Wikileaks veröffentlicht **beunruhigende** Daten

Bislang wurden Nerds, die die Kameralinse an ihrem Laptop mit einem Klebestreifen zukleistern, ja oft noch mitleidig belächelt … immer diese Paranoiker. Zumindest das sollte sich eigentlich spätestens seit heute ändern.

von Jens Berger

Wie die jüngsten Enthüllungen von Wikileaks belegen[1], verfügt die CIA über zahlreiche Hacker-Techniken, mit denen sie nicht nur traditionelle Software auf Computern infizieren und für ihre Zwecke nutzen kann. Das besondere Interesse der CIA scheint vor allem darin zu bestehen, sogenannte „smarte" Elektronikgeräte in Wanzen und Überwachungskameras umzuwandeln. Dies ist eine neue Eskalationsstufe im Krieg um unsere Privatsphäre.

In Zeiten von Skype, iPhone, Alexa, Siri, Bordcomputern im Auto und internetfähigen Fernsehgeräten, Waschmaschinen und Mikrowellen sind wir von Geräten umgeben, die man mit einem kleinen Hack zu Überwachungstechnik umfunktionieren kann, mit der jeder unserer Schritte, jede unserer Gesten und jedes unserer Worte protokolliert werden kann. Ach ja – nebenbei hat Wikileaks auch veröffentlicht, dass das US-Konsulat in Frankfurt am Main offenbar eine verdeckte Hacker-Basis betreibt. Und wo bleibt der Aufschrei? Keine 12 Stunden nach der Veröffentlichung auf Wikileaks haben die Medien schon wieder auf Alltag umgeschaltet. SPON berichtet von russischen Verschwörungstheorien, die Süddeutsche echauffiert sich über das Frauenbild der „Populisten" und die WELT lobt Ungarns Umgang mit den Flüchtlingen. Anders die NZZ, die sich mächtig aufregt … und zwar über das böse Wikileaks, das sich „erneut in russische Pläne hat einspannen lassen" und „die USA und ihre Verbündeten" attackiert[2]. **Nicht die Verantwortlichen, sondern die Überbringer der schlechten Nachrichten stehen mal wieder im Fokus des medialen Zorns. Wahnsinn.**

Das Smartphone, das gerade eben neben ihnen liegt, könnte theoretisch auch eine sehr smarte Wanze sein. Es hat ein Mikrofon, eine Kamera, einen GPS-Empfänger, es kann ihre Mails und ihre Chatnachrichten lesen, ihre Schritte tracken und ein lückenloses Bewegungsprofil von ihnen erstellen. Über Funk und WLan lassen sich diese Daten auch mühelos auslesen, wenn man denn Zugriff auf die Technik hat. Und Hand aufs Herz – würden sie einen größeren Betrag darauf wetten, dass die US-Dienste keinen Zugriff auf diese Informationen und keinen Zugriff auf die Hardware in ihrem Smartphone haben? Wenn ja, dann schauen Sie sich doch bitte vorher noch einmal die Dokumente von Wikileaks an. Das Apple-Smartphone- und –Tablett-Betriebssystem iOS steht bei der CIA mit zahlreichen Schwachstellen auf der Gerätelist[3], und der große Konkurrent Android sieht mit seinen zahlreichen Zero-Days[4,5], Exploits und weiteren Schwachstellen kaum besser aus. Laut Wikileaks setzt sich das Hacker-Arsenal der CIA dabei sowohl aus Eigenentwicklungen als auch aus Zukäufen und Zulieferungen vom GCHQ, von der NSA, vom FBI oder von privaten Entwicklern von Hacking-Tools zusammen. Und dieses Arsenal ist durchaus beeindruckend. Es ist übrigens davon auszugehen, dass nicht nur das CIA über diese Techniken verfügt. Die NSA dürfte über ein mindestens genau so großes Arsenal verfügen und auch das britische GCHQ wird sicher beim großen Lauschangriff nicht außen vor bleiben.

Es sind dabei keinesfalls „nur" die Smartphones, die bei CIA und Co. auf der Liste der Ziele stehen. Wenig überraschend dürfte sein, dass der Großteil der verfügbaren Tools immer noch auf Software für Windows, Mac OS und Linux basiert – angefangen bei Programmen für die Steuererklärung, über Browser, Mail- und Konferenzprogramme, bis hin zu Spielen, Sicherheits- und Anti-Viren-Lösungen. Überraschender ist da schon, dass auch die Software, die auf einigen Fernsehgeräten und in zahlreichen Autos läuft[6], von der CIA vorsätzlich manipuliert wird. Dass sie in ihrem eigenen Auto von der CIA abgehört werden und die Software ihres Autos (VSEP) auch auf Befehl von CIA-Hackern ihr Auto gegen einen Baum steuern könnte, war bislang nur in Spionage-Thrillern, wie Michael Lüders prophetischen „Never Say Anything"[7] zu lesen. Wenn die Techniken, die Wikileaks in seinem „Vault 7" aufdeckt, wirklich existieren und funktionieren, ist genau dies schon heute möglich.

Im Zentrum der Hacking-Aktivitäten scheint jedoch die smarte Unterhaltungselektronik zu stehen. Über das Projekt „Weeping Angel"[8] hat die CIA eine Software entwickelt, die smarte Fernsehgeräte von Samsung in einen „Fake-Off-Modus" versetzt, dem Nutzer also vorgaukelt, dass das Gerät ausgeschaltet sei. In Wirklichkeit zeichnet Samsungs Fernseher jedoch über die Mikrofone auf, was sie sagen, und kann sie mit den implementierten Kameras, die für Videokonferenzen gedacht sind, auch filmen. Wie war das noch mit der abgeklebten Kamera und der Paranoia?

Genau diese Technik ist es auch, die uns besonders beunruhigen sollte. Und dies aus gleich mehreren Gründen. Zum Einen ist die Updatefrequenz der Software auf smarten Elektrogeräten wesentlich langsamer als auf Computern oder Smartphones. Schwachstellen wie Zero-Days oder Exploits bleiben so mitunter jahrelang erhalten, sodass die Dienste es besonders einfach haben, auf diese Geräte zuzugreifen. Zum Anderen sind derlei smarte kleine Helfer absolut im Trend. Vor allem die Stimmerkennung gilt als eine Zukunftstechnik mit großem Potential. Was heute als Siri, Alexa, Google Assistant oder Cortana auch bereits auf TV-Boxen, Fernbedienungen, Lautsprechern und anderen Home-Elektronik-Geräten läuft, wird schon bald in unzählige Geräte des Alltags implementiert sein. Ein Albtraum für Datenschützer, ein Traum für Hacker im Dienst der Dienste.

Das absolute Albtraum-Szenario, bei dem die Dienste ohne großen Aufwand in jedem Auto, jedem Gebäude und via Smartphone sogar in der freien Wildnis jeden Menschen nach freiem Belieben abhören können, ist vielleicht gar nicht mehr so weit und in einzelnen Fällen sicher bereits Realität. Die Wikileaks-Enthüllungen gehen jedoch noch einen Schritt weiter. Nach Aussagen ehemaliger CIA-Mitarbeiter zeigen die Dokumente auch auf, dass die Software in der Lage ist, falsche Fährten zu legen[9]. „Wenn man einen Cyberangriff durchführt, möchte man nicht, dass draufsteht ‚Made

in USA“, so der ehemalige CIA-Arbeiter Philipp Mudd gegenüber tagesschau.de. Die ARD-Nachrichtenmacher lassen dieses Zitat so im Raum stehen. Was aber bedeutet diese – nicht unbedingt neue – Erkenntnis im Kontext zur aktuellen Debatte rund um die angeblichen Hacking-Aktivitäten der Russen? Wir befinden uns offenbar noch ganz am Anfang einer viel größeren Debatte über digitale Forensik und die Unmöglichkeit, digitale Beweise abseits der allmächtigen Geheimdienste zu bewerten.

Dass es wieder einmal einen US-Dienst „erwischt“ hat, ist natürlich kein Zufall. Mit Sicherheit versuchen auch französische, deutsche, russische, chinesische, indische oder albanische Dienste an derlei Techniken zu kommen … offenbar sind die USA da aber tatsächlich eine Klasse für sich, was freilich auch etwas mit den unglaublichen Mitteln zu tun hat, die den US-Diensten zur Verfügung stehen.

Wieder einmal sind die Amerikaner erwischt worden; wieder einmal hält sich der Protest in Deutschland in sehr überschaubaren Grenzen. Dabei hat Wikileaks als kleines Schmankerl doch sogar die zweite CIA-Hacker-Zentrale, neben Langley/Virgina offenbart – und die liegt in der Gießener Straße in Frankfurt am Main, in einem Areal des US-Konsulats, das offenbar als „Sensitive Compartmented Information Facility“ (SCIF) bezeichnet wird. **Die CIA spioniert also von Frankfurt aus. Interessant. Und wen spioniert man wo mit welcher Begründung aus? Ist das demokratisch legitimiert? Und juristisch? Fragen über Fragen … Fragen, die nicht gestellt werden und daher auch nicht beantwortet werden müssen.** Denn vor allem die deutsche Regierung ist bei den Spionage-Aktivitäten der US-Dienste ja schon traditionell desinteressiert. Warum sollte das auch anders sein? Die Medien interessieren sich für solche Dinge ohnehin nur am Rande und in zwei Tagen ist der Spuk ohnehin vorbei und auch „das Netz“ treibt dann schon wieder die nächste Sau durchs Dorf. Erdogan? Trump? Oder diesmal Bernd Höcke? Irgendwer wird sich schon finden, der den nächsten Shitstorm auslöst und das Thema CIA endgültig von der Agenda verdrängt.

Wäre es nicht die CIA, sondern der FSB gewesen … ja dann sähe die Sache freilich anders aus. Dann hätten wir schon gestern einen ARD-Brennpunkt gehabt und alle Zeitungen würden Zeter und Mordio schreien. Dann gäbe es sicher auch schon morgen einen nationalen Sicherheitsplan zur Cyber-Abwehr und die SPIEGEL-Grafiker würden sich schon mal an den Entwurf eines lauschenden Russen machen, der in unserem Wohnzimmer sitzt und auf dem nächsten Cover des SPIEGEL verewigt werden soll.

Ja, ja, die Russen. Können Sie sich eigentlich noch an den „großen Hackerangriff“ auf die Telekom im November letzten Jahres erinnern? Der Angriff, der laut Medien mit den „Machenschaften russischer Gruppierungen“[10] in Verbindung stehen soll? Der Hauptverdächtige sitzt seit zwei Wochen in Großbritannien in Untersuchungshaft[11]. Es ist ein britischer Staatsbürger … kein Wunder, dass sie von dieser Meldung sicher noch nichts gehört haben. Auch die aktuellen Enthüllungen von Wikileaks werden sicher sehr schnell in Vergessenheit geraten.

Quellen:

[1] **Wikileaks.org, Vault 7:** CIA Hacking Tools Revealed‘ ‹https://wikileaks.org/ciav7p1/›

[2] **Nzz.ch, Neue Attacke** von Wikileaks gegen die USA ‹https://www.nzz.ch/international/wikileaks-enthuellungen-mutmassliche-cia-spionage-im-cyberspace-aufgedeckt-ld.149780›

[3] **Wikileaks.org, Vault 7:** CIA Hacking Tools Revealed ‹https://wikileaks.org/ciav7p1/cms/space_2359301.html›

[4] **Wikileaks.org, Vault 7:** CIA Hacking Tools Revealed ‹https://wikileaks.org/ciav7p1/cms/space_11763721.html› und ‹https://wikileaks.org/ciav7p1/cms/page_11629096.html›

[5] **Wikileaks.org, Vault 7:** CIA Hacking Tools Revealed ‹https://wikileaks.org/ciav7p1/cms/page_11629096.html›

[6] **Wikileaks.org, Vault 7:** CIA Hacking Tools Revealed ‹https://wikileaks.org/ciav7p1/cms/page_13763790.html›

[7] **Chbeck.de, Never Say** Anything ‹http://www.chbeck.de/Lueders-Never-Say-Anything/productview.aspx?product=16011169›

[8] **Wikileaks.org, Vault 7:** CIA Hacking Tools Revealed ‹https://wikileaks.org/ciav7p1/cms/page_12353643.html›

[9] **Tagesschau.de, Zwischen Schweigen** und Schäumen ‹https://www.tagesschau.de/ausland/wikileaks-117.html›

[10] **Tagesspiegel.de, Was passiert** ist, wer dahinter steckt, was Kunden tun können ‹http://www.tagesspiegel.de/politik/hackerangriff-auf-die-telekom-was-passiert-ist-wer-dahinter-steckt-was-kunden-tun-koennen/14906320.html›

[11] **Focus.de, Britische Ermittler** verhaften Verdächtigen in London ‹http://www.focus.de/digital/internet/drei-monate-nach-hacker-angriff-britische-ermittler-nehmen-mutmasslichen-telekom-hacker-in-london-fest_id_6693033.html›

Autor:

Jens Berger

ist freier Journalist, Wirtschaftsexperte und politischer Blogger der ersten Stunde. Als Redakteur der NachDenkSeiten und Herausgeber des Blogs Der Spiegelfechter schreibt er regelmäßig zu sozial-, wirtschafts- und finanzpolitischen Themen.

Dieser Text wurde zuerst am 08.03.2017 auf den Nachdenkseiten unter der URL ‹http://www.nachdenkseiten.de/?p=37327/› veröffentlicht. (Lizenz: Nachdenkseiten)

‹http://www.free21.org/?p=26951›

Publiziert auf Free21 am 17.03.2017, 12:30 Uhr, von Jens Berger auf nachdenkseiten.de (Lizenz: CC BY-SA 3.0)