)SCIP(

06/2014

MONTHLY SECURITY SUMMARY

Cons – Zeitverschwendung?
Kurz vor der Schweizer Security Conference Area41 teilt ein Organisator ein paar Gedanken. > 2

Das gehackte Auto
Steuerung, Bremsen, Anzeige und mehr können an einem Auto bereits manipuliert werden. > 3

Controls Management
In stetig komplexeren IT-Umgebungen ist es wichtig, den Überblick zu wahren. Eine Anleitung. > 6

NEWS

Informationssicherheit in Swiss Engineering

Die Schweizerische technische Zeitschrift Swiss Engineering STZ enthält in der Ausgabe des 5. Mai 2014 einen Beitrag von Dominik Bärlocher. In diesem kommt Marc Ruef zu Wort, der den grundlegenden Ansatz seiner Tätigkeit bei scip AG illustriert. Dabei wird unter anderem auf die aktuelle Bedrohungslage durch Industriespionage und die Möglichkeiten des Social Engineering eingegangen.

Bild: sprachwerk.ch

Das Cover der jüngsten Ausgabe.

Die scip AG an der InfoSec-Konferenz area41

Mit area41 haben die Hashdays einen würdigen Nachfolger gefunden. Am 2. und 3. Juni haben sich 350 Hacker aus 14 Nationen im Zürcher Komplex 457 getroffen. Stefan Friedli hat als Organisator ein Interview gegeben und Marc Ruef trat als Speaker auf und sprach über die Qualitäten einer Verwundbarkeitsdatenbank Zudem hat Radio Ö1 ein Interview geführt. Weiteres zur Convention finden Sie auf Seite 2.

Interview zu Blackshades in 20 Minuten

Nach der Festnahme von 16 Schweizern, denen der Kauf und di Nutzung der Spionagesoftware *Blackshades*, das laut Berichten 500000 Computer infiziert hat, zur Last gelegt wird, äussert sich Marc Ruef in der Zeitung 20 Minuten. Im Interview erläutert er die Funktionsweise und Möglichkeiten der kommerziellen Lösung.

EDITORIAL

Von BlackShades und Helden

Im Zuge der neuesten Bedrohung aus dem Internet sieht sich der InfoSec-Sektor erneut im Rampenlicht. Die Entwicklung ist mit Vorsicht zu geniessen.

Dominik Bärlocher

Es hat nach Heartbleed nicht lange gedauert bis die nächste Schockmeldung, über die internationalen Newsoutlets hereingekommen ist. BlackShades heisst die jüngste digitale Bedrohung. Und laut Medien ist es bereits wieder so weit: Wir müssen alle sterben. Okay, sterben vielleicht nicht grade, aber ganz schlimm ist es sicher. Eine mittlere Katastrophe, mindestens.

Alle sind wir bedroht und jeder kann BlackShades anwenden. Dazu auch ein Telefonat in unser Büro vor Kurzem: «Ich glaube, mein Nachbar spioniert mich mit BlackShades aus. Was kann ich tun», fragt der Anrufer. Er hat Angst. Verständlich, wenn man Nachrichten schaut und bedenkt, was BlackShades so alles können soll. Vor allem aber auch, dass die Software zum Verkauf steht. Oder besser: stand. Denn die Behörden gehen aggressiv gegen BlackShades vor.

Unsere erste Reaktion: Wohl eher nicht. Denn so einfach, wie die Medien das darstellen, ist das Ganze eben nicht. Dem ist meistens so. Genau das sollten wir im InfoSec-Sektor auch zu Herzen nehmen.

Was ist BlackShades?

BlackShades ist ein Trojaner. Laut Berichten kann er allerlei. Ein böser Hacker hat Nacktbilder von Miss Teen USA aufgenommen, mit ihrer eigenen Webcam. Das ist noch längst nicht alles. BlackShades könne noch viel mehr. Das Tool sei ein Keylogger, könne zu Ransomware-Zwecken verwendet werden und eben auch zum Datenklau. Wenn BlackShades läuft, wie das von Statten geht erkläre ich später, kann der Bildschirm, den der Angreifer vor sich sieht, mit dem von TeamViewer verglichen werden. Anders als bei TeamViewer aber muss die Session auf dem ferngesteuerten Computer nicht bestätigt werden.

Hinter dem eingängigen Namen steckt ein *Remote Administration Tool (RAT)*. Ein RAT ist keine neue Erfindung, auch nicht unter Kriminellen. Bereits im Jahre 1998 machte Back Orifice Computer weltweit unsicher. Nur dass damals die Awareness für Computersicherheit in den Medien wie auch den Köpfen der Leser noch nicht so ausgeprägt war. Das trotz der Tatsache, dass Hackers erst drei Jahre zuvor über die Bildschirme geflimmert war. Heute, in einer Welt die zusehends digitaler wird, ist das anders. Darum wohl auch die weitverbreitete Angst.

Bin ich infiziert?

Die kurze Antwort darauf lautet «Wahrscheinlich nicht», denn einfach so, ohne weiteres, wird ein PC nicht so von BlackShades infiziert. Und wer einige grundsätzliche Regeln im Umgang mit dem Internet beachtet, wird wohl kaum infiziert werden. Denn BlackShades benötigt nach wie vor menschliches Zutun. Ein User muss einen Client auf seinem PC ausführen, bevor der Angreifer seine Schandtaten begehen kann.

Daher gilt, wie schon seit Jahren: *Keine unbekannten Applikationen ausführen*. Problem gelöst. Weiter ist das Setup eines BlackShades-Clients für den bösartigen Nachbarn wohl zu komplex, muss ein Angreifer doch die IP und eine ganze Menge anderer Daten über den Computer des Opfers kennen, bevor er überhaupt einen funktionierenden Client generieren kann.

Ausserdem ist die Infektion mit BlackShades statistisch unwahrscheinlich. Die BBC berichtet, dass über 500000 Computer weltweit infiziert sind. Das klingt nach viel. Aber: Die Zahl ist verschwindend klein, nur schon verglichen mit der Anzahl Computer, die in diesem Jahr bereits verkauft worden sind, denn die Zahl liegt etwa bei 115 Millionen zum Zeitpunkt, an dem ich das hier schreibe.

Bleiben wir cool

Jetzt, da wir den Tech-Support für Familie und Freunde aus dem Weg haben, können wir uns fragen, was wir aus dieser Sache lernen. Wir, das sind all jene, die auch nur entfernt mit dem InfoSec-Sektor zu tun haben. Auf einmal sehen wir uns öfter in den Medien. Wir sind auf einmal die Experten für die Sicherheit der digitalen Existenz aller.

Die Medien wollen natürlich immer einen Superlativ in ihren Schlagzeilen. Der böseste Mörder, die schnellste Raser, der schlimmste Hacker. Je übler, desto besser. Computer sind immer gut für so eine Schlagzeile, denn die Zahlen sind in der Regel recht hoch. Eine halbe Million infizierte Rechner. Schlimm. Facebook kauft WhatsApp für Milliarden. Viel. Wir kennen alle die Schlagzeilen. Oft lächeln wir und denken: «Wenn die nur wüssten».

Genau dies können wir tun. Wir können sie wissen lassen. Wenn wir als Experten von Medien gefragt werden, müssen wir nicht zwingend dem Hype helfen, noch grösser zu werden. Denn Journalisten wissen oft auch nicht viel mehr als User. *Genau darum fragen sie ja bei Experten, also uns, nach*. Genau darum können wir die Stimme der Raison sein. Genau darum liegt es an uns, dann einen kühlen Kopf zu wahren, wenn wir gefragt werden und mit stichhaltiger, wahrer und verlässlicher Information aufzuwarten.

Auch sollte uns der neugefundene Ruhm nicht zu Kopfe steigen. Klar, wir können neu im Fernsehen auftreten, dort unsere Informationen auch noch verbreiten. Aber Superstargehabe muss doch nicht sein. Gibt es denn nicht schon genug Leute aus dem IT-Sektor, die sich in den Medien aufbauschen?

NEWS

Interview zu ProtonMail in watson

Der freie Dienst ProtonMail aus Genf verspricht eine abhörsichere Mail-Kommunikation für jedermann. Marc Ruef kommt im Beitrag auf watson zu Wort und gibt Auskunft darüber, welche Angriffsmöglichkeiten dennoch gegeben sein könnten. Zum Schluss bleibt auch hier erforderlich, dass man dem Betreiber des Dienstes vertraut. Denn dieser hat immer die Möglichkeit, volle Einsicht in die Kommunikation erhalten zu können.

Interview zu Darknet in watson

Der am Dienstag durch das Fedpol veröffentlichte Jahresbericht beschreibt, dass illegale Aktivitäten im Web hauptsächlich ins Darknet abwandern. Im umfangreichen Interview für watson gibt Marc Ruef Auskunft darüber, wie dieses strukturiert ist und wie die Ermittlungsarbeit der Behörden aussieht. Dabei werden sowohl technische als ermittlungstaktische Facetten diskutiert.

Vortrag zu Source Code Reviews an Hacking Day

Am von *Digicomp* organisierten Hacking Day hat Marc Ruef einen Vortrag gehalten. Er hat darin die Grundlagen der Source Code Analyse beleuchtet. Er hat einen möglichst praktikablen Ansatz vorgestellt, wie die Sicherheit einer Software durch eine entsprechende Untersuchung bestimmt werden kann.

BLOG DIGEST

Die besten Links aus einem Monat Internet

- A Technical Analysis of CVE-2014-1776 (blog.fortinet.com)
- And the Zodiac Killer is (washingtonpost.com)
- Antivirus pioneer Symantec declares AV 'dead' and 'doomed to failure' (arstechnica.com)
- AVFoundation, how to turn off the shutter sound (stackoverflow.com)
- Burying the URL (allenpike.com)
- CBS Orders 'NCIS', 'CSI' Spinoffs and More to Series (aceshowbiz.com)
- Dirty PowerShell WebServer (obscuresecurity.blogspot.com)
- Disclosing vs. Hoarding Vulnerabilities (schneier.com)
- Facebook App Knows What You're Hearing and Watching (blogs.wsj.com)
- Hacks! An investigation into aimbot dealers, wallhack users (pcgamer.com)
- Heartbleed vs. Heartblead: Why IPS Alone Makes for Poor Security (securityintelligence.com)
- How to get security updates for Windows XP until April 2019 (ghacks.net)
- iOS 7 doesn't encrypt email attachments (zdnet.com)

LABS

Reine Zeitverschwendung?

Security Conferences haben derzeit einen etwas schweren Stand. Einige Gedanken zur Identität einer Con eines Organisators der Konferenz area41.

Stefan Friedli

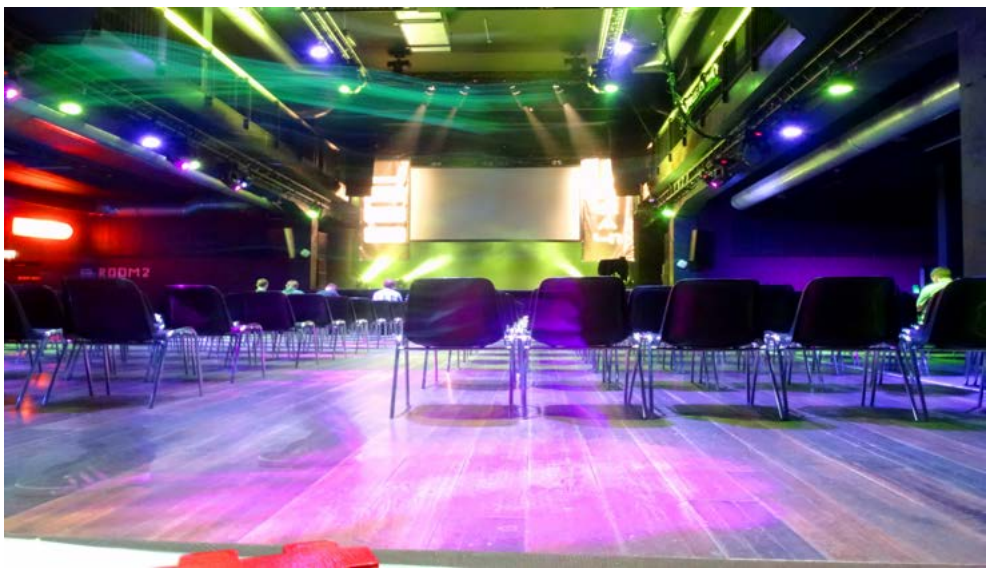


Bild: Adrien Chevalier

Drohen Conventions leere Stühle und verlassene Bühnen?.

Im Jahr 2007 durfte ich eine Veranstaltung besuchen, die bis heute eine der einflussreichsten Erfahrungen blieb, die ich bis dato machen durfte: Das *Chaos Communication Camp* 2007 in Finowfurt. Die Gründe dafür sind vielfältig und nicht ganz einfach zu erklären. Wahrscheinlich war es die Mischung aus dem ehemaligen, zum Museum umfunktionierten, Flughafen auf dem weltbekannte Researcher Vorträge in ehemaligen Bunkern hielten. Gleichzeitig präsentierten ausserhalb Tausende von Bastlern aus aller Welt ihre LED-bestückten Quadcopter, RFID-Gadgets und unzählige andere technische Spielereien, die uns 2007 noch als deutlich futuristischer vorkamen als heute, über ein halbes Dutzend Jahre später.

Das Chaos Communication Camp 2007 war nicht die erste Konferenz die ich besuchte. Schon als Teenager haben mich Events wie der Kongress des CCCs angezogen, die DEFCON in Las Vegas war damals unerreichbar, aber hatte einen einschlägigen Ruf. Auch lokale Events, meistens von Linux User Groups veranstaltet, waren gerngesehene Möglichkeiten zum Austausch, zum Lernen neuer Skills und boten auch eine gewisse Geselligkeit. Auch eine Serie von Invite-Only Konferenzen in Berlin, die ein heute langjähriger Freund organisierte, hat mir enorm dabei geholfen meinen Platz in der Industrie und im Sicherheitsbereich zu finden. Später, nachdem ich meine Position bei der scip AG eingenommen hatte, kamen weitere Konferenzen und Conventions dazu: Die obengenannte DEFCON, die kommerzielle Schwesterkonferenz BlackHat, SOURCE-Konferenzen - viele durfte ich besuchen, an vielen durfte ich selber vortragen. Eine Möglichkeit, die ich als Privileg sehe.

Grosser Aufwand - wofür?

Solche Veranstaltungen waren für mich für lange Zeit, und teilweise sind sie das noch heute, die einzige wirkliche Möglichkeit, in unserem schnelllebigen Bereich effektiv an Informationen und auch Inspiration heranzukommen. Vor einigen Jahren dann, hatte ich die Gelegenheit selber an einer Plattform zu ebendiesem Informationsaustausch mitzuarbeiten. Die damals noch als *hashdays* bekannte Sicherheitskonferenz wurde zu einem bekannten Namen, sogar international. Heute, in 2014, hat die Eventserie den neuen Namen *Area41* angenommen, existiert aber im gleichen Geiste weiter - immer noch mit erfreulich grossem Erfolg.

Ich arbeite heute immer noch an der Organisation der Area41 mit. Der Zeitaufwand, der dabei zu Lasten von Freizeit und Familie anfällt ist gross. Alleine für die Auswahl, Koordination und Betreuung von Referenten, die aus aller Welt anreisen, sind Dutzende von Arbeitsstunden notwendig. Das Organisieren von Sponsoren und Aushandeln von Verträgen gehört vermutlich zu den härtesten Aufgaben, die man in einem Non-Profit Umfeld bewältigen muss. Und die Detailaufgaben, zum Beispiel das Bereitstellen eines Logos, das Onlineschalten von Informationen, das Bezahlen von Bagatellrechnungen, kumulieren sich schnell zu einem überraschend wohlgefüllten Wochenende. Der Aufwand hat sich bis heute aber im Hinblick auf das Endprodukt gelohnt. Trotzdem stehe ich dem Thema Konferenzen heute kritischer gegenüber, als noch vor sieben Jahren - ein Umstand der so manchen überraschen mag.

Wofür sind Konferenzen eigentlich gut? Was nach einer etwas polemischen Fangfrage klingt, ist letzten Endes hochrelevant. Die Beweggründe, die jemanden dazu bringen eine Konferenz zu besuchen sind mannigfaltig. Für die einen ist eine reine Sache des Inhalts: Die Vorträge, die Workshops, die kleinen Kniffe die man von anderen Teilnehmern lernen kann. Für den anderen ist es die geschäftliche Komponente: Ein neuer Job, das Präsentieren als Arbeitgeber oder Servicedienstleister gegenüber potentiellen Interessenten. Noch einmal andere schätzen die rein soziale Komponenten: Mit Gleichgesinnten ein kaltes Bier oder äquivalentes alkoholfreies Getränk geniessen und über Technik und Privates plaudern. Dazu kommen vermutlich sämtliche Kombinationen der vorgängig genannten Szenarien, sowohl zwangsläufig einige, die ich im Rahmen dieses Artikels nun vernachlässige.

Warum also doch?

Heute, im Jahre 2014, leben wir in einer Welt in der Information so verfügbar ist wie niemals zuvor. Die Präsentationen, die heute an einer BSides in den USA gezeigt werden, können morgen in FullHD-Video verfügbar sein. Die Slides, vielleicht sogar Whitepapers mit Hintergrundinformationen sind vermutlich schon online bevor der Speaker überhaupt die Bühne betritt. Nur der Information halber muss heute niemand mehr eine Konferenz besuchen.

Auch die geschäftlichen und sozialen Komponenten sind weniger stark als früher: Heute buhlen dermassen viele Recruiter und HR-Verantwortliche um fähige Mitarbeiter, Jobangebote auf Twitter sind ein durchaus akzeptierter Standard. Kunden findet man an solchen Events so oder so selten, hat die Industrie für die *weniger technischen Entscheidungsträger* doch längst spezialisierte, weniger freakige Sales-Events organisiert. Diese kommen zwar ohne 0-Days aus, dafür aber mit mehr Anzügen und in der Regel mit teureren Apéros. Auch die rein soziale Komponente ist schwächer geworden, seit die InfoSec-Community überraschend positiv auf Twitter reagiert hat und dort sehr repräsentativ vertreten ist.

Man muss sich also schon fragen: Was bringen uns Konferenzen noch? Auch ich, in der Rolle als Organisators, habe mir diese Frage oft gestellt. Die Antwort gefunden habe ich bislang lediglich in den Feedback-Formularen und Anmeldungen für die diesjährige Konferenz: Der Enthusiasmus, etwas mitzuerleben. Nicht On-Demand, als mkv-File oder auf YouTube, sondern vor Ort. Als aktiver Teilnehmer mit der Möglichkeit mitzureden, und Einfluss zu nehmen. Das grosse Potenzial von Sicherheitskonferenzen liegt in ihrer inhärent kollaborativen Natur. Es sind nicht die einzelnen Aspekte, sondern das Ganze, das letzten Endes grösser als die Summe aller Teile, die den Reiz und den Wert dieser Veranstaltungen noch ausmacht.

LABS

Wissenswertes zu Car-Hacking

Mit dem Release von Watch Dogs lebt die These «alles kann gehackt werden» wieder auf. Darunter auch das Hacken von Autos. Researcher haben bereits viel erreicht, doch sie stossen auf Widerstand.

Dominik Bärlocher

Es begann mit einem Videospiel. Ubisoft hat vor kurzem das Spiel *Watch Dogs* veröffentlicht. Der Titel gehört zu den am meisten beworbenen Spielen des Jahres und erzählt die Geschichte des Hackers Aiden Pearce. Dieser will den Tod seiner Nichte rächen und macht im Zuge dieser Racheaktion Gebrauch von seinem Smartphone. Denn damit kann er so ziemlich alles hacken, was im Spiel existiert.

Es wird viel Werbung für das Spiel gemacht. Das Online-Technologie-Magazin Motherboard, das von den selben Leuten geführt wird wie VICE.com, hat eine Doku-Serie gestartet, die direkt mit der Marketingkampagne des Spiels verknüpft ist. Der Ansatz der Serie: *Alles kann gehackt werden*.

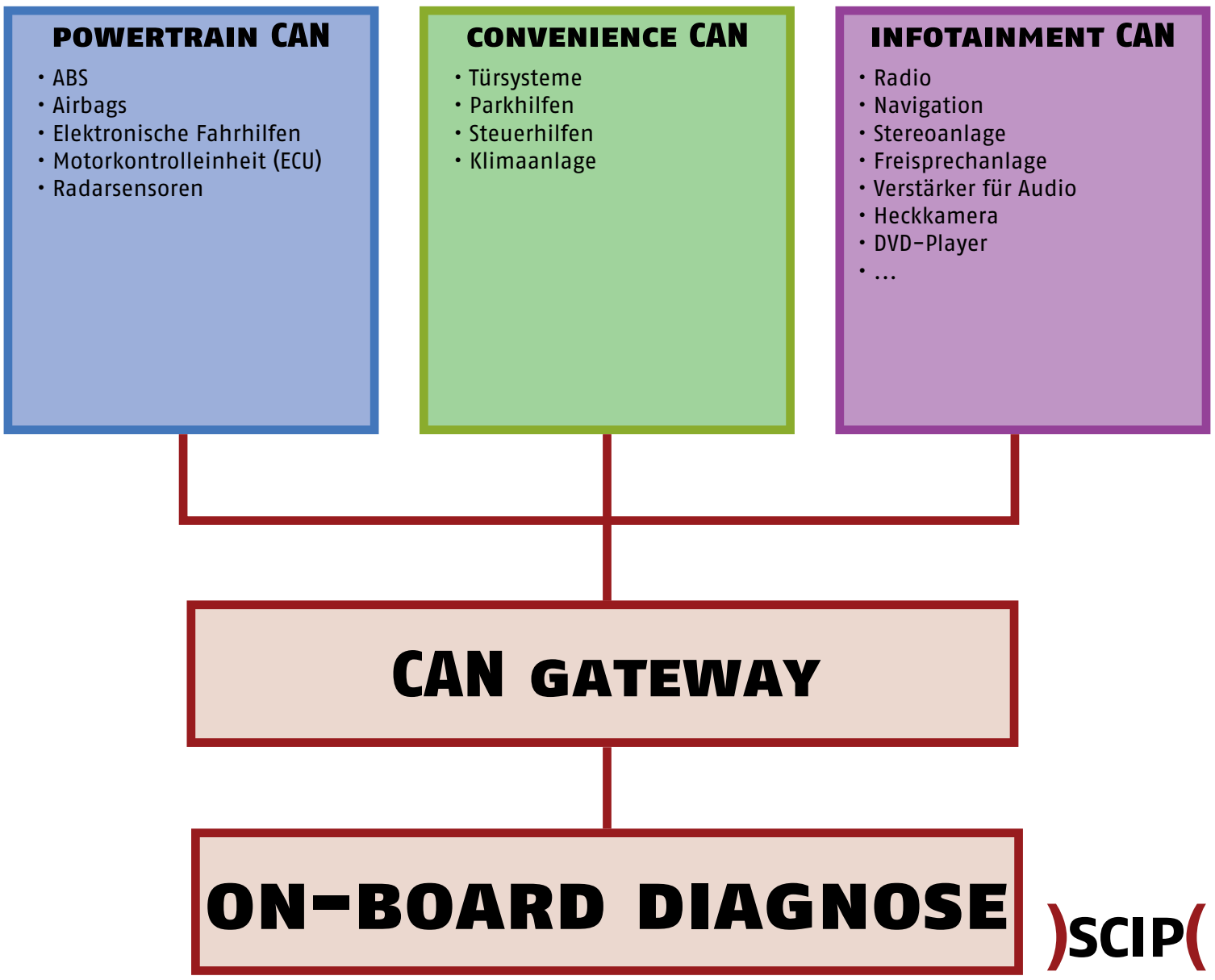
Die Verbreitung der Story

In der jüngsten Episode der Dokuserie vom 29. Mai 2014 ist das Hacken von Autos das Thema. Dieses Thema hat hohe Wellen geschlagen, die nicht nur aufzeigen, dass die Medien einander abschreiben und alle zusammen eine Sache ignorieren: **Car Hacking ist nicht neu.**

Das ist die Folge, die von den Medien aufgegriffen wurde. Weil viele Leute Auto fahren und die meisten Autofahrer haben keine grosse Lust darauf, ihr Auto gehackt zu haben. Denn wenn ein Auto mit Fahrer ausser Kontrolle ist, dann ist der Fahrer in etwa anderthalb Tonnen Stahl, die grade die Strasse runterrasen, eingeschlossen. CNN Money hat die Geschichte aufgegriffen und hat darüber berichtet, dass Autofirmen veralteten Code verwenden, oder sogar gar keine Sicherheitsmassnahmen. Andere hingegen machen wieder viel für die Sicherheit ihrer IT-Systeme im Auto.

Die Geschichte CNNs wurde dann von der Schweizer Zeitung 20 Minuten kopiert und der verlinkte Artikel ist eine recht gute Übersetzung des CNN-Artikels. Einzige Neuerung: Die Zeitung hat Informationen aus einem undatierten Artikel des Deutschen Automagazins Auto Motor und Sport einfliessen lassen.

In dem Artikel wird erstmals erwähnt, dass die News nicht neu ist. Weil wo die aktuelle Spur der Story mit *Watch Dogs* beginnt, ist das Thema Car Hacking allermindestens ein Jahr alt. Die Geschichte ist zudem grösser als nur *Autos können gehackt werden*. Die Geschichte zeigt uns, dass es Hersteller gibt, die aktiv gegen Car-Hacker vorgehen und sogar die Publikation von Research verhindern, die Sicherheitslücken in Autosystemen offenlegen. Doch, es muss an dieser Stelle gesagt werden, dass ein guter Grund vorliegt, der aber hoffentlich nicht zum Präzedenzfall wird.



Grafik: scip nach Felix Domke

Die Grundzüge der Architektur eines Computersystems in einem Auto.

Start ohne Zündschlüssel

Im vergangenen Jahr haben die holländischen Researcher Roel Verdult und Baris Ege von der Radboud University Nijmegen gemeinsam mit Flavio D. Garcia der University of Birmingham einen Talk zusammengestellt, der da Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer hiess. Den Talk wollten sie am 22. Usenix Security Symposium im August 2013 präsentieren. Dazu kam es aber nie.

Megamos Crypto ist ein System, das als *Vehicle Immobilizer* - als Wegfahrsperre - dient. Es ist eine letzte Verteidigungslinie, die es dem Fahrzeug verbietet, zu starten, wenn eine unautorisierte Person ohne den echten Autoschlüssel im Cockpit des Fahrzeugs sitzt und sich an der Zündung zu schaffen macht. Verdult, Ege und Garcia sind in der Lage *einen fortgeschrittenen Autoschlüssel zu fälschen und ein Auto ohne validen Zündschlüssel zu starten*.

Autohersteller geben sich zweifelsohne grosse Mühe, den Diebstahl ihrer Fahrzeuge zu verhindern, was durch die Existenz von Systemen wie Megamos Crypto erwiesen ist. Megamos Crypto scheint, so weit feststellbar, eine simple Single-Factor Authentication zu sein, die auf der Interaktion von Maschinen beruht. Das Auto kommuniziert mit dem Schlüssel und zeigt ihm einen `Key Value`, woraufhin der Schlüssel den `Proof Key` sendet. Nur dann erlaubt das Auto den Start des Motors. Der Fahrer bemerkt von dem Vorgang nichts, da er kabellos und in sekundenschnelle passiert.

Die genauen Mechanismen von Megamos Crypto scheinen aber nach wie vor geheim zu sein, worauf wir gleich zu sprechen kommen. Wie dem auch sei, die Researcher vergleichen die Komplexität und die Praktikabilität des Angriffs mit dem Angriff auf ein mit Hitag2 gesichertes Auto. Details, wie das genau funktioniert, können dem Talk zum Thema entnommen werden. Die Haken:

- Ein Angriff kann nur dann ausgeführt werden, wenn der Angreifer auf etwa fünf Zentimeter an den Originalschlüssel herankommt.
- Währen einer Attacke muss das System des Angreifers mit dem Originalschlüssel kommuniziert haben.
- Ein Angreifer muss immer noch alle anderen Sicherheitsvorkehrungen am Auto, wie Alarmanlage und das Türschloss, umgehen.
- Der Angreifer muss nach wie vor die Zündung des Fahrzeugs kurzschliessen.

Die Researcher geben freilich zu, dass ihre Methode nicht sehr praktikabel ist. Kurz: Ihr Ansatz ist nur in der Lage, die elektronische Wegfahrsperre zu umgehen. Alle anderen Sicherheitsmassnahmen bleiben unangetastet.

Megamos Crypto ist zudem veraltet und wird in manch einem Luxusauto verwendet. Unter anderem sind die Marken Audi, Porsche, Bentley und Lamborghini betroffen.

Der Gerichtsfall

Als verantwortungsbewusste Researcher haben Verdult, Ege und Garcia alle Involvierten über ihre Funde informiert. Die Hersteller waren wohl

nicht direkt darüber erfreut, dass ihre 96bit-Verschlüsselung nicht mehr so sicher ist, wie Tags zuvor, und dass jemand mit einem Stein, einem Schraubenzieher und einem gut ausgerüsteten Computer ein Auto mit Megamos Crypto stehlen kann.

Volkswagen hat die Researcher verklagt, mit dem Resultat, dass Verdult, Ege und Garcia ihre Erkenntnisse nicht vortragen dürfen. Dies hat der London High Court unter der Leitung von Richter Birss beschlossen.

Das Gericht hat aber erkannt, dass das Urteil als ein Angriff auf die Redefreiheit, die Verhinderung von akademischem Fortschritt und die Wahrung von rein finanziellen Interessen angesehen werden kann. Auf diese Bedenken ging Richter Birss mit folgendem Argument ein:

> Ich anerkenne den hohen Wert der akademischen Redefreiheit, aber ich sehe auch einen weiteren hohen Wert: Die Sicherheit von Millionen von Volkswagen-Fahrzeugen.

Daher sind Millionen von Fahrzeugen nach wie vor mit verwundbarem Code ausgerüstet. Volkswagen hat im vergangenen Jahr keinerlei Ankündigungen über eine allfällige Änderung ihre Kryptographie oder die Verbesserung ihres Codes gemacht.

Trotz dem Urteil hat Verdult den Talk an der Usenix-Convention abgehalten, wenn auch in zensierter Form.

Das Computersystem eines Autos

Alle modernen Autos sind im Grunde genommen gleich aufgebaut, wenn es um die Computersysteme an Bord des Fahrzeugs geht. Genaue Spezifikationen unterscheiden sich von Modell zu Modell, von Generation zu Generation. Generell kann aber festgehalten werden, dass ein gewisser gemeinsamer Grundsatz in allen Fahrzeugen vorhanden ist, der auf dem System den *Controller Area Network Bus* (CAN Bus) beruht. Dieser wurde im Jahre 1983 entwickelt und vereint seither die Kabel in einem Auto. Seither sind viele Versionen auf den Markt gekommen, die aber allesamt auf der von Bosch entwickelten Version beruhen. Denn vor 1983 wurden bis zu zwei Kilometer Kabel in einem Auto verbaut.

Im Rahmen der CAN Bus Architektur sind die Systeme des Autos in Zonen aufgeteilt. Auch hier gilt: Die Anzahl und der exakte Aufbau der Zonen variiert von Fahrzeug zu Fahrzeug.

Diese Zonen sollten untereinander keinerlei Kommunikation haben. Sprich, wenn ein Angreifer in der Lage ist, mit dem Infotainment CAN - das aktuell wohl als das einfachste Ziel gilt, da es schon grundlegend auf Kommunikation mit externen Geräten ausgelegt ist - zu kommunizieren, sollte es ihm nicht möglich sein, Signale vom Powertrain CAN oder dem Convenience CAN abzufangen oder Signale an diese zwei CANs zu senden. Sollte ein Angreifer in der Lage sein, mit einem der beiden anderen CANs zu kommunizieren, so sollte er nicht auf das Infotainment CAN zugreifen können.

Alle diese CANs greifen über ein CAN Gateway auf die On-Board Diagnose Systeme (OBD-II) zu, wo die Daten von Fahrzeug und Fahrt analysiert und interpretiert werden.

Trotz dieser Vorkehrungen zur Verhinderung der Kommunikation der CANs ist es erwiesen, dass auf alle drei CANs zugegriffen werden kann. Signal Injection und Hijacking ist möglich. Was aber bis anhin noch nicht möglich ist, ist der Angriff aus der Ferne und schon gar nicht ohne vorherigen Zugang zum Cockpit des Fahrzeugs. Denn die meisten, wenn nicht sogar alle CAN Buses werden in der Fahrgastzelle des Fahrzeugs untergebracht. Ohne weiteres kann nur von dort aus auf den CAN Bus zugegriffen werden.

Es ist noch kein Fall von Remote Exploitation - dem Eingriff in die Systeme des Fahrzeugs mit kabelloser Verbindung zum Auto - mit vorherigem physischen Zugriff auf den CAN Bus bekannt. Doch die Möglichkeit dürfte gegeben sein. Die spanischen Researcher Alberto Garcia Illera und Javier Vazquez Vidal haben einen Prototypen eines Geräts vorgestellt das nach der Verbindung mit einem Fahrzeug eine Vielzahl der Funktionen des Autos beeinflussen kann. Es sollte möglich sein, dieses Gerät - *Car Hacking Tool* (CHT) genannt - mit einem 3G-Modul zu versehen, was dann die Remote Exploitation möglich macht.

Ein Auto in Echt hacken

Jenseits der Zündung eines Autos gibt es eine grosse Anzahl computergesteuerte Systeme und Sensoren, die gehackt werden können und gehackt worden sind. Als Experten in diesem Feld gelten Chris Valasek und Charlie Miller. Die beiden Amerikaner haben erfolgreiche Angriffe auf die Lenkung, die Bremsen und die Beschleunigung wie auch die Displays eines Autos ausgeführt.

Während den Tests haben Valasek und Miller zwei Autos mit Jahrgang 2010 verwendet. Einen Ford Escape und einen Toyota Prius. Sie haben ihren eigenen Connector gebaut, um mit den Fahrzeugen kommunizieren zu können und benötigten stets eine Kabelverbindung zum Fahrzeug, damit ihre Hacks funktionieren können.

Trotz all der Bastelei und dem Kabelsalat, ist es den Tüftlern Valasek und Miller gelungen, beliebige Werte auf dem Tachometer anzeigen zu lassen und andere Anzeigen, die manuell aussehen, wie die Tempoanzeige oder den Umdrehungsmesser, zu beeinflussen.

Unter anderem gelang es den beiden, auf dem Tachometer eine Geschwindigkeit von 199 Meilen pro Stunde (etwa 320 Kilometer pro Stunde) anzuzeigen - während das Auto stillstand.

Zudem haben sie es geschafft, das System des Autos vollständig zu überlasten, was sämtliche Lenkhilfen, wie die Servolenkung, deaktiviert hat.

> Beim Ford ist es uns gelungen, die ECU zum Absturz zu bringen. Dadurch sind sämtliche Steuerhilfen ausgefallen. Das Lenkrad ist dann nur schwer beweglich und kann nicht weiter als 45% gedreht werden, egal wie sehr der Fahrer das versucht. Das bedeutet, dass ein angegriffenes Fahrzeug keine engen Kurven mehr fahren sondern nur noch weite Bögen machen kann.

Die zwei sind zwar in der Lage, die Lenkung des Fahrzeugs zu beeinflussen, aber praktische Nutzen jenseits des herbeigeführten Unfalls sind keine bekannt. Soweit ist es Valasek und Miller nicht möglich, ein Auto komplett fernzusteuern.

> Indem wir ungültige Geschwindigkeitsangaben über ein Ecom-Kabel und Lenkwinkel- wie auch Angaben zum eingelegten Gang über ein zweites Kabel ans Auto gesendet haben, waren wir in der Lage, das Lenkrad bei jeder Geschwindigkeit zu beeinflussen. Die Präzision unserer Lenkmanöver ist aber nicht mit der des Parkleitsystems zu vergleichen. Es handelt sich bei unseren Manövern um ruckartige, starke Bewegungen des Lenkrads, was die Stabilität des Autos bei jeder Geschwindigkeit beeinflusst aber nicht zur Fernsteuerung des Autos geeignet ist.

Zudem ist es den beiden gelungen, den Fahrer direkt physisch anzugreifen. Valasek und Miller sind in der Lage, den Diagnose-Modus des Autos anzusteuern und die automatische Anspannung des Sicherheitsgurts auszulösen, die dazu gedacht ist, den Fahrer in den Sitz zurückzuziehen, wenn das Auto in einen Unfall verwickelt ist.

Das ist noch lange nicht alles, was Valasek und Miller mit den zwei Fahrzeugen angestellt haben. Eine komplette Liste der Car Hacks ist im Link oben auffindbar. Nach vielen Experimenten sind die zwei Researcher sind zum folgenden Schluss gekommen:

> Autos sind mit physischer Sicherheit als Grundgedanke designt worden. Doch physische Sicherheit kann ohne Datensicherheit nicht erreicht werden. Wenn ein Angreifer (oder auch nur eine korrupte Elektronische Kontrolleinheit) Daten ans CAN senden kann, kann das die Sicherheit des Fahrzeugs beeinflussen.

Die Grenzen des Car Hackings

Hacker hören selten bis nie damit auf, etwas nur leicht zu beeinflussen. Sie versuchen stets, die Grenzen zu erreichen und diese zu überschreiten.

Im vergangenen Dezember hat Felix Domke alias tmbinc es geschafft, eigenen Code auf seinem Fahrzeug auszuführen. Dazu hat er Python in sein Auto integriert (Das Zertifikat der Website ist mit Absicht seitens des Chaos Computer Clubs ungültig.)

Um das zu erreichen hat er die Systeme des Fahrzeugs über das Bluetooth Kit angesteuert, um sich ins zentrale System des Armaturenbretts zu hacken, das mit der selben Technologie wie die Fahrzeuge von Valasek und Miller läuft. Er hat in der Folge entdeckt, dass sein Auto *auf Linux läuft* und in der Folge Python installiert.

So weit bekannt ist, hat Domke nichts weiter mit dieser Erkenntnis gemacht, aber die Möglichkeit, eigenen Code in ein Fahrzeug zu injizieren und eigene Software im Auto auszuführen, eröffnet viele Möglichkeiten.

Fazit

Jedes System eines modernen Fahrzeugs kann mit relativer Leichtigkeit kompromittiert werden. Doch die Angriffe sind noch nicht weit ausgereift. Die Angriffe auf Lenkung, Bremsen, Airbags und Displays können noch nicht aus der Distanz ausgeführt werden.

Das bedeutet aber nicht, dass ein Angriff von ausserhalb des Autos unmöglich ist. Es ist theoretisch möglich, ein Gerät namens Car Hacking Tool mit einem 3G-Modul zu ergänzen und es so für Angriffe aus der Ferne zu verwenden.

Um ein Auto zu hacken, muss ein Angreifer zuerst Zugang zur Fahrgastzelle des Autos haben, über mechanische wie auf informatische Kenntnisse verfügen, die weit über ein End-User-Wissen hinausgehen und dazu noch einen Satz gutes Werkzeug bei sich tragen.

Videos, die Car-Hacking in Aktion zeigen, finden Sie auf scip.ch

IMPRESSUM

Redaktion:
scip AG, Jakob-Fügli-Strasse 18, 8048 Zürich
Telefon: +41 44 404 13 13
Fax: +41 44 404 13 14
E-Mail: info@scip.ch

Redaktor: Dominik Bärlocher

Autoren: Andrea Covello, Stefan Friedli, Rocco Gagliardi, Flavio Gerbino, Oliver Kunz, Marc Ruef, Michael Schneider, Simon Zumstein

Das scip Monthly Security Summary erscheint monatlich.

Anmeldung: smss-subscribe@scip.ch

Abmeldung: smss-unsubscribe@scip.ch

LABS

Virtuelles Security Testing

Unter Zeitdruck einen Sicherheitstest durchzuführen ist schwierig, wenn die eigenen Qualitätsansprüche hoch sind. Schwierig heisst aber nicht unmöglich. Ein Programm macht das einfach: Vagrant.

Andrea Covello

Endlich! Meine Configuration Files, nach denen ich schon vor Wochen gefragt habe, sind hier. Ich freue mich riesig. Aber die Freude über die Dateien hält nur gerade ein paar Minuten an. Höchstens ein paar Minuten. Weil die Engineers behaupten jetzt auf einmal, dass die Einstellungen der Config Files den Sicherheitsanforderungen genügen und der PMO macht Druck. Ich soll die Sache schnellstmöglich validieren und dann noch schneller die ganze Sache als ISEC Compliant abhaken.

Nach einem ersten Blick auf die Files bin ich nicht amüsiert... Okay, ja, sieht so aus, als ob die minimalen ISEC-Anforderungen erfüllt sind. Aber eben: Sieht nur so aus. Etwas fällt mir ins Auge. Ich erkenne das Konstrukt, klar. Aber die Sache hat einen Haken: Sie läuft auf einer anderen Linux Distro als die, die ich bevorzuge. Ich mag ja Debian, aber das hier ist RHE. Und überhaupt: In meinem Job ist "sieht so aus" schlicht nicht gut genug. Ich muss - und wenn ich ehrlich bin, dann will ich das auch - so genau wie möglich sein können, wenn ich eine Sache als ISEC compliant deklariere.

Demnach ist es für mich von Wichtigkeit, dass ich die Konfiguration auf einem laufenden System testen kann. Das ist der Moment, an dem es mir auffällt. Das Gesicht des Managers. Die Nachricht über meinen Plan erfreut ihn gar nicht. Mir kommt auf Anhieb gerade keine Situation in den Sinn, in der er noch weniger erfreut war.

Versteht mich jetzt bitte nicht falsch. Ich weiss genau, was er meint. Ich verstehe sein Problem. Er hat eine Deadline. Ich habe eine Deadline. Das Projekt muss so schnell wie möglich fertig werden, damit wir uns anderen Projekten widmen können.

Daher ist Erfindungsgeist gefragt. Die Situation: Ich bin beim Kunden vor Ort. Ich habe nur grade mein heiss geliebtes MacBook bei mir, das zwar eine Virtualisierungsarchitektur bereit hält, aber sonst nichts. Alles in allem könnte ich schlechter auf den Test vorbereitet sein. Doch mein Hauptproblem ist immer noch da: Der Manager, der wirklich nichts von wegen "Ich brauche einen Tag, um das zu testen" hören will. Weil, wenn ich das sage, dann seufzt er, fragt, ob ich das nicht schneller machen könne, dann muss ich ihm sagen, dass Qualität halt nun mal seine Zeit braucht und dass man sowas nicht abkürzen sollte. Blöde Situation, das.

Moment Mal! Ich kann das abkürzen. Ich erkläre später, was ich tue. Aber, lieber Leser, vertrau mir schnell.

Weisser Text jagt über einen schwarzen Bildschirm und rund 180 Zeilen später bin ich fertig. Was passiert, kann hier nachgelesen werden.

Meine Tricks

Die Tools, die ich verwendet habe, sind die folgenden.

1. Vagrant
2. VirtualBox

Ich gehe mal davon aus, dass ich VirtualBox nicht gross erklären muss. Daher schauen wir uns Vagrant genauer an.

Bei Vagrant handelt es sich um ein Tool, das nicht nur auf MacOSX sondern auch auf Windows und Linux läuft. Es ist kompatibel mit einer Vielzahl von Virtualisierungsmöglichkeiten, wie VirtualBox, VMware Fusion, VMware Workstation, Hyper-V und AWS.

Auf der Website des Herstellers gibt es eine kurze Erklärung, was Vagrant eigentlich ist.

bq. Vagrant stellt eine einfache, reproduzierbare und portable Arbeitsumgebung zur Verfügung, die nach höchsten Industrie-Standards gebaut ist und von einem einzelnen, konsistenten Workflow kontrolliert wird. So wird die Produktivität und Flexibilität von Ihnen und Ihrem Team maximiert.

Damit Vagrant das alles kann, muss es sich auf die Schultern von Riesen stellen. Virtual Machines sind auf VirtualBox provisioniert. Oder auf VMware, AWS oder einem beliebigen anderen Provider. In der Folge können dann die Standardprovisionierungstools wie Shell Scripts, Chef oder Puppet eingesetzt werden, um Software auf der Virtual Machine zu installieren und sie zu konfigurieren.

Aber zurück zu meinem Test, der glücklicherweise keinen ganzen Tag in Anspruch nimmt: Alles, was ich dazu brauche ist Vagrant 1.6.3 und VirtualBox 4.3.12. Die sind bereits auf meinem MacBook installiert. Dazu benötige ich nur noch einen Internetanschluss, damit ich die veröffentlichte VM runterladen kann. In Vagrant werden die übrigens Boxes genannt. Und auch das hatte ich.

Die ganze Sache nahm weniger als 15 Minuten in Anspruch. Jeder, der bereits eine solche Erfahrung gemacht hat, weiss, wie lange das sonst dauert. Und wenn nicht: Im Normalfall kann das locker etwa einen halben Tag in Anspruch nehmen.

Schauen wir uns also die Schritte genau an:

1. Erstellen wir unseren Spielplatz in einem Subordner.
2. Der Befehl `vagrant init` initialisiert den VM Container und definiert, wie die Box namens `chef/centos-6.5` runtergeladen wird. Es gibt eine Vielzahl von Containern, die kostenlos und nach Registrierung in der Vagrant Cloud erhältlich sind. Und weitere gibt es hier:

Es gibt zudem die Möglichkeit, eine eigene Box zu veröffentlichen. Dies geht mit einem kostenlosen Accounts.

Mehr Tricks.

1. `vagrant up` wird Folgendes ausführen:
   - Download der Virtual Disk in den lokalen Speicher
   - Konfiguration der VirtualBox VM Instanz
   - Start der Virtual Machine
   - Start der VM
   - Erstellung des Users `vagrant`
   - Konfiguration für SSH Key Authentication mit der lokalen Maschine
   - Konfiguration von Local Port Forwarding auf TCP/2222 um mit dem VM SSH-Daemon zu verbinden, denn die Maschine ist hinter einer NAT-Konfiguration
   - Erstellung eines freigegebenen Ordners zwischen der neuen VM und der lokalen Maschine
2. `vagrant ssh` erlaubt es uns, mit einem unprivilegierten Benutzer namens `vagrant` anzumelden. Wenn wir Privilegien wollen, dann müssen wir `sudo` verwenden.
3. Jetzt müssen wir das System so einstellen, dass wir es zu unseren Testzwecken brauchen können. Dazu benötigen wir den SNMP-Daemon (`net-snmp.x86_64`)
4. Zeit, die Konfigurationsdateien auf die Virtual Machine zu bringen. Dazu kopieren wir die erhaltene `snmpd.conf` in den Ordner, wo wir die Vagrant Box installiert haben (`tmp-rh-65-instance-01`)
5. Der Ordner synchronisiert sich in der VM im Ordner `/vagrant`
6. Überschreiben wir nun die bestehende Datei mit der synchronisierten SNMP-Konfiguration und starten den Service neu im privilegierten Modus mit `sudo`.

Erfolg! Ich hatte Recht. Die Konfiguration hat zwei Fehler auf den Zeilen 464 und 465. Ich kann weiterhin behaupten, dass ich keine Konfigurationsfile absegne, die ich nicht vorher getestet und auf ihre Funktionstauglichkeit geprüft habe. Zudem bin ich nicht der, der einfach so Dinge ISEC-compliant nennt.

Meine Arbeit ist erledigt und alle sind beeindruckt. Zeit, mein MacBook wieder zurückzusetzen. Weil, seien wir mal ehrlich, 256 GB SSD reicht einfach nirgends hin. Daher: `sudo halt` und das System stoppt.

LABS

Virtuelles Testen (Fortsetzung)

Zurück in der MacOSX-Konsole kann ich nun die Daten einfach entfernen und zwar mit `vagrant destroy`. Was bleibt ist die `snmpd.conf` Datei und die kann ich natürlich auch löschen.

Fazit

Dieses kleine Beispiel kratzt nur an der Oberfläche des Vagrant-Frameworks. Sie können es auch für die Erstellung von komplexen Umgebungen mit mehreren Hosts und sogar für provisionierte Application Frameworks mit Puppet, CFEngine oder gar Shell Scripts nutzen.

Stellen Sie sich ein Vagrant-Framework vor, das dazu da ist, die Sicherheit von Webapplikationen zu testen. Es startet in Minuten und kann genau auf die Bedürfnisse des Testers abgestimmt werden. Und das mit minimalem Aufwand.

Zuguterletzt: Die erstellte virtuelle Umgebung kann geteilt werden Oder Sie können es auch auf ihrem eigenen Web Server speichern oder auch nur den Vagrant Client verwenden, der sich mit einem Server verbindet, der wiederum alle Ihre Maschinen hostet und ausführt. Remotely. Viele Vagrant Boxes sind bereits öffentlich und das sollte Ihre Arbeit erleichtern... weil Zeit ist immer noch wertvoller als Gold.

Dieser Artikel wurde aus dem Englischen übersetzt. Das Original, ebenfalls von Andrea Covello, finden Sie auf www.scip.ch.

BLOG DIGEST

Die besten Links aus einem Monat Internet

- Lua Web Application Security Vulnerabilities (seclists.org)
- Mobile App Security Essentials: 4 Ways to Protect My Apps (securityintelligence.com)
- mXSS (thespanner.co.uk)
- So You Like Pain and Vulnerability Management? (tripwire.com)
- The 'Cobra Effect'that is disabling paste on password fields (troyhunt.com)
- The Subway Line 8 - Exploitation of Windows 8 Metro Style Apps (blackhat.com)

LABS

Controls Management

Die Welt der IT wird stets komplexer. Damit der Überblick, die Ordnung und die Integrität gewährt wird, hilft ein IT Generals Controls Manual.

Flavio Gerbino

Das Konzept von *IT General Controls* (ITGC) wird in Unternehmen und Organisationen zusehends wichtiger. Die stets zunehmenden Regulationen in der IT und der Bedarf an einer effektiven sowie effizienten IT Governance zeigt an, dass Organisationen sehr an einer solchen interessiert sind und die vollständige Kontrolle über die Kontrollen über ihre gesamte Organisation haben wollen.

Mit Hilfe von gut etablierten IGCs kann eine Organisation viele komplexe Themen unter einen Hut bringen, darunter Informations- und IT-Sicherheit, interne und externe Audits, IT-Compliance, Risikomanagement und IT-Governance Management.

ITGCs bestehen aus Prozeduren und Policies, die folgendes bieten:

- Die Informationstechnologie in einer Organisation operiert so, wie vorgesehen.
- Die Daten sind verlässlich
- Die Organisation hält sich an Gesetze und andere Vorgaben.

Dieser Artikel wird versuchen, einen kurzen Überblick über die *wichtigsten Punkte in der Handhabung von ITGCs* zu geben. Darin enthalten sind die organisatorischen Aspekte wie auch deren Struktur und deren Handling.

Einleitung und Definition

Ein umfassendes *IT General Control Manual* (ITGCM) als eine Art Policy sollte die Standards für die Implementation effektiver und effizienter Kontrollsysteme definieren.

Das ITGCM bietet einen Referenzrahmen für eine Organisation, die *Control Procedures* und *Policies* in ihrem Verantwortungsbereich implementiert oder diese implementieren will:

- Interne Audit Perform Reviews
- Compliance- und Monitoringfunktionen können die Effektivität der ITGC evaluieren und rapportieren.

Die Tragweite des *ITGCM* beinhaltet eine Vielzahl organisationaler Aktivitäten, die mit dem Management von IT-Systemen und anderen Information Assets, darunter auch Non-IT-Assets, zusammenhängen. Darunter sind die Folgenden:

- Logische Zugriffskontrollen über die Infrastruktur, Applikationen und Daten
- Systementwicklungs- und Lebenzeitskontrolle
- Physische Zugriffsbeschränkungen zum Datencenter
- Backup- und Recoverykontrollen für System und Daten
- Nutzungskontrollen für Computer.

Daher sollte die Implementation eines ITGCM über die gesamte Organisation hinweg Pflicht sein.

Abweichungen vom ITGCM sollten nur als Ausnahme und nur nach einer eingehenden Untersuchung eines entsprechenden Requests stattfinden. Dies auch nur dann, wenn vorher ein Standardprozess für Ausnahmen definiert worden ist.

Das ITGCM besteht aus:

- Einer Matrix oder einer Liste mit ITGCs, die alle Pflichtkontrollen definieren. Dies ist der Hauptteil dieses Labs und wird weiter unten beschrieben.
- ITGC Assessment Prozess
- ITGC Rollen und Verantwortungen

Das bedeutet, dass das ITGCM die Standards für ein effektives und effizientes IT Governance Management Control System bildet.

Natürlich ist das Management verantwortlich dafür, sicherzustellen dass die ITGCs implementiert, dokumentiert, getestet und für das generelle ITGCM mit Beweise belegt sind.

ITGC Matrix

Die ITGC Matrix ist das Schlüsselelement, das alle anwendbaren Controls definiert und weitere Informationen enthält, die für die Implementation, das Testing und das Assessment der Controls genutzt werden können.

Ihr Zweck:

- Definition der Control Objectives und der Anforderungen
- Leitfaden für die Implementation der Control Procedures und Policies
- Leitfaden für das Assessment der Prozeduren und Policies.

Eine ITGC Matrix sollte dreierlei Informationen in sich integrieren:

- Klassifizierung der Assets und Kategorisierung der Information
- Control Objectives und Anforderungen
- Control Assessment Criteria

Die ITGCs können unterschiedlich strukturiert werden. Die Tabelle «Typische Activity Sets» zeigt ein typisches individuelles Set von Activity Domains und das Set, das vom Institute of Internal Auditors empfohlen wird:

Ein IT Governance Team sollte dafür verantwortlich sein, die Controls mittels Zielen und Anforderungen für jede einzelne Control zu definieren. Diese werden dann für Reviews vom Internen Audit-Team als Teil der Audit-Kriterien genutzt.

Die Implementation der ITGC Matrix ist Pflicht für die gesamte Organisation.

Diese Prozeduren und Policies sollten dazu designt sein, ein gesundes Mass an Sicherheit zu bieten. Vor allem dann, wenn es um das Erreichen der Control Ziele geht. Diese sind:

- Effektivität und Effizienz der gesamten Information Management Operations.
- Verlässlichkeit von Information Assets.
- Compliance mit den Gesetzen, Regulierungen und geschäftlichen Anforderungen.

GUIDELINES

Typische Activity Sets

Typisches Set	Global Technology Audit Guide *
IT Business Continuity	GTAG 1: Information Technology Controls
Backup Management	GTAG 2: Change and Patch Management Controls: Critical for Organizational Success
Change Management	GTAG 3: Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment
Configuration Management	GTAG 4: Management of IT Auditing
Information Management Organization and Processes	GTAG 5: Managing and Auditing Privacy Risks
Incident / Problem Management	GTAG 6: Managing and Auditing IT Vulnerabilities
IT Organization	GTAG 7: Information Technology Outsourcing
IT Operations	GTAG 8: Auditing Application Controls
Project Management	GTAG 9: Identity and Access Management
Physical Security	GTAG 10: Business Continuity Management
Risk Management	GTAG 11: Developing the IT Audit Plan
Service Provider Management	GTAG 12: Auditing IT Projects
System and Information Security	GTAG 13: Fraud Prevention and Detection in the Automated World
	GTAG 14: Auditing User-developed Applications
	GTAG 15: Information Security Governance
	GTAG 16: Data Analysis Technologies
	GTAG 17: Auditing IT Governance

* Der Global Technology Audit Guide (GTAG) wird vom Institute of Internal Auditors herausgegeben.

Updates der Matrix sollten nur als Folge eines strikt geregelten Prozesses passieren. Change Management und Abweichungen sollen nur durch die Einhaltung der bereits bestimmten Standards geschehen

Die Parameter in der Tabelle «Parameter der Matrix» der ITGC Matrix, mit möglichen Werten, oder ähnliche können dazu genutzt werden, die Information Assets zu klassifizieren und zu kategorisieren und die Liste der darauf passenden Controls für diese Assets zu identifizieren.

Jede ITGC kann auf eine oder mehrere dieser vordefinierten Asset Kategorien und Klassifikationen mit einem Indikator - *Applicable* oder *Not Applicable* - gemappt werden.

ITGC Objectives und damit verbundenen Anforderungen für die Implementation der Controls - zum Beispiel die Control Activities, inklusive der möglichen Validationsschritte und den empfohlenen Beweisführungen - sind für jede Control in der Matrix definiert.

Das Assessment der Controls sollte folglich die folgenden Reife-Parameter nutzen:

- Reife
    1. Optimierend
    2. Gesteuert
    3. Definiert
    4. Wiederholbar
    5. Beginnnend
- Detaillierte Beschreibung der echten lokalen Control Procedures und Policies, die für die Control-Ziele relevant sind.
- Remediation (diese können Teil des Risk Management Prozesses sein):
    - Aktionsplan oder Rechtfertigung (basierend auf einem Risk Assessment)
    - Name des Verantwortlichen, Deadline
    - Aktueller Status

Diese Standard-Parameter der ITGC Matrix müssen zwingend verwendet werden, um die Resultate des Control Assessment zu dokumentieren, die Resultate deren Tests zu dokumentieren und um den Fortschritt der Control Gap Remediation (im Risk Management Prozess enthalten) zu dokumentieren.

Das ITGC Manual bietet eine Baseline für das Interne Audit Department um die IT-Aktivitäten zu auditieren. Aber die Tragweite eines internen Audits ist nicht auf diese Baseline limitiert und kann auch Nicht-IT- und Nicht-Governance-Aktivitäten enthalten.

Ein Audit und Compliance Committee der Direktion kann die gefundenen Probleme der externen Auditors reviewen.

ROLLEN UND VERANTWORTUNG

Simple Klarheit

Wer ist verantwortlich?	Was stellen sie sicher?
Governance	Besitz des IT Policy Frameworks, inklusive Policies, Direktionen, Standards und Prozesse. Insbesondere aber das ITGCM, das die Standards des internen Informationsmanagements etabliert
	Die Erhaltung von Zustimmung seitens Audit-, Governance- und Policy-schaffenden Gruppen in der Organisation betreffend der Inhalte und der Nutzung des ITGCM.
	Unterstützung der Implementation des ITGCMs
	Bereitstellen von ITGCM Trainingsmaterial wenn nötig
	Durchführung von Checks der Asset Klassifikationen, Control Assessments, Tests der Controls, Risk Assessments und Mitigationsplänen zur Sicherstellung eines ausgeglichenen Approaches über die Organisation
	Review und Approval von Ausnahmen
	Konsolidierung und Reporting des Control Status
Internes Audit	Assessment des Designs und der Effizienz der Controls
	Reporting ans Management
	Reporting ans Audit und Compliance Committee der Direktion
	Review der Effektivität, Effizienz und Eignung des Information Management Prozesses wie auch der Controls mit Fokus auf • Verlässlichkeit des Information Management Prozesses • Festhalten an Group Policies und der Anforderungen • Schutz der Information Assets
Externes Audit	• Meinung zu den Controls • Review der Dokumentation des ITGCMs als Unterstützung ihres Assessments der Organisation. • Review der Beweisführung in der Dokumentation der Control Procedures und Policies als Unterstützung der Compliance. • Ratschläge betreffend der Controls und der Schwächen des Systems

IT GENERAL CONTROLS IM DETAIL

Parameter der Matrix

Information Asset Kategorien	Information Asset Klassen
Information Asset Kategorien	IT Unit Information/Archiv IT Application Platform/Service Server/Database/Speicher Network/Communication Service End-User Geräte Datencenter Service Provider
Information Asset Klassen	Keine Klassifikation Group Policies SOX, PCI-DSS oder NFCM sowie jede andere Regulierung Vertraulichkeit Integrität Verfügbarkeit Verantwortung Nicht-Zurückweisung Data Privacy Records Management Other classification

ITGC Assessment Prozesse

Der ITGC Assessment Prozess ist in drei Teile aufgeteilt: **Initiales Risk Assessment** Die Information Assets einer Organisation sind identifiziert, kategorisiert, klassifiziert und analysiert, damit die Risiken in Verbindung mit der Nutzung des Assets festgestellt sind. Dieser Schritt ist die Basis für die Identifikation der Information Assets und deren Klassifikation sowie Kategorisierung.

1. **Controls Assessment**
   Basierend auf den Resultaten des ersten Schritts sind alle Controls für jedes Information Asset der Organisation identifiziert und ihre Implementation ist sowohl assessed als auch getestet. Das aktuelle Control Environment ist mit den Control Objectives verglichen damit die Reife der Control festgestellt werden kann.
2. **Remediation Management**
   Aktionen für die Remediation sind, wo nötig, definiert und implementiert nachdem das mit ihnen zusammenhängende Risiko evaluiert worden ist. Dieser Prozess ist im Normalfall im Risk Management Prozess integriert.

Der Controls Assessment Prozess wird entweder durch das jährliche Re-Assessment der Controls oder durch Änderungen, welche die Organisation oder Information Assets betreffen, ausgelöst. Diese sind unter anderem:

- Für die Organisation: Eine grosse Veränderung in der internen Struktur der Organisation. Oder in der Personalstruktur, der Verantwortlichkeiten und der Rollenverteilung, dem Offshoring von Aktivitäten, neuen Outsourcing-Lösungen, Akquisitionen und anderem.
- Für die IT Assets: Eine neue Implementation oder ein grosses neues Release, bedeutende Wechsel im Bereich Operations oder der Infrastruktur, ein grösserer Incident, unzufriedenstellendes Sicherungs-Review, neue Shared Services etc.
- Generell nach:
    - Änderungen in der Legislation oder der externen Regulierungen
    - Gescheiterten Tests der Controls
    - Identifikation der Lücken in den Controls oder sonstigen Schwachstellen
    - Neuklassifizierung der Assets folgend der Policy und des Klassifikationsprozesses.
    - Unzufriedenstellende Audit-Resultate
    - Komplettierung der Remediations

Der Controls Assessment Prozess wird für einzelne Information Assets in der Organisation ausgeführt. Die Hauptaufgaben des des Prozesses sind die Folgenden:

- Identifikation der Applicable Controls basierend auf der ITGC Matrix.
- Dokumentation der realen Local Control Procedures und Policies.
- Assessment des Reifegrades der Controls
- Identifikation der Lücken in den Controls wo das Reifelevel nicht erreicht ist.

Der Schlüssel-Output des Assessments beinhaltet:

- Reports über den Risikostatus.
- Bewilligte Risikomitigationspläne

Reporting und Monitoring sind ständig laufende Prozesse, die während dem ganzen Risikobehandlungsprozess erfolgen sollten.

Teilungen müssen sicherstellen, dass das Risikoreporting etabliert ist, damit der Fortschritt der Remediation Plans stets nachverfolgt werden kann, wie auch der Grad des Risikos, dem die Organisation gegenübersteht.

Fazit

Indem ein Lebenszyklus mit gut ausgewählten Kontrollen etabliert wird, ist es möglich, die Qualität und die Reife von mehreren kritischen Domains der Organisation stetig zu verbessern. Die Kontrollen können ein sehr wichtiges Element in der Sicherstellung der Compliance in einem Umfeld werden, das immer mehr verpflichtende und komplexe Regulationen erfordert.

Es ist daher absolut und in jedem Fall lohnenswert eine Organisationsstruktur und ein Konzept einzuführen, das sich um diese Art der Governance dreht. Zudem können so viele Synergien mit anderen wichtigen Abteilungen - wie zum Beispiel dem Internen Audit Team, der Information Security, abteilung dem Risk Management Office oder der Qualitätssicherung - geschaffen werden.

Dieser Artikel wurde aus dem Englischen übersetzt. Das Original, ebenfalls von Flavio Gerbino, finden sie auf www.scip.ch.

VULDB

Die Top 5 Schwachstellen im Mai/Juni

Die Top 5 Liste zeigt die interessantesten und schwerwiegendsten Schwachstellen des laufenden Monats. Alle Schwachstellen und Statistiken gibt es in der scip VulDB.

1 OpenSSL Cryptography and SSL/TLS Toolkit

OpenSSL DTLS Fragment Handler d1_both.c Pufferüberlauf

Datum	05.06.2014
Risiko	kritisch
Link	http://www.scip.ch/?vuldb.13454

Eine kritische Schwachstelle wurde in OpenSSL 0.9.8/1.0.0/1.0.1 ausgemacht. Hierbei geht es um eine unbekannte Funktion der Datei ssl/d1_both.c der Komponente DTLS Fragment Handler. Ein Upgrade auf die Version 0.9.8za, 1.0.0m oder 1.0.1h vermag dieses Problem zu beheben. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Die Entwickler haben entsprechend sofort reagiert.

2 Microsoft Windows™

Microsoft Windows TCP/IP Packet Handler Denial of Service

Datum	10.06.2014
Risiko	kritisch
Link	http://www.scip.ch/?vuldb.13548

Es wurde eine Schwachstelle in Microsoft Windows bis Server 2012, ein Betriebssystem, gefunden. Sie wurde als kritisch eingestuft. Dabei betrifft es eine unbekannte Funktion der Komponente TCP/IP Packet Handler. Die Schwachstelle lässt sich durch das Einspielen des Patches MS14-031 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 Microsoft Windows™

Microsoft Windows GDI+ Pufferüberlauf

Datum	10.06.2014
Risiko	kritisch
Link	http://www.scip.ch/?vuldb.13544

Eine kritische Schwachstelle wurde in Microsoft Windows bis Server 2012, ein Betriebssystem, ausgemacht. Hierbei geht es um eine unbekannte Funktion der Komponente GDI+. Die Schwachstelle lässt sich durch das Einspielen des Patches MS14-036 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.

4 ISC

ISC BIND EDNS Option Handler Denial of Service

Datum	11.06.2014
Risiko	problematisch
Link	http://www.scip.ch/?vuldb.13581

Es wurde eine Schwachstelle in ISC BIND 9.10.0/9.10.0-P1 entdeckt. Sie wurde als problematisch eingestuft. Hiervon betroffen ist eine unbekannte Funktion der Komponente EDNS Option Handler. Ein Aktualisieren auf die Version 9.10.0-P2 vermag dieses Problem zu lösen. Das Erscheinen einer Gegenmassnahme geschah sofort nach der Veröffentlichung der Schwachstelle. ISC hat daher unmittelbar gehandelt.

5 Cisco™

Cisco IOS XR IPv6 Packet Handler Denial of Service

Datum	11.06.2014
Risiko	problematisch
Link	http://www.scip.ch/?vuldb.13576

In Cisco IOS XR – die betroffene Version ist unbekannt – auf ASR 9000 wurde eine problematische Schwachstelle gefunden. Das betrifft eine unbekannte Funktion der Komponente IPv6 Packet Handler. Ein Upgrade vermag dieses Problem zu beheben. Das Erscheinen einer Gegenmassnahme geschah sofort nach der Veröffentlichung der Schwachstelle. Cisco hat offensichtlich unmittelbar reagiert.

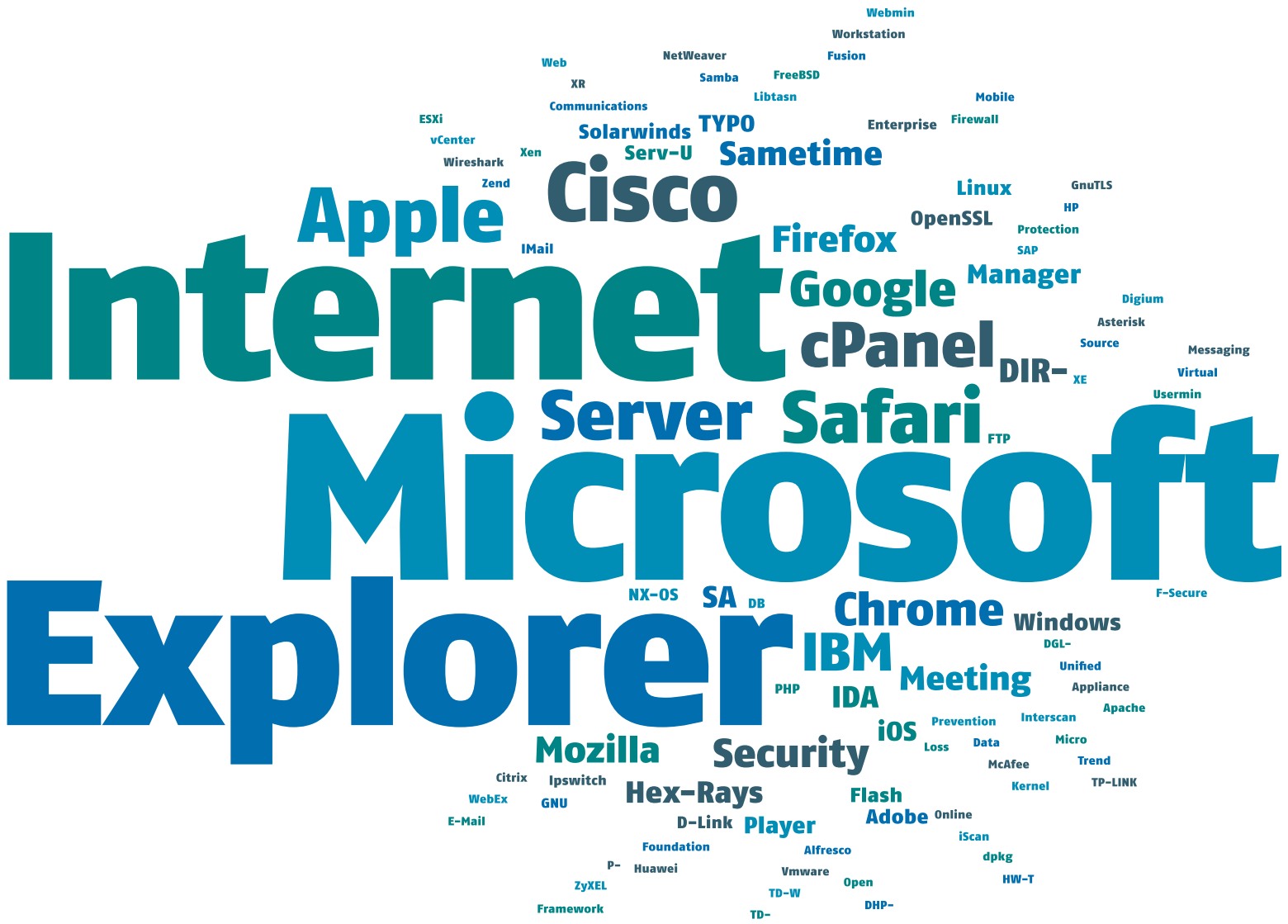
Auswertungsdatum: 18.06.2014

VULDB

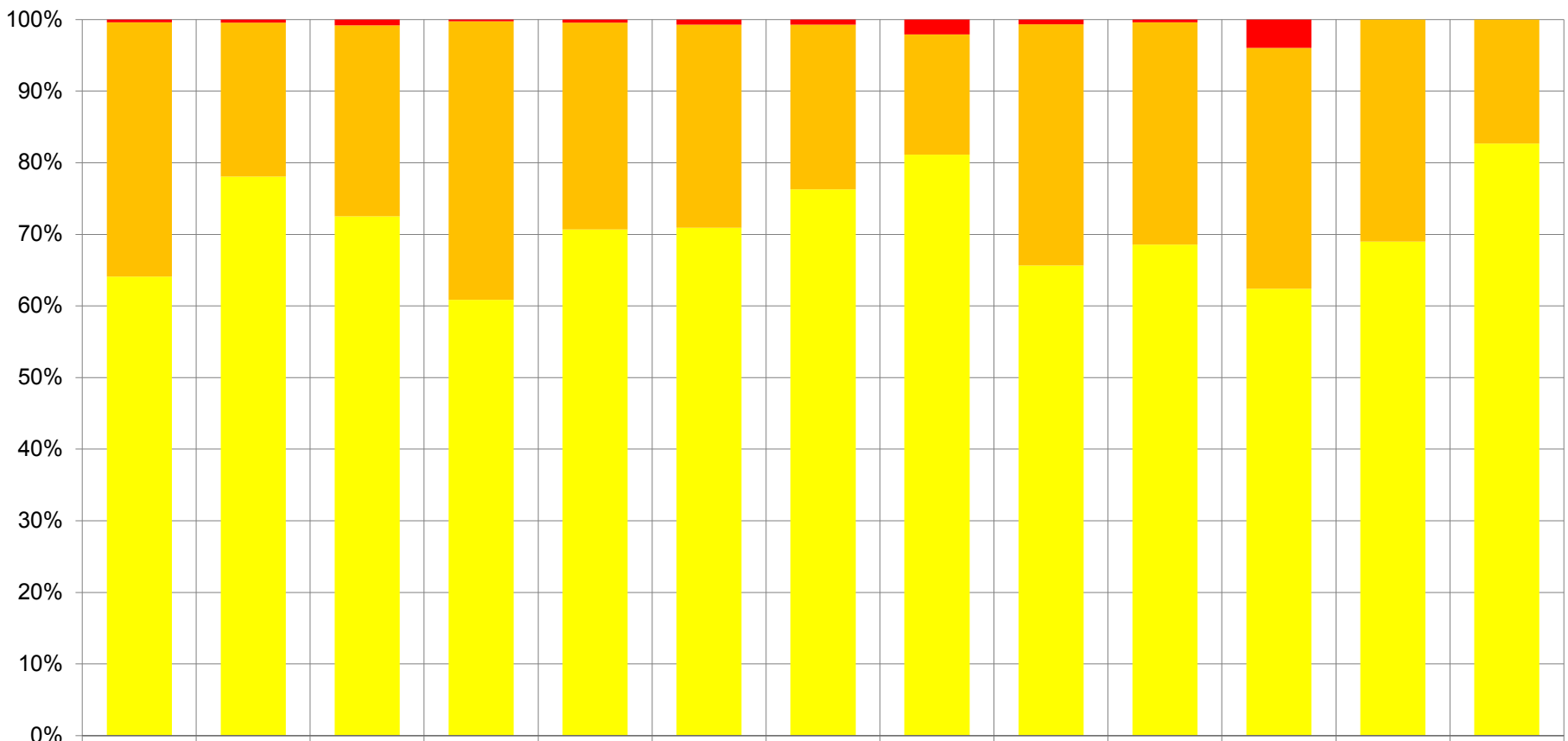
Statistiken aus der VulDB

Die Welt der Information Security wandelt sich stets. Um einen Überblick über den Verlauf und die Entwicklungen der Schwachstellen zu erhalten, analysieren wir die scip VulDB einmal im Monat.

MEISTBETROFFENE PRODUKTE MAI/JUNI 2014



VERLAUF DER SCHWACHSTELLEN ÜBER DIE VERGANGENEN 12 MONATE



	2013-6	2013-7	2013-8	2013-9	2013-10	2013-11	2013-12	2014-1	2014-2	2014-3	2014-4	2014-5	2014-6
sehr kritisch	1	2	2	1	2	2	2	8	2	1	14	0	0
kritisch	93	93	67	165	132	76	62	64	98	81	119	80	26
problematisch	168	338	182	258	323	190	206	309	191	179	221	178	124

Auswertungsdatum: 18.06.2014

RÄTSEL

Ein rosa Rätsel

IN EinEM EINsTÖcKiGen ROSA HAuS WOhNT eIN RoSA MAnn MiT EINeR ROSA KATzE, EineM RosA cOMPuTEr UND Einem ROsa sTUhL. AuCH SeIN TeIEFoN IsT ROsA. geNaU wIE Seine dUscHE. AILES iST rosA. WeLChe faRBe HAT DIe TRePpE? es GIbt KeINe TReppE iN EIneM eINstöCKIGEn HAus!

DIE LÖSUNG:

DER PREIS

Gewinnen Sie ein Exemplar der gesammelten und neu aufbereitenen Labs-Aritkel der scip-Mitarbeiter, mit dem Titel **"scip Labs 2013".** Es enthält Berichte aus der Szene, technische Artikel und wichtige Ratschläge von IT-Security-Profis.

Mailen Sie uns die Lösung des obigen Rätsels an die Adresse doba@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 15.07.2014. 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.

SERVICE

Security Assessment

Fast wie bei einem Angriff sammeln die Experten der scip AG Informationen, um dann die Schwachstellen im Netzwerk zu finden. Das Assessment verlangt den Mitarbeitern viel ab, bietet dem Kunden aber viel.

Traditionell im Sicherheitsbereich verankert sind so genannte Security Assessments oder Security Audits. Bei diesen werden spezifische Objekte - auch Assets genannt - auf die bestehende Sicherheit hin untersucht. Dies geschieht, um ein Maximum an Wirtschaftlichkeit erreichen zu können, zu großen Teilen mittels automatisierten Lösungen. Durch quelloffene und kommerzielle Vulnerability Scanner werden typische Probleme ermittelt.

Exaktheit und Wissen ist Trumpf

Das Fachwissen der Auditoren wird von herausragender Wichtigkeit, wenn es um die Interpretation der anfallenden Daten geht. Sodann gilt es Falschmeldungen, False Positives und False Negatives, zu erkennen und richtig auf sie zu reagieren. Eine Qualität eines Security Assessments ist massgeblich von der Genauigkeit der Prüfung abhängig.

In einem weiteren Schritt werden die etwaigen Schwachstellen durch manuelle Zugriffe quergeprüft. Durch ein dediziertes Exploiting kann sodann die effektive Existenz einer Sicherheitslücke verifiziert werden. Damit wird der Anteil der fehlerhaften Resultate auf ein absolutes Minimum reduziert.

Test aus Angreifersicht

Das Vorgehen bei solchen Sicherheitsüberprüfungen unterscheidet sich nur in wenigen Punkten von dem eines echten Angreifers. Auch hier werden zuerst Daten zur Zielumgebung gesammelt. Eine Auswertung dieser soll Angriffspunkte, die sodann angegangen werden sollen, ausgemacht werden.

Es geht nicht darum, in ein System zu kommen, sondern die Angriffsfläche alle potentiellen Schwächen auszumachen. Längerfristig soll nämlich die Sicherheit in allen Bereichen gewahrt oder gar erhöht werden können.

Haben wir Ihr Interesse geweckt? Zögern Sie nicht und kontaktieren Sie uns unter der Telefonnummer +41 44 404 13 13 oder schicken Sie eine Mail an info@scip.ch.