SWITCHcert Report zu aktuellen Trends im Bereich IT-Security und Privacy

Januar / Februar 2018

SWITCH

I. Meltdown und Spectre: Security Supergau direkt ab Prozessor

Die Bombe platzte kurz nach dem Jahreswechsel. Und sie hatte mit lautem, aber harmlosem Silvester-Feuerwerk nichts, aber auch überhaupt nichts, zu tun. Vielmehr offenbarten die Berichte über massive Sicherheitslücken in Prozessoren von INTEL, AMD, ARM den Supergau der IT-Security. Bereits im Juni 2017 hatte Jann Horn vom Google Project Zero die drei marktführenden Prozessorenhersteller über gravierende Sicherheitslücken in deren Produkten informiert. Nach einer langen «Anstands?»-Frist informierte INTEL die Öffentlichkeit erst Anfang Januar 2018 über der Lücken. Fakt ist: Abermillionen Computer, Smartphones und Mobilgeräte, in denen die Chips verbaut sind, sind Angriffen wie Spectre oder Meltdown so hilflos ausgesetzt, dass das CERT-Team der Carnegie-Mellon-University als Patch zunächst nur dazu raten konnte, die aktuellen Betriebssysteme zu installieren oder die Prozessoren auszutauschen. Inzwischen sind einige Patches verfügbar, dennoch ist das Sicherheitsproblem so ernst, dass wir an dieser Stelle einen Überblick in 5 Punkten liefern wollen:

1) Was macht Meltdown & Spectre zu einem solch grossen Sicherheitsrisiko?

Computer und Mobilgeräte besitzen Sicherheitsmechanismen, die verhindern sollen, dass Programme jedweder Art beliebig Daten aus dem Speicher eines Geräts abrufen können. Spectre und Meltdown sind zwei verschiedene Angriffsmuster, welche diese

© SWITCH 2018

Sicherheitsmechanismen ausser Kraft setzen. Sind die Sicherheitsmechanismen geknackt, laden und speichern Programme auch solche Daten, die sie gar nicht benötigen, die aber von entsprechend programmierter Schadsoftware gelesen und «entführt» werden können, darunter zum Beispiel Passwörter und Krypto-Schlüssel.

2) Wie funktioniert das?

Damit sie schneller und leistungsfähiger arbeiten, nutzen sogenannte «Out-of-Order»-Prozessoren eine Technik namens «Speculative Execution». Der Name der Technik ist dabei – in des Wortes wahrstem Sinn – Programm: Der Prozessor arbeitet Out of Order und spekuliert auf die nächstfolgenden Befehle. Wenn diese nicht ausgeführt werden, werden die dafür benötigten und auf «Vorrat» bereits in den Speicher geladenen Daten «zum Müll gebracht». Jedoch werden sie nicht vernichtet, sondern in Speicherbereichen von Programmen oder des Betriebssystems abgelegt. Genau diese «Mülltonnen» durchwühlen Spectre und Meltdown, um sich die besten Reste herauszupicken. Konkret: Zugangsdaten, Codes, Kryptoschlüssel und mehr (eine andere schöne Erklär-Analogie findet sich im unten angegebenen Artikel auf ds9a.nl)

3) Was kann man dagegen tun?

Generell gilt: jedes System soll stets mit den neusten Updates des jeweiligen Herstellers auf aktuellem Stand sein. Im einzelnen sind jedoch so viele Geräte so vieler Hersteller betroffen, dass wir ausnahmesweise im Lauftext einen Link setzen und auf die hervorragende Zusammenstellung der Massnahmenvorschläge der einzelnen Hersteller bei heise.de verweisen:

https://www.heise.de/security/meldung/Meltdown-und-Spectre-Die-Sicherheitshinweise-und-Updates-von-Hardware-und-Software-Herstellern-3936141.html

Die meisten Hersteller arbeiten nach eigenen Aussagen fieberhaft daran, die Sicherheitslücken zu schliessen. Bei genauem Hinsehen stellt sich aber heraus, dass die Patches primär für 64-bit-Architekturen entwickelt wurden und die älteren 32-bit-Modelle weiterhin grossteils ungeschützt bleiben. Zur Oberpeinlichkeit gerieten schliesslich die ersten Patches von Intel, die so fehlerhaft waren, dass Intel Ende Januar selbst empfahl, die zuvor empfohlenen Updates nicht aufzuspielen. Es sieht so aus, als sei dem Chiphersteller der «Anhalter durch die Galaxis» abhanden gekommen, auf dem ja bekanntlich in freundlichen grossen roten Lettern die Worte stehen: KEINE PANIK!

© SWITCH 2018

4) Sind schon Angriffe ausgeführt worden?

Ja. Denn ein Security- und Patch-Chaos, wie es derzeit herrscht, ist ja geradezu ein roter Teppich für Trittbrettfahrer und Hacker. So kursieren SPAM-Mails, in denen angeblich das deutsche Bundesamt für Sicherheit in der Informationstechnik BSI zum Upload eines als Meltdown-/Spectre-Patch getarnten Trojaners auffordert. Am 1. Februar 2018 informierte die Firma AV-Text auf Twitter, bislang 139 Malware Samples gefunden zu haben, die mit Spectre und Meltdown in Verbindung stehen. Auch Fortinet will beobachtet haben, dass Hacker Javascript-Code modifizieren, um beide Sicherheitslücken ausnutzen zu können.

5) Wie geht´s weiter?

Die Arbeit an den Patches geht eher schleppend voran. Während Apple und Google mit Betriebssystem- und Browser-Updates die durch diese Lücken verursachten Gefahren nach eigenen Angaben gebannt haben, geben sich die anderen Tech-Giganten – obwohl sonst mit vollmundigen Vorankündigungen und Terminversprechen nicht eben zurückhaltend – überraschend einsilbig und verweigern auch schon mal jeden Kommentar. Es bleibt also nur der – niemand zufriedenstellende – Rat der CERT-Experten der Carnegie Mellon University: Betriebssystem-Updates installieren und notfalls den Prozessor tauschen.

Nachzulesen unter:

https://www.heise.de/security/meldung/Analyse-zur-Prozessorluecke-Meltdown-und-Spectre-sind-ein-Security-Supergau-3935124.html

https://ds9a.nl/articles/posts/spectre-meltdown

https://www.heise.de/security/meldung/Meltdown-und-Spectre-Die-Sicherheitshinweise-und-Updates-von-Hardware-und-Software-Herstellern-3936141.html

https://www.heise.de/security/meldung/Meltdown-Patches-32-Bit-Systeme-stehen-hinten-an-3940207.html

http://www.spiegel.de/netzwelt/web/intel-us-chiphersteller-warnt-vor-sicherheitsluecken-meltdown-und-spectre-a-1189294.html

https://www.netzwelt.de/betrugswarnungen/163398-vorsicht-betrug-gefaelschte-bsi-mails-ueber-meltdown-spectre-update.html#utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:%20netzwelt%20(netzwelt.de%20-%20Aktuelle%20News)

http://www.maclife.de/news/wird-ernst-erste-malware-spectre-meltdown-unterwegs-100100109.html

© SWITCH 2018

II. Leaks, Fakes und Kryptowährungshacks: Geschäftsmodelle der anderen Art

Die Zeiten, in denen alleine um der Hackerehre willen gehackt wurde, scheinen sich mit Mainframes und PCs als epocheprägende Geräte ihrem Ende zu nähern. In der vernetzten und mobilen Welt geht es auch bei den Bösen fast immer nur um schnöden Mammon. Drei Geschäftsmodelle haben dabei in letzter Zeit immer wieder für Aufmerksamkeit gesorgt:

1) Das Geschäft mit geleakten LogIn-Daten

Brian Krebs, Autor und Betreiber des Blogs «krebsonsecurity» hat in seinem lesenswerten Artikel «The Market for Stolen Account Credentials» sehr detaillierte Fakten zu diesem Geschäftsmodell zusammengetragen. Er konnte nachweisen, dass sich eine Nutzername-Passwort-Kombination auf der ersten Marktstufe des Darknets für 8 Dollar verkaufen lässt. Einer der Verkäufer konnte so in den ersten sieben Monaten des Jahres 2017 ca. 35.000 Zugangsdaten-Paare zum Preis von 288.000 Dollar losschlagen. Der Aufkäufer – quasi der Grosshändler – verkauft diese Daten dann weiter für 15 US-Dollar, in seltenen Fällen für bis zu 150 US-Dollar! Lebensmittelhändler, die mit effektiven Gewinnmargen im niedrigen einstelligen Bereich kämpfen, würden blass vor Neid. Auf der Dark-Website eines solchen Grosshändlers findet sich denn auch eine ganz normale Preisliste mit den Zugangsdaten von Nutzern von mehr als 200 e-commerce- und Bank-Websiten, sorgfältig aufgelistet, mit Angaben zu Preisen und zur verfügbaren Zahl der gehackten Account-Daten. Und einen Service gibt´s auch: Denn neben den Zugangsdaten werden auch gestohlene Komplett-Identitäten von User verkauft, inklusive ausgewiesener Kreditwürdigkeit – je höher die ist, desto höher der Preis für die Identität.

2) Das Geschäft mit gefakten Followern

Gefakte Follower sind schon lange ein Problem für Social Media Plattformen. So schätzt CNN, dass etwa 83 Millionen Facebook-Accounts Fake-Accounts sind, generiert einzig zum Zweck, Followers zu generieren, die dann von echten Celebrities oder solchen, die glauben, es damit werden zu können, gekauft werden, um für ihre eigenen Accounts einen Einfluss vorzutäuschen, der nicht vorhanden ist (funktionierte gemäss Aussagen der Wahlkampfleiterin von Donald Trump gegenüber BBC auch so im amerikanischen Präsidentschaftswahlkampf). Business Insider behauptet, dass 8% aller Instagram Accounts gefaket sind.

© SWITCH 2018

Marktführer im Geschäft mit den gefaketen Followers ist die New Yorker Firma Devumi, die alleine für die Twitter-Accounts von Politikern, Sportlern, Schauspielern und anderen 200 Millionen (!) Fake Followers verkauft haben soll. Ende Januar 2018 veröffentlichte die New York Times eine detaillierte Story über die «Follower Factory», die jetzt für Devumi ein juristisches Nachspiel haben wird. Denn zum einen waren die verkauften Followers keine menschlichen Users, sondern Bots. Darin sieht der New Yorker Staatsanwalt Eric Schneidermann einen Betrug, den er nun zur Anklage gebracht hat. Zum anderen sollen unter den 200 Millionen Followers mindestens 55.000 die Daten realer menschlicher User kopiert haben – auf die Bots also Name, Heimatort und viele andere Daten geklont worden sein. Dieser Identitätsdiebstahl wiegt denn auch noch schwerer als der Betrug mit den Bots und bringt nicht nur Devumi in Verruf, sondern stellt das gesamte Modell des Influencer-Marketings in Frage.

3) Der Bankraub ohne Bank (Diebstahl von Kryptowährung in der Blockchain)

Mit dem Diebstahl von geschätzten 400 bis 450 Millionen Euro in der japanischen Kryptowährung NEM an der Tokioter Börse Coincheck Ende Januar hat der virtuelle «Bank»raub eine neue Dimension erreicht – zumindest was die Grösse der Beute betrifft. Zuvor hatten vor allem die Hacks von Mount Gox und DAO nicht nur die Anleger ärmer gemacht, sondern vor allem das Vertrauen erschüttert, dass Kryptowährungen in der Blockchain vor Raubzügen im grossen Stil gefeit seien (siehe SWITCH Security Report 7/2016).

Nachzulesen unter:

https://krebsonsecurity.com/2017/12/the-market-for-stolen-account-credentials
https://thenextweb.com/contributors/2017/08/27/influencer-marketing-trouble-fake-followers
https://www.derstandard.de/story/2000073187437/200-millionen-follower-vermittelt-fake-verdacht-gegen-social-media-firma
https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html
https://www.coindesk.com/coincheck-confirms-crypto-hack-loss-larger-than-mt-gox
http://www.chip.de/news/Bitcoin-Boerse-um-400-Millionen-Dollar-erleichtert-Nutzer-sollen-trotzdem-Geld-zurueckbekommen_132851182.html
https://www.nzz.ch/wirtschaft/hackerangriff-trifft-japanische-krypto-boerse-ld.1352017

© SWITCH 2018

III. Italianitá im Smartphone – Staatstrojaner überwacht Smartphone-Nutzer

Italien und Trojaner mögen für Historiker und Linguisten zusammenpassen wie Spaghetti und Retsina, für IT-Security-Experten gehören sie zusammen wie der Wind und das Meer. So machte im Jahr 2015 der Hack des italienischen Staatstrojaner-Anbieters «The Hacking Team» Schlagzeilen, die bis in die Schweiz Wellen schlugen, hatte doch die Kantonspolizei Zürich mehr als eine halbe Million Franken in einen nach dem Hack nicht mehr einsetzbaren Trojaner (fehl-)investiert (siehe SWITCH Security Report 8/2015).

Nun warnen Sicherheitsexperten der Kaspersky Labs (mehr dazu im nächsten Punkt) vor dem bereits seit 2014 aktiven gefährlichen Staatstrojaner «Skygofree», der sich auf Android-Smartphones unbemerkt Root-Zugriff verschafft, um damit das Telefon samt Mikrofon und Kamera(s) komplett zu übernehmen. Die Datenspuren, die die Kaspersky-Experten fanden, deuten auf Italien als Herkunftsland von «Skygofree» hin, die Methoden erinnern an die der Hacking-Team-Trojaner.

Die mächtige und hochinnovative Spyware kann nicht nur Daten abgreifen, Telefonate, SMS und WhatsApp mitschneiden, sondern auch Mikrofon und Kamera aktivieren, wenn sich das Telefon an von den Angreifern festgelegten GPS-Koordinaten befindet. Aufs Smartphone gelangt sie via gefaktem System-Update von einer ebenso gefakten Mobilfunkanbieterseite, zu deren Besuch die Nutzer aufgefordert werden. Ist der Trojaner einmal installiert, integriert sich die Malware als geschützte App, so dass sie auch bei abgeschaltetem Bildschirm weiterläuft.

Um sich vor «Skygofree» und anderer fortschrittlicher mobiler Malware zu schützen empfiehlt Kaspersky Lab folgende Sicherheitsmaßnahmen:

- Eine zuverlässige Sicherheitslösung auf allen mobilen Endgeräten installieren
- Vorsicht bei E-Mails von unbekannten Personen oder Organisationen mit unerwarteten Anfragen oder Anhängen
- Nicht auf Links in E-Mails klicken, bevor die verlinkte Seite auf Integrität und Ursprung überprüft wurde. Im Zweifelsfall den Service Provider kontaktieren
- Systemadministratoren sollten die Application-Control-Funktionalität in ihren mobilen Sicherheitslösungen aktivieren, um Programme zu kontrollieren, die für solche Angriffe anfällig sind.

Der untenstehende Link zu weiteren Details auf der Kaspersky-Website ist sicher.

© SWITCH 2018

Nachzulesen unter:

https://www.n-tv.de/technik/Staatstrojaner-ueberwacht-Smartphone-Nutzer-article20235630.html
http://www.zeit.de/digital/datenschutz/2018-01/skygofree-android-whatsapp-schadsoftware
https://www.heise.de/security/meldung/Skygofree-Ausgefeilter-Android-Trojaner-spioniert-seit-2014-Smartphones-aus-3943853.html
http://newsroom.kaspersky.eu/de/texte/detail/article/skygofree-hochentwickelte-spyware-seit-2014-aktiv

IV. Out für Kaspersky auch in Litauen

Ob die Warnung vor Staatstrojanern oder der – von Kaspersky vehement bestrittene – Vorwurf, NSA-Daten an russische Behörden geliefert zu haben, oder einfach Trumps America First-Politik dazu geführt haben, dass amerikanische und britische Behörden keine Kaspersky-Software mehr einsetzen dürfen, kann hier nicht geklärt werden (siehe SWITCH Security Report 5/2018). Fakt ist: Seit Ende 2017 darf die Software des Sicherheitsunternehmens mit Moskauer Wurzeln trotz ihrer Qualität, Verbreitung und Beliebtheit auch in Litauens Behörden nicht mehr eingesetzt werden. Darüber hinaus verbietet die Regierung auch privaten Unternehmen aus dem Finanz-, dem Energie- und dem Logistiksektor den Einsatz von Kaspersky-Software, weil diese die nationale Sicherheit gefährden könnte.

Inzwischen hat US-Präsident Trump im Gesetz zum Verteidigungsbudget auch das Verbot der Kaspersky-Security-Software fixiert, obwohl der IT-Konzern alle Vorwürfe vehement bestreitet und darauf verweist, dass geheime NSA-Programme nur deshalb auf Kaspersky-Servern landeten, weil ein NSA-Mitarbeiter auf seinem Laptop neben dem Kaspersky Anti-Viren-Scanner eine Raubkopie für Microsoft-Software installiert hatte.

Um gegen den Vertrauens- und Einnahmenverlust anzukämpfen hat Kaspersky eine Transparenz-Initiative angekündigt, in deren Rahmen auch der Quellcode der Software veröffentlicht werden soll.

Nachzulesen unter:

https://futurezone.at/digital-life/kaspersky-software-auch-in-litauen-verboten/303.246.654
https://derstandard.at/2000070337380/Trump-fixiert-Verbot-von-Kaspersky-Software-fuer-US-Behoerden
https://derstandard.at/2000066667979/Kaspersky-NSA-Hacker-installierte-falsche-Microsoft-Software
http://www.spiegel.de/netzwelt/netzpolitik/kaspersky-wirbt-mit-transparenzinitiative-um-vertrauen-a-1174252.html

© SWITCH 2018

V. Strava Leaks – Fitness Secrets einmal anders

Während in Washington Kaspersky der Spionage bezichtigt wird, haben Mitarbeitende amerikanischer Militär- und Sicherheitsbehörden dank der Veröffentlichung ihrer Fitness-Aktivitäten im Internet – wohl eher ungewollt – Lagepläne und Strukturen hochgeheimer amerikanischer Militär- und Sicherheitseinrichtungen auf der ganzen Welt für jedermann zugänglich gemacht. Verantwortlich dafür ist die Fitness-App Strava, die von vielen Fitness-Trackern genutzt wird, damit Sportlerinnen und Sportler ihre Trainings aufzeichnen und posten können. Alle Daten fügt Strava zu einer sog. Global Heat Map zusammen. Auf der Website des Unternehmens könne Interessierte nachvollziehen, wo und in welcher Intensität Strava-App-Nutzer besonders aktiv sind. Aus mehr als 3 Milliarden einzelnen GPS-Datenpunkten, einer Milliarde Fitnesszyklen und 27 Milliarden Streckenkilometern hat Strava im November 2017 eine Weltkarte der besonderen Art entwickelt und online gestellt.

Unerwünschte Nebenwirkung: Mitten im ansonsten eher trackfreien Afghanistan, in Somalia oder in Syrien zeichnen sich auffällige Strukturen bis in Grundrisse hinein ab. Der geübte Spion schliesst daraus sofort: Hier bewegen sich Menschen, die sich Fitnesstracker leisten können und diese auch aktiv nutzen. Die Wahrscheinlichkeit, das es sich dabei um amerikanische, europäische oder russische Soldaten oder Geheimdienst- oder Botschaftsangehörige handelt, dürfte weitaus höher liegen als die, dass afghanische, somalische oder syrische Zivilisten eben öfters um den Block gejoggt sind. Zumal die US-Streitkräfte den Einsatz von Fitness-Trackern und -Apps aktiv fördern und 2013 sogar 2.500 Fitbit-Tracker in einem Pilotprojekt verteilt haben. Dabei haben sie wohl einen Ratschlag des 2012 verstorbenen amerikanischen Leadership-Gurus Stephen Covey nicht beachtet: «Always begin with the end in mind!»

Nachzulesen unter:

https://www.wired.de/collection/life/eine-fitness-app-enthuellt-geheime-militaerbasen
https://labs.strava.com/heatmap/#8.76/20.92056/39.58226/hot/all

Dieser SWITCH-CERT Security Report wurde von Dieter Brecheis und Michael Fuchs verfasst.

Der Security Report spiegelt nicht die Meinung von SWITCH wider, sondern ist eine Zusammenstellung verschiedener Berichterstattungen in den Medien. SWITCH übernimmt keinerlei Gewähr für die im Security Report dargelegten Inhalte, Meinungen oder deren Richtigkeit.

© SWITCH 2018