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

Dezember 2015

SWITCH

I. Pawlow in Paris – Wie das Reiz-Reaktionsmuster von Terroranschlägen die reale mit der Online-Welt verlinkt

Dass reale und Online-Welt weitaus interdependenter miteinander verknüpft sind als allgemein zu vermuten wäre, zeigt sich traurigerweise gerade nach Terroranschlägen wie denen von Paris. Und es ist besonders bitter, feststellen zu müssen, dass Terroranschläge seit den Anfängen der RAF über 9/11 bis hin zu denen von Paris eine Art zynischer Routine heraufbeschwören, die der klassischen Konditionierung nach Iwan Petrowitsch Pawlow nicht unähnlich ist: Je brutaler und menschenverachtender der Anschlag als Stimulus, desto lauter ertönen die Rufe nach stärkerer Online-Überwachung, Ausweitung von Datensammlung und -speicherung durch Sicherheitsbehörden und Einschränkung der Informationsfreiheit als Response.

Angesichts des Ausmasses der Anschläge von Paris war davon auszugehen, dass Taten folgen und in kürzester Zeit umgesetzt würden. Der unmittelbar nach den Anschlägen proklamierte Ausnahmezustand wirkt sich aber nicht nur im realen Leben Frankreichs aus, sondern betrifft auch die virtuelle Welt. Die kürzlich verabschiedete Erweiterung der französischen Notstandsgesetze erteilt dem

Innenminister die Befugnis, im Verdachtsfall auch ohne richterlichen Beschluss Websites und Social Media-Dienste zu sperren. Und die EU-Minister beschlossen ein Terrorabwehrpaket, das - ziemlich vorhersagbar - die deutliche Ausweitung der Vorratsdatenspeicherung vorsieht.

Auch vorhersagbar und mit beinaher obszöner Routine werden auch Spammer und Cyberkriminelle nach Anschlägen aktiv: Schamlos nutzen sie Betroffenheit, Mitgefühl oder Angst der Menschen, um via gefakter Solidaritätsmails oder Email-Warnungen Viren und andere Malware zu verbreiten.

Es lässt sich aber auch viel Positives finden: Facebook, Google, Twitter, AirBnB, Skype und andere Mobilkommunikationsanbieter stellten kurzfristig Apps, Tools oder andere Angebote bereit, um aus der Onlinewelt heraus Hilfe, Informationen und Solidarität in die reale Welt zu bringen.

Nachzulesen unter:

http://futurezone.at/meinung/terror-in-paris-ein-ueberwachungsaufschrei/164.022.301
http://www.heise.de/newsticker/meldung/Pariser-Anschlaege-Polizei-ruft-nach-erweiterter-Vorratsdatenspeicherung-2921757.html
http://www.nzz.ch/newsticker/grossbritannien-will-anti-terror-gesetze-deutlich-verschaerfen-1.18431200
http://www.welt.de/politik/ausland/article148847901/Ausnahmezustand-in-Frankreich-Was-heisst-das.html
http://futurezone.at/netzpolitik/frankreich-darf-nun-soziale-netzwerke-und-webseiten-sperren/165.004.716
http://www.heise.de/newsticker/meldung/Antwort-auf-Terror-von-Paris-Grenzkontrollen-Datensammlungen-Datenaustausch-3010264.html
http://futurezone.at/digital-life/warnung-vor-spam-welle-nach-anschlaegen-in-frankreich/164.511.959
http://www.salzburg.com/nachrichten/welt/politik/sn/artikel/innenministerium-warnt-hinterhaeltiger-paris-virus-verbreitet-173661/
http://www.theguardian.com/technology/2015/nov/16/facebook-safety-check-technology-paris-terrorist-attacks

II. «Added value» ab Werk – Neugeräte kommen mit Malware und extra Sicherheitslücken

Bereits im Security Report vom März dieses Jahres hatten wir über den Lenovo/ Superfish-Skandal berichtet. Eigentlich sollten Käuferinnen und Käufer technischer Produkte davon ausgehen können, dass Neugeräte ab Werk sauber, also frei von Malware oder groben Sicherheitslücken, ausgeliefert werden. Nun wurde bekannt, dass auch Dell Computer mit eingebauter «Root-Zertifikat-Hintertür» ausgeliefert hat und damit einen scheunentorgrossen Angriffsvektor öffnet. Denn neben dem Zertifikat selbst hat Dell auf den Rechnern auch noch einen privaten Schlüssel installiert, so dass Hacker mit einer Man-in-the-Middle-

Attacke auch https-verschlüsselte Verbindungen knacken können. Wie zuvor bereits Lenovo, so entschuldigte sich Dell im hauseigenen Blog damit, dass das Zertifikat im Bemühen installiert wurde, besseren Kundenservice und -support bieten zu können. Zudem stellten die Texaner dort eine Anleitung sowie ein Tool zum Entfernen des Zertifikats bereit. Doch kaum glaubte man, dass damit die Delle ausgebügelt sei, da entdeckten aufmerksame User bereits die nächste mit dem Namen «Dell System Detect», die sich von der Dell-Website herunterladen lässt und die gleichen Sicherheitslücken aufreisst wie eDellRoot.

Malwareverseuchte Neuware wird aber nicht nur im Direktvertrieb ausgeliefert. Seit November ist bekannt, dass (laut The Register) zehntausende Tablets verschiedener Marken, die bei Amazon angeboten werden, mit «Cloudsota» infiziert sind. Der Trojaner verhindert das Wegklicken von Werbung, deinstalliert Security-Software und Apps und installiert sich automatisch von neuem, wenn er entfernt wird.

Noch dreister mutet der aktuelle «Conficker»-Fall an. Bereits 2010 wurde Conficker beim Versuch ertappt, die Netzwerke der Stadtverwaltung und der Polizei von Manchester zu kompromittieren, nachdem er dort durch Windows-Sicherheitslücken eingedrungen war. Nun wurde er in Florida gesichtet. Gut getarnt steckte er in zwei sogenannten Bodycams der Polizei, die im Rahmen von Entwicklungsarbeiten für ein cloudbasiertes Speichersystem für Behörden und die Polizei genutzt wurden.

Sicherheitsprobleme bestehen aber nicht nur für Discount-Tablets aus China und einzelne Bodycams. Die Sicherheitsexperten von Googles Project Zero fanden in der von Samsung modifizierten Android-Variante für das neue Smartphone-Flagschiff Galaxy S6 Edge elf (!) Security Bugs mit hohem Sicherheitsrisiko.

Nachzulesen unter:

http://www.switch.ch/export/sites/default/security/.galleries/files/security-reports/SWITCH_Security_Report_2015-03_de.pdf
http://www.zdnet.de/88252615/superfish-20-dell-liefert-computer-mit-vorinstalliertem-root-zertifikat-aus
https://blog.hboeck.de/archives/876-Superfish-2.0-Dangerous-Certificate-on-Dell-Laptops-breaks-encrypted-HTTPS-Connections.html
http://en.community.dell.com/dell-blogs/direct2dell/b/direct2dell/archive/2015/11/23/response-to-concerns-regarding-edellroot-certificate
http://www.golem.de/news/https-verschluesselung-noch-ein-gefaehrliches-dell-zertifikat-1511-117615.html
http://www.theregister.co.uk/2015/11/13/amazon_vendors_flog_thousands_of_rooted_malwareladen_tablets
http://futurezone.at/digital-life/tablets-mit-vorinstallierter-malware-im-angebot-von-amazon/163.251.676
http://winfuture.de/news,53287.html
http://www.zdnet.com/article/crooks-use-old-school-conficker-virus-to-infect-police-body-cams

http://blog.check-and-secure.com/trojanisierte-body-cams_15-11-19
http://www.theguardian.com/technology/2015/nov/04/google-samsung-galaxy-s6-edge-high-impact-security-bugs

III. Profiler in aller Stille – Audio Beacons ermöglichen Werbern umfassendes Tracking

In der letzten Security Report-Ausgabe hatten wir über eine gute Sache berichtet: Einem Forscherteam der ETH Zürich war es mithilfe eines Sound-Proofs gelungen, die Zwei-Faktor-Authentifizierung wesentlich zu vereinfachen.

In dieser Ausgabe müssen wir auf die dunkle Seite der Macht verweisen, die sich in Mikrofonen in Tablets, Smartphones, Lap- oder Desktops versteckt. Denn seit mehr als einem Jahr nutzen Werbeunternehmen eine auf Sound basierte und vor allem vom Start-Up Unternehmen «SilverPush» propagierte Tracking-Technologie, an der auch Firmen wie Adobe, Drawbridge und Flurry an vergleichbaren Technologien arbeiten sollen. Ziel ist es generell, Webnutzer zu Werbezwecken auszuspionieren, User- und Werbeprofile zu verfeinern und entsprechend weiterzuverkaufen oder selbst zu verwenden. Und zwar über alle Geräte hinweg, mit denen der jeweilige User mit dem Netz verbunden ist, also Smartphones und Tablets, Car Computer, Fernseher, Laptop, Desktop, Wearables usw. Wen interessiert schon, was sich an einer IP-Adresse an Kundenverhalten abgreifen lässt, wenn er mit dem sogenannten «Cross Device Ad Targeting» das ganze 360-Grad-Paket bekommt?

Was einfach klingt, ist technisch relativ aufwändig und funktioniert in einer Art «Zwei-Wege-Erkennung». Apps auf Smartphone oder Tablet, die mit der SilverPush-Technologie ausgerüstet sind, reagieren auf für Menschen unhörbare hochfrequente Audiosignale, die von Werbung im TV oder im Netz, die ihrerseits SilverPush nutzt, ausgestrahlt werden. Dieser Sound Beacon meldet automatisiert an den SilverPush-Server, dass das Gerät, das den Beacon ausgestrahlt hat und das, das ihn empfangen hat, zusammengehören. Damit ist SilverPush in der Lage, TV-Geräte, Computer, Tablets etc. einem Smartphone-Nutzer zuzuordnen und sein Verhalten geräteübergreifend aufzuzeichnen.

Der Nutzer hat derzeit keine Möglichkeit, dieses perfide Tracking abzuschalten, ohne die entsprechenden Apps von seinen Mobilgeräten zu entfernen. Einer der ersten Kunden, die dieses Tracking im grossen Stil einsetzen, ist der

Konsumgüterriese Procter & Gamble, doch zeigen offenbar viele werbeintensiven Unternehmen Interesse an der neuen Technologie.

Nachzulesen unter:

https://www.switch.ch/export/sites/default/security/.galleries/files/security-reports/SWITCH_Security_Report_2015-11_de.pdf
http://www.netzwelt.de/news/155813-werbung-geraeteuebergreifendes-tracking-dank-sound-beacons.html
http://www.nzz.ch/digital/unhoerbare-toene-spionieren-webnutzer-aus-ld.3054
http://www.theatlantic.com/technology/archive/2015/11/your-phone-is-literally-listening-to-your-tv/416712

IV. Ads, Adblocker, Anti-Adblocker, Anti-Adblock-Killer – das Wettrüsten geht weiter

Dass die unter Punkt III dargestellte Technologie dazu geeignet ist, das Image der Onlinewerbung zu verbessern, muss bezweifelt werden. Dabei wäre es bitter nötig. Denn würden Ads nicht nerven, tracken oder gar Malware verbreiten, gäbe es keine Adblocker, die eben genau dies verhindern sollen. Weil deren Einsatz die Erlösmodelle kommerzieller Webseiten-Betreiber gefährdet, setzen diese bekanntlich Anti-Adblocker ein, die wiederum von Anti-Adblock-Killern in Form von Skripten entdeckt und umgangen werden können. Dieser Teufelskreis der Werbung ähnelt allmählich einem Wettrüsten der Art, bei der man sich fragen muss, ob Kunden wirklich Könige oder nicht doch eher Kriegsgegner sind.

So wurde vor kurzem der Anti-Adblocker-Anbieter Pagefair Opfer einer Hackerattacke in deren Folge Malware über Kunden-Webseiten wie z.B. der des «Economist» ausgeliefert wurde.

Mitte November wurde bekannt, dass Yahoo Nutzern, die einen Adblocker verwenden, den Zugang zum plattformeigenen E-Mail-Service Yahoo Mail verweigert.

Auch die seit August 2013 zum Amazon-Imperium Jeff Bezos´ gehörende Washington Post hatte in diesem Jahr in einem Test damit geliebäugelt, Lesern, die Adblocker verwenden, nicht alle Artikel zur Verfügung zu stellen.

Zu drastischeren Mitteln griff vor kurzem der deutsche Axel-Springer-Verlag: Er liess auf juristischem Weg einen User abmahnen, der auf YouTube ein Erklärvideo hochgeladen hatte, das zeigte, wie der Anti-Adblocker auf bild.de zu umgehen sei. Dass Springer juristisch gegen Adblocker vorgeht ist nicht neu. Im

September hatte das Medienunternehmen in einem Verfahren vor dem Landgericht Köln gegen den Werbeblocker AdblockPlus den Kürzeren gezogen und dabei viel journalistisches Aufsehen erregt: Die Springer Anwälte hatten nämlich versucht, die Argumentation auszuhebeln, mit der das Landgerichts Hamburg im April 2015 die Zulässigkeit von Adblockern damit begründete, dass das Kerngeschäft von Medien die Vermittlung journalistischer Inhalte sei, und dieses Kerngeschäft nicht von Werbeblockern beeinträchtigt werde. Vor dem Landgericht Köln erklärten die Anwälte nun: "Das Kerngeschäft der Klägerin ist die Vermarktung von Werbung. Journalistische Inhalte sind das Vehikel, um die Aufmerksamkeit des Publikums für die werblichen Inhalte zu erreichen." – bei genauerer Betrachtung ein journalistischer Offenbarungseid, der zeigt, wie schnell sich das Adblocker-Karussell abwärts bewegt.

Einen Ausweg aus dem Dilemma will in Kürze das New Yorker StartUp «Data Arbitrage» in der Form bereitstellen, die «Datenherrschaft» den Usern zurückzugeben. Bis 2019, so das ambitionierte Ziel der Software-Entwickler, soll der Handel mit persönlichen Daten beendet sein. Dazu will Data Arbitrage die Datenpools der Händler mit gefakten Userprofilen und –daten verunreinigen und damit letztlich entwerten. Das System arbeitet mit einer lernenden Software und einem «ArbiBot», der den Account erstellt und mit Nutzerdaten füllt. Die Testphase mit aktuell 30.000 Accounts auf Facebook, Twitter und Instagram hat gezeigt, dass das System damit auch nicht unerheblich Geld verdienen kann – ein Kritikpunkt vieler Interessenten. Ob mit einem solchen Vorgehen die gewünschte Wirkung erzielt werden kann, ist jedoch fraglich, zumal Datenhändler persönliche Profile auch ausserhalb sozialer Netzwerke generieren.

Nachzulesen unter:

http://www.computerworld.com/article/2993382/malware-vulnerabilities/malvertising-is-a-troubling-trend.html
http://www.nzz.ch/digital/pagefair-liess-malware-ausliefern-ld.2870
http://www.sueddeutsche.de/medien/jeff-bezos-zur-uebernahme-der-washington-post-aus-liebe-zur-zeitung-1.2250060
http://www.golem.de/news/adblocker-sperre-bild-de-mahnt-youtuber-wegen-erklaervideo-ab-1510-117011.html
http://www.golem.de/news/adblock-plus-axel-springer-sieht-journalismus-nur-als-vehikel-fuer-werbung-1509-116587.html
http://www.telemedicus.info/urteile/Wettbewerbsrecht/Werbung/1584-LG-Hamburg-Az-416-HKO-15914-Zulaessigkeit-von-Adblockern-mit-Whitelist-Funktion.html
http://futurezone.at/digital-life/mit-falschinformationen-gegen-den-datenhandel/164.969.633
http://t3n.de/news/data-arbitrage-datenhandel-659495

Zum Stöbern: spannende Präsentationen, Artikel und Videos

Die Slides und Whitepaper der diesjährigen BlackHat Europe 2015 sind online verfügbar. Unter anderem mit der Vorstellung eines Metasploitmoduls, dass die Grenzen von LastPass und anderen Passwort-Managern aufzeigt:

https://www.blackhat.com/eu-15/briefings.html

Wieviele Möglichkeiten gibt es, die Nutzer von Webbrowsern zu tracken? Johannes B. Ullrich hat für SANS mal 11 zusammengetragen:

https://isc.sans.edu/forums/diary/11+Ways+To+Track+Your+Moves+When+Using+a+Web+Browser/19369/

Die Situation der IT-Sicherheit in Deutschland 2015 fasst das BSI in seinem aktuellen Lagebericht zusammen:

http://docs.dpaq.de/9977-2015_11_19_bsi_lagebericht_2015.pdf

Bitte sagen Sie uns Ihre Meinung! - Leserbefragung

SWITCH führt eine Leserbefragung über den Security Report durch. Tragen Sie mit Ihrer Meinung zu dessen Weiterentwicklung bei. Mit Ihrer Teilnahme können wir den Security Report besser auf Ihre Bedürfnisse zuschneiden und für Sie noch attraktiver gestalten. Alle Angaben und Antworten werden von uns in anonymisierter Form ausgewertet.

Bitte füllen Sie den Fragebogen bis spätestens Freitag, 18. Dezember 2015 aus. Sie werden dazu etwa 8 bis 10 Minuten Zeit benötigen.

Mit diesen Links gelangen Sie direkt zum Fragebogen:
Deutsch: http://swit.ch/befragung-secrep
Englisch: http://swit.ch/survey-secrep

Falls Sie beim Ausfüllen Fragen haben, zögern Sie bitte nicht, uns zu kontaktieren: roland.eugster@switch.ch.
Wir danken Ihnen herzlich für Ihre Teilnahme!

Dieser SWITCH-CERT Security Report wurde von Dieter Brecheis und Frank Herberg verfasst.