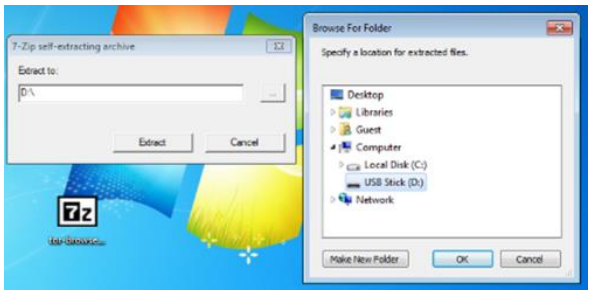
24.10.2013 Stefan Friedli, stfr-at-scip.ch

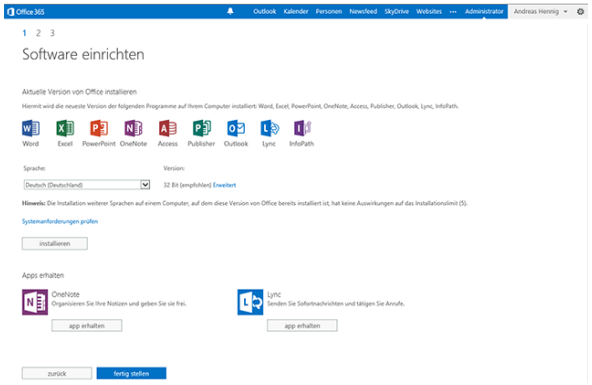
Only a couple of weeks ago, *Dread Pirate Roberts* (DPR) was arrested for his extensive involvement in Silk Road, an online platform only reachable via Tor offering more than ten-thousand sales listings for controlled substances. The variety of the products offered was immense: LSD, cocaine, methamphetamine, heroin, ecstasy – if you can name it, it was most likely for sale on Silk Road. You could have considered Silk Road something like eBay for illegal drug trafficking. You could find almost everything and even leave a seller feedback once the transaction was done and over. But not only drugs were sold on Silk Road: Hacked accounts for social networks, weapons, and various *services* ranging from digital petty theft to more extreme things, contract killers being just one of the more unsettling examples. Ross William Ulbricht, DPR's real name, allegedly made millions with his website. The actual amount is disputed, but it is to be assumed that it was worth the trouble.



Silk Road's performance depended massively on the fact that it was hosted anonymously and was only accessible via Tor. Tor is an important tool to provide users with anonymity, leaving it up to them how they use this privilege. People that are threatened and violated by oppressive governments can use Tor to communicate their dissent. Sokwanele for example, is a Zimbabwean website promoting democracy, illustrating the atrocities of the regime under Robert Mugabe. The content, while horrific in its nature, is important and puts the creators at great risk of being in harm's way for publishing it. Tor is providing an amount of anonymity that makes it easier to stay moderately safe, no matter if this anonymity is required to exercise free speech or to buy drugs on Silk Road. Silk Road was incredibly popular, especially considering the fact that it was never reachable outside of Tor. Contrary to popular opinion, it is not hard to access sites like these, even for less tech-savvy users. Easy installers are readily available, that will allow access to Tor within minutes without any configuration or the need for credentials. TorBrowser, for example, is a standalone, portable installation of Firefox that

will automatically redirect all traffic via Tor. It is easier to install than the most recent versions of Microsoft Office.





The question that the Silk Road bust raised almost instantly is clear: If this website was only accessible via Tor, how was Dread Pirate Roberts caught? Especially considering the fact that leaked documents recently confirmed that intelligence services were trying hard to get a handle on Tor, but were still failing? .

According to available sources, the key to Ulbricht's downfall was not based on any intelligence agency's skillful interception of encrypted communication. Tor, as far as we know today, remains a fairly anonymous way to use and offer services, whereas anonymous does not necessarily mean secure. Ulbricht, however, failed where most people do: When it comes to OpSec.

Considering that Ulbricht made a ton of money running a fairly smooth operation that enabled the sale of mostly illegal products and services for a surprisingly long time, the list of mistakes he made, concerning his operational security, that have now surfaced is surprising. For example, Ulbricht was looking for an IT professional for a bitcoin-backed venture in a forum, using his real email address to communicate with potential candidates. In a world where it is hard to determine if anyone you talk to on a computer is really what he claims to be, this seems like a really, really unfortunate idea. A similarly bad idea is the use of social networking to be vocal about ethical and ideological mindsets. That rings true for almost everyone, especially in a world after Snowden, but especially if you are currently building and running an international black market and try to stay somewhat in the shadows to avoid going away for a long, long time.

But it does not stop there. Dread Pirate Roberts also used various drug-related forums outside of the Tor-Protected Internet to market his product and get in touch with customers. He connected to his VPN server after logging into his Gmail account with the same IP address. He used his StackOverflow.com-alias frosty in the public SSH key stored on the Silk Road server. He also used his real name on StackOverflow. The list does not stop there, but it illustrates how many mistakes he made down the road that ultimately led to his arrest.

There are a couple of things that are interesting about all of this. First of all: Most OpSec mistakes seem not too bad as long as you look at them as a trail leading from you to a certain incident. But it is often forgotten that the trail works the other way too. Often, an investigation will start at the scene of the crime, search for the cookie crumbs and then follow them back to the jar they came from. Ulbricht's post about an anarchistic vision of economic simulation he posted on LinkedIn in early 2012 would most likely not have been suspicious, but once the investigators got him on their list, the statement made a lot more sense in the context of Silk Road. Bold statements on your world-views are risky in this time and age, even if you don't run an international drug exchange. If you do, you might want to shut down your Facebook account before you do it or at least refrain from posting content related to your activity.

The other conclusion is much more concerning though: What if Dread Pirate Roberts did everything right? What if he did not make these mistakes or if somebody learns from his school-of-hard-knocks lesson on OpSec? If it takes that many mistakes to be taken down, we might just face the next Dread Pirate Roberts very soon.

5.4 Blog Digest Oktober 2013

31.10.2013 Marc Ruef, maru-at-scip.ch

Der scip Blog Digest ist eine am Ende des Monats erscheinende Zusammenfassung der wichtigsten, spannendsten und verrücktesten Beiträge aus der internationalen Blogosphäre. Mit der Durchsicht dieser Postings wird es einfach und unkompliziert möglich, in Bezug auf Entwicklungen im Bereich IT-Security auf dem Laufenden zu bleiben. Folgen Sie unserem Team auf Twitter, um jeweils die aktuellsten News zu erhalten.

- 40 inappropriate actions to take against an unlocked PC (troyhunt.com)
- Backdoor Evasion Using Encrypted Content (blog.sucuri.net)
- Bypassing security scanners by changing the system language (net-security.org)
- Feds Take Down Online Fraud Bazaar 'Silk Road', Arrest Alleged Mastermind (krebsonsecurity.com)
- Fingerprinting Ubuntu OS Versions using OpenSSH (blog.spiderlabs.com)
- Fingerprints are Usernames, not Passwords (blog.dustinkirkland.com)
- Hacking a Counterfeit Money Detector for Fun and Non-Profit (blog.ioactive.com)
- How 'bout them apples (hackerfactor.com)
- How I compiled TrueCrypt 7.1a for Win32 and matched the official binaries (madiba.encs.concordia.ca)
- How to Design – And Defend Against – The Perfect Security Backdoor (wired.com)
- iMessage Privacy (blog.quarkslab.com)
- Introducing WhiteHat Aviator – A Safer Web Browser (blog.whitehatsec.com)
- LinkedIn's New Mobile App Called 'a Dream for Attackers' (bits.blogs.nytimes.com)
- Metasploit website hijacked by pro-Palestinian hackers… via fax (grahamcluley.com)
- Mozilla Lightbeam Add-On Shows Risk of Third Party Sites (taosecurity.blogspot.com)
- Photo Forensics: Detect Photoshop Manipulation with Error Level Analysis (resources.infosecinstitute.com)
- Reminder: Finishing the Removal of an Old Search Setting (newsroom.fb.com)
- Reverse Engineering a D-Link Backdoor (devttys0.com)
- RFC 7034 – HTTP Header Field X-Frame-Options (tools.ietf.org)
- Security Awareness Training Evolution: Why Bother (securosis.com)
- So it turns out that annoying high frequency… (facebook.com)
- The Bonehead Mistake That Brought Down an Online Drug-Dealing Empire (slate.com)
- TrueCrypt Audit Could Answer Troubling Questions (threatpost.com)
- Under Pressure (securelist.com)
- Watch 15 Awesome MS-DOS Viruses in Action (wired.com)
- What Do Attendees During a Security Conference? (blog.rootshell.be)
- Why you should not use autocomplete (yoast.com)

6. Rätselgeschichte

Bild: Niki Edge

Im zweiten Teil der scip-Fortsetzungsgeschichte begeben wir uns in ein Zürich, das wir noch nicht kennen. Es ist das Zürich der Zukunft, in der Information zur Währung geworden ist. Damit sind Codes und Rätsel an der Tagesordnung.

Was bisher geschah: Ein namenloser Informationshändler hat eine Festplatte von einem Deutschen erhalten, der sogleich angeschossen wurde. Die Daten auf der Festplatte sind für eine gewisse Anne wichtig. Ihr Aufenthaltsort: unbekannt.

Der Albisriederplatz. Eigentlich war das ja klar. Vor ein paar Jahren haben sich da viele Exil-Deutsche niedergelassen. Warum, das weiss keiner. Auf jeden Fall sind sie da. Dort gibt es auch Currywurst aus Fleisch unbekannter Herkunft und was in der Currysauce ist, will erst recht keiner wissen. Sonst ist es wie überall in Europa, wie überall in der Schweiz. Grau, zusammengeschustert und gerade noch so knapp funktionstüchtig. Nach dem Krieg, nachdem all die Wracks der Panzer beseitigt und die meisten unexplodierten Bomben gefunden und entschärft wurden, haben die Überbleibsel der politischen Elite – die für das ganze Debakel verantwortlich waren – festgestellt, dass der Krieg wohl gar keine so gute Idee war. Obwohl ich damals noch nicht auf der Welt war, hätte ich das denen schon vor der ersten Explosion in Deutschland sagen können. Wenn es nicht so tragisch wäre, dann müsste ich darüber lachen. Und es ist nicht so, als ob diese Gedanken neu wären. Aber wenn ich vom Paradeplatz zum gehe, dann habe ich während den ganzen drei Kilometern Zeit zum Nachdenken, denn keiner will so recht an den Strassenrand schauen.

Es ist zwar besser als auch schon. Kurz nach dem Zusammenbruch der Gesellschaft, die wir mittlerweile nur noch aus Büchern und was noch auf Servern von Zeitungen übrig ist kennen, war alles grauenhaft. Die Strassen hatten Krater, ausgebrannte Autos und verbrannte Menschen lagen am Strassenrand. Mittlerweile sind die Krater mit Erde aufgefüllt worden, die Autos grösstenteils beseitigt obwohl es immer Ausnahmen gibt. Trams stehen komischerweise noch viele herum. Die waren wohl zu schwer um wegzuschaffen. Und anstelle von menschlichen

Überresten liegen oder sitzen am Strassenrand die Obdachlosen. Manchmal sehen die auch eher tot als lebendig aus.

Am Albisrieder Zoll vorbei mache ich einen kleinen Umweg zu Maik. Nicht Mike, sondern Maik. Da ist der Maik pingelig. Der Mann aus Dresden kennt laut eigenen Angaben jeden, der im Deutschen Bezirk wohnt. Ich will wissen, was er über Anne weiss. Mag Motorräder, hat noch mehr Tattoos. Das auf dem Rücken ist das eines Phönix. Schon doof, denke ich mir. Wieso macht man sich Tattoos, wenn diese ein so guter Identifikationsfaktor sind? Aber sie hat auch nicht den selben Job wie ich, bei dem es oft drauf ankommt, so unauffällig wie möglich zu sein.

Wie dem auch sei, Maik kennt die Anne nur vom Hörensagen. Er weiss, dass sie Kaffee mag. Wie mir das nützen soll, weiss ich nicht. Wenn ich nicht wüsste, dass keine Information vollkommen nutzlos ist, dann wäre ich sauer auf den Preis, den ich für Annes Beschreibung und das Wissen über ihre Vorliebe für Kaffee bezahlt habe. Immerhin hat er mir die Adresse bestätigt: Zwölfter Stock im 2000er-Haus. Das ist ein Gebäude, aus drei Gebäuden bestehend, die wohl in den 1960ern oder 70ern gebaut wurden und irgendwie zusammengewachsen sind. Das Haus heisst so, weil eine alte Werbeschrift noch da steht. Wofür sie Werbung macht, weiss aber keiner mehr. Ursprünglich war das Haus auch nicht so hoch, aber als in Zürich der Wohnraum knapp geworden ist, sind viele Häuser einfach aufgestockt worden. Ich werde nervös, als ich im Treppenhaus bin. Was, wenn Anne bewaffnet ist? Schusswaffen sind zwar ausser Mode, weil sie Munition brauchen, aber sie ist Rebellin gegen die Deutsche Krone. Und mit denen hatte ich noch nicht zu tun. Ich weiss einfach zu wenig.

Zwölfter Stock. Es ist offensichtlich, wo Anne wohnt. Das Vorhängeschloss an der Eisentüre ist ein sicherer Indikator. Aber Vorhängeschlösser sind einfach zu knacken. Keine Minute später stehe ich in einer recht schmucken Wohnung. Klar, Fensterscheiben sind auch keine mehr da, aber die fehlen beinahe überall. Dafür haben wir mehr als genug Scherben. In der Luft liegt der Geruch von verwirbeltem Staub, der entsteht, wenn Computer zu lange in geschlossenen Räumen laufen. Auch die Temperatur weist darauf hin. Strom. Anne hat's gut. Sogar Luxusgeräte hat sie. Was der Wohnung fehlt ist aber eines: Anne. Sie scheint nicht zu Hause zu sein. Schade. Wobei: Ich glaube kaum, dass sie Fremde in der verschlossenen Wohnung mag. Bevor ich die Küche untersuche, schaue ich mir den Computer an. Windows 8. Uralt. Passwortgeschützt. Das würde einige Zeit dauern. Zeit, die ich nicht habe und das Laptop mitnehmen, kommt auch nicht in Frage. Aber die Festplatte einfach so dazulassen, geht auch nicht. Ein Blick in die Küche: Brot auf dem Tisch, dreckige Teller im Lavabo. Sie scheint sogar fliessend Wasser zu haben. Echt luxuriös. Neben dem Kochherd beginnt das Wasser in einem elektrischen Wasserkocher zu dampfen. Ein Klicken lässt mich wissen, dass das Wasser heiss ist. Nützt mir nichts. Ich gehe wieder, verschliesse die Wohnung und gehe nach Hause.

Mein Zuhause: Ein altes Bürogebäude an der Jakob-Fügli-Strasse. Es ist auch der Grund, warum ich meinen Job habe. Als ich eines Donnerstags auf das verlassene Büro gestossen bin, habe ich vier funktionsfähige Computer und jede Menge Möbel, darunter eine Couch, entdeckt. Und auf dem Dach sind Solarpanel installiert. Der Eingang zum Gebäude ist gut versteckt und vom dritten Stock aus habe ich gute Aussicht. Mittlerweile wohnt auch meine Geschäftspartnerin in den Räumen. Da läuft aber sonst nichts. Ehrlich.

«Und? Wie war's», fragt sie mich. Ich erzähle ihr die Geschichte von Frank und dem Schuss, zeige ihr die Festplatte. Sie schnappt sie sich und startet einen der Computer auf. Sie kann den Daten einfach nicht widerstehen. Das Aufstarten dauert so seine Zeit, denn die alten Maschinen sind auch nicht mehr das, was sie einmal waren. Dann kommt die typische Schweizer Frage:

«Und sonst?»

Ich erzähle ihr von meinem Besuch bei Anne, die nicht zu Hause war. Auf einmal ist der Computer nicht mehr so wichtig.

«Erzähl mir jedes Detail. Sofort.» Gut. So sei es. Code. Zwölfter Stock. Einbruch. Computer. Passwort. Ich erzähle ihr alles. Meine Partnerin schaut mich an. Der Blick alleine sagt mir, dass sie etwas weiss, das ich nicht weiss. Und dass ich einen Fehler gemacht habe.

«Ich weiss genau, wo Anne ist. Auf etwa 60 Quadratmeter genau», höre ich.

«Und kann mir Fräulein Genie auch sagen, wie sie das weiss», frage ich mit sarkastischem Unterton.

«Nein, Herr Hirni, die zwei Gründe kannst du selbst auf dem Weg zu Anne rausfinden.» Woher wusste sie das?

Warum weiss die Mitarbeiterin genau, wo Anne ist? Sie nennt zwei Gründe. Welche sind das?

1. _____

_____

_____

2. _____

_____

_____

Wettbewerb

Mailen Sie uns die zwei Gründe, warum Annes Aufenthaltsort offensichtlich ist, an die Adresse info-at-scip.ch inklusive Ihren Kontakt-Koordinaten.

Das Los entscheidet über die Vergabe des Preises. Teilnahmeberechtigt sind alle ausser den Mitarbeiterinnen und Mitarbeitern der scip AG sowie deren Angehörige. Es wird keine Korrespondenz geführt. Der Rechtsweg ist ausgeschlossen.

Einsendeschluss ist der **15.12.2013**.

Die GewinnerInnen werden nur auf ihren ausdrücklichen Wunsch publiziert. Die scip AG übernimmt keinerlei, wie auch immer geartete Haftung im Zusammenhang mit irgendeinem im Rahmen des Gewinnspiels an eine Person vergebenen Preises.

Gewinnen Sie ein Exemplar des Buches „Die Kunst des Penetration Testing“ von Marc Ruef. Dem meistverkauften deutschsprachigen Penetration Testing Fachbuch auf dem Markt.

http://www.computec.ch/mruef/?s=dkdpt
911 Buchseiten, ISBN 3-936546-49-5

7. Impressum

Herausgeber

scip AG
Jakob-Fügli-Strasse 18
CH-8048 Zürich
T +41 44 404 13 13
info-at-scip.ch
http://www.scip.ch

Zuständige Person

Dominik Bärlocher
Public Relations
T +41 44 404 13 13
doba-at-scip.ch

scip AG ist eine unabhängige Aktiengesellschaft mit Sitz in Zürich. Seit der Gründung im September 2002 fokussiert sich die scip AG auf Dienstleistungen im Bereich Information Security. Unsere Kernkompetenz liegt dabei in der Überprüfung der implementierten Sicherheitsmassnahmen mittels **Penetration Tests** und **Security Audits** und der Sicherstellung zur Nachvollziehbarkeit möglicher Eingriffsversuche und Attacken (**Log-Management** und **Forensische Analysen**). Vor dem Zusammenschluss unseres spezialisierten Teams waren die meisten Mitarbeiter mit der Implementierung von Sicherheitsinfrastrukturen beschäftigen. So verfügen wir über eine Reihe von Zertifizierungen (Solaris, Linux, Checkpoint, ISS, Cisco, Okena, Finjan, Trend-Micro, Symantec etc.), welche den Grundstein für unsere Projekte bilden. Das Grundwissen vervollständigen unsere Mitarbeiter durch ihre ausgeprägten Programmierkenntnisse. Dieses Wissen äussert sich in selbst geschriebenen Routinen zur Ausnutzung gefundener Schwachstellen, dem Coding einer offenen Exploiting- und Scanning Software als auch der Programmierung eines eigenen Log-Management Frameworks. Den kleinsten Teil des Wissens über Penetration Test und Log-Management lernt man jedoch an Schulen – nur jahrelange Erfahrung kann ein lückenloses Aufdecken von Schwachstellen und die Nachvollziehbarkeit von Angriffsversuchen garantieren.

Einem **konstruktiv-kritischen Feedback** gegenüber sind wir nicht abgeneigt. Denn nur durch angeregten Ideenaustausch sind Verbesserungen möglich. Senden Sie Ihr Schreiben an smss-feedback@scip.ch. Das Errata (Verbesserungen, Berichtigungen, Änderungen) der scip monthly Security Summarys finden Sie online. Der Bezug des scip monthly Security Summary ist **kostenlos**. Anmelden! Abmelden!