des ADC bereit und lässt sich durch Software auslesen. Software sortiert auch in die Kanäle.

Um die beiden Karten anzusteuern, nutzen wir ein 6502 Assembler-Programm. Eine Inspektion verläuft in vier Schritten: Zunächst wird die Hochspannung eingeschaltet, dann ein Gammaspektrum des Templates aufgenommen. Anschließend kann ein Gammaspektrum eines zu inspizierenden Objekts aufgenommen werden. Im letzten Schritt werden beide Spektren verglichen. Für diesen Vergleich werden die Daten der Spektren in je nur 12 Kanäle zusammengefasst. Die resultierenden Verteilungen werden dann mit einem Chi-Quadrat-Test verglichen. Ist das Resultat kleiner als ein Schwellwert, wird von einer Ähnlichkeit ausgegangen, der V
ten ist er nicht erfolgreich. Das je
am Bildschirm oder über Leuchtd
ren beeinflussen die erzielbare Z
(dauert etwa 10–15 µs), Digitalisierung (10–15 µs) und Verarbeitung mit 6502 (35–50µs). Nach maximal 100 µs ist das Signal aufgenommen, vom 6502 verarbeitet und in den Speicher geschrieben. Theoretisch sind mit der IBX II also bis zu 10 000 Ereignisse pro Sekunde messbar. Typischerweise betreiben wir die IBX II in einem Bereich von 2000 Ereignissen pro Sekunde. Ein Spektrum kann in 1-2 Minuten aufgenommen werden.

Als Teil des Entwicklungsprozesses haben wir zu Testzwecken einen existierenden Apple II Emulator (LinApple) so erweitert, dass er auch die Funktion der beiden Erweiterungskarten enthält. Damit konnten Programmentwicklung und -tests an einem modernen Rechner durchgeführt werden. Interessierte, die unsere Arbeit testen wollen, aber nicht über die notwendige Hardware verfügen, bietet der Emulator einen guten Startpunkt (siehe Endnote 2).

Durch Entwicklung und Test der beiden Erweiterungskarten konnten wir zeigen, dass die Idee, alte Hardware zu benutzen, grundsätzlich funktionieren kann. Bisher noch als Erweiterungskarten im selbst relativ komplexen Apple IIe lässt sich ein ähnliches Design in Zukunft auch auf ein einfacheres 6502-basiertes System anpassen. So ist eine Informationsbarriere vorstellbar, die neben der Hardware der Erweiterungskarten nur einen 6502, etwas ROM für die Software und ausreichend RAM für das Template enthält. Weitere Schritte in Zukunft sind eine Optimierung
her auch der entwickelten Hard-
cht werden, möglichst verschie-
nen Alter bzw. Authentizität des
nachgewiesen werden können.
Methoden, etwa Röntgenmikroskopie, und destruktive Methoden vorstellbar. Gerne nehmen wir Ideen und Hinweise von anderen auf. Auch wenn noch einige Schritte zu tun sind, hoffen wir, dass unser hier vorgestelltes Projekt ein kleiner Beitrag auf dem Weg zu einer kernwaffenfreien Welt ist.

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

Anmerkungen

1 *Inhalte dieses Artikels wurden auf dem 34c3 vorgetragen.*
2 *Software, Hardware Design und modifizierter Emulator verfügbar unter www.vintageverification.org*
3 *visual6502.org*
4 *monster6502.com*

FIfF e. V. – Pressemitteilung

FIfF-Sachverständigenauskunft zum Trojanereinsatz durch den hessischen Verfassungsschutz

FIfF lehnt Hessentrojaner ab

7. Februar 2018 – Am 8. Februar 2018 findet eine öffentliche mündliche Anhörung des hessischen Innenausschusses zum Gesetzentwurf der Fraktionen von CDU und Bündnis 90/Die Grünen für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen (HVSG) statt. Weil dem hessischen Verfassungsschutz innerhalb dieser Gesetzesnovelle auch der Einsatz von Trojanern in Form von verdeckter Quellen-TKÜ und geheimer Online-Durchsuchung erlaubt werden soll, ist das FIfF als Sachverständiger eingeladen worden. Wir empfehlen dringend, die Quellen-TKÜ und die heimliche Online-Durchsuchung ersatzlos zu streichen.

Einleitung

Geheimdienste, also staatliche Behörden, die wesentlich auf verdeckte Maßnahmen, Tarnoperationen, „Vertrauensleute“ oder verdeckte MitarbeiterInnen setzen, sind inhärent auf Intransparenz angelegt und angewiesen, da Heimlichkeit das primäre Mittel ist, die ihnen übertragenen Aufgaben auszufüllen. Ermächtigungen derartiger Dienste müssen folglich besonders kritisch analysiert werden, da einmal freigegebene Maßnahmen und ermöglichte Methoden meist nur nach Skandalen erneut zur breiten Diskussion gestellt werden (können).

Auch wenn sich die Aufgabenbereiche von Polizeien und Geheimdiensten mittlerweile gefährlich überlappen, sind dennoch die Berichts- und Transparenzpflichten von polizeilichen Behörden – im Gegensatz zu verdeckt tätigen Organisationen – zumindest grundsätzlich auf Offenheit angelegt. Wegen dieses gewichtigen Unterschieds gehen die rechtfertigenden Referenzen des Gesetzentwurfs bezüglich der Entscheidung des Bundesverfassungsgerichts zum BKA-Gesetz natürlich prinzipiell fehl. **Ein Geheimdienst ist keine Polizei und eine Polizei ist kein Geheimdienst.**

Der aktuelle Vorstoß, Geheimdiensten wie dem Verfassungsschutz die Ermächtigung zu geben, informationstechnische Systeme zu infiltrieren, ist in einen stetigen, sehr beunruhigenden Trend einzuordnen: den schrittweisen Ausbau von informationstechnischen Offensivfähigkeiten der Behörden im Sicherheitsbereich. Der Bundesnachrichtendienst (BND) hat mit seiner 300 Millionen Euro teuren *Strategischen Initiative Technik* die Fähigkeiten bekommen, technische Systeme verdeckt und offen angreifen können[1]. Aber auch die Bundeswehr wurde durch die *Strategische Leitlinie Cyber-Verteidigung* aufgerüstet, die explizit – anders als der Name impliziert – auch „offensive Cyber-Fähigkeiten" als *Wirkmittel* vorsieht.[2]

Es werden also viele hundert Millionen Euro in geheime IT-Angriffsstrategien investiert; doch beispielsweise für das *Nationale Referenzprojekt zur IT-Sicherheit in Industrie 4.0*[3] – die digitale Absicherung der Zukunft der deutschen Industrie – gibt es nur eine Finanzierung von 33 Millionen Euro; ein klares Missverhältnis. **Wir halten diese primäre Offensivausrichtung für die schlechteste aller Digitalisierungsstrategien.**

Gewährleistung der Vertraulichkeit und Integrität unserer Infrastruktur

Wenn wir von einer vernetzten Gesellschaft mit *Cloud, Industrie 4.0, Internet of Things* und *smarten* Infrastrukturen sprechen wollen, so muss immer auch die damit einhergehende gegenseitige Abhängigkeit und Verwundbarkeit mitgedacht werden. Wird also ein Hersteller oder Softwareprodukt durch bestimmte Maßnahmen und Regelungen geschützt, werden parallel dazu auch die anderswo eingesetzten Systeme, NutzerInnen und Nutzungsarten mitgeschützt. Im Gegenzug bedeutet dies jedoch auch, dass Schädigungen oder Schwächungen von bestimmten Softwarekomponenten gleichermaßen auch alle anderen Einsatzweisen schwächt und unsicherer macht. Aus diesem Grunde war es beispielsweise möglich, dass die Schadsoftware *Wannacry* sowohl private Laptops als auch ganze Krankenhaus-, Eisenbahn- und Providersysteme lahmlegen konnte.[4]

Nun nutzen alle Formen staatlichen Hackings, wie etwa die verdeckte Quellen-TKÜ oder die geheime Online-Durchsuchung – bekannte oder unbekannte – Sicherheitslücken. Doch woher kommen diese und was hat die Nutzung für Auswirkungen auf die allgemeine (IT-)Sicherheit?

Analyse der Kollateralschäden

Üblicherweise sind gerade staatliche Akteure im Sicherheitsbereich finanziell gut ausgestattet und können Sicherheitslücken am weltweiten Schwarzmarkt erwerben. Doch dadurch werden diese Unsicherheits-Märkte ganz wesentlich erzeugt, vergrößert und fatalerweise sogar demokratisch legitimiert. Gefundene Lücken werden nun zunehmend nicht mehr an Hersteller gemeldet, sondern auf den Märkten an die Meistbietenden versteigert. **In der Folge wird die gesamte IT-Infrastruktur unsicherer, da die Lücken natürlich auch Kriminellen, nicht befreundeten und auch „befreundeten" Staaten offenstehen.**

Üblicherweise verkaufen diese Sicherheitslücken-Händler ihre toxische Ware auch nicht nur an demokratische Staaten, wie man an der aktuell vom Bundeskriminalamt (BKA) beauftragten[5] deutschen Firma *Gamma/FinFisher* sehen kann. Deren Software *FinSpy* wurde damals auch von bahrainischen Behörden genutzt, um DissidentInnen zu verfolgen und den Arabischen Frühling niederzuschlagen.[6] Weitere Kunden der Firma sind Behörden in Diktaturen wie Dubai oder Katar.[7] Dabei werden auch diese Firmen immer wieder gehackt und dann deren Software, Sicherheitslücken und interne Dokumente veröffentlicht.[8]

Das ist der aktuelle katastrophale Zustand der weltweiten IT-Sicherheit. Und deutsche Behörden wollen nun weiter mithelfen, diesen Status quo zu noch weiter zu verschlechtern. Wir halten das für inakzeptabel. Das wohl bekannteste Beispiel für den Irrweg, Lücken zu behalten, war sicherlich der oben schon erwähnte Erpresserwurm *Wannacry.* Er infiltrierte weltweit zehntausende Systeme und nutzte dafür Sicherheitslücken, die der US-Geheimdienst NSA seit Jahren für eine spätere Verwendung aufgehoben hatte – und das trotz diesbezüglicher, interner Risikoabwägungsmechanismen.[9]

In der wohlwollenden Interpretation unterstützen deutsche Behörden mit Steuergeldern also schäbige Geschäftsmodelle. **In der besorgniserregenderen Deutung finanzieren deutsche Behörden Firmen, die direkt oder indirekt an der Verfolgung von DissidentInnen und MenschenrechtsverteidigerInnen in Diktaturen beteiligt sind.** Unsere Freunde von *Amnesty International* können schon jetzt vom bitteren „Erfolg" dieser Strategie berichten.[10]

Kurzum, wenn es tatsächlich um Sicherheit gehen soll, so muss die Suche nach Sicherheitslücken strukturiert, koordiniert und konsequent angegangen werden, ohne Ausnahme. Die globalisiert-vernetzte Informationsgesellschaft bedeutet mittlerweile eben auch: **Es gibt keine öffentliche Sicherheit mehr ohne IT-Sicherheit.**

Wieder *Terrorismus* als Begründung

Im Gesetzesentwurf gibt es mehrere konkrete Erwähnungen des NSU- und internationalen Terrorismus als Begründung. Der Terror soll nun noch entschlossener bekämpft werden, auch durch staatliches Hacking. Drei Beispiele aus der aktuellen Terror-Debatte seien hier einmal kurz kommentiert:

1. Gerade im skandalösen Fall des NSU und seiner (Nicht-) Aufklärung waren fehlende QKTÜ/OD-Fähigkeiten sicherlich das kleinste Problem im ganzen Debakel.[11]

2. Im Fall der rechtsextremen Oldschool Society (OSS), weitläufig bekannt durch den strittigen Telegram-Zugriff durch das BKA, waren die so erlangten Informationen vor dem Münchner Oberlandesgericht für die Verurteilung letztlich gar nicht verwendet worden.[12]

3. Der weltweit berühmte Fall um die San-Bernadino-Bomber und ihr verschlüsseltes iPhone machte zwar gute Schlagzeilen für Apple, basierte jedoch auf einem Password-Reset-Fehler der Ermittler, der dann erst den extrem teuren Hack

nötig machte. Das Öffnen des iPhones brachte im Übrigen gar keine nützlichen Informationen hervor.[13]

Insgesamt sehen wir die Begründung der neuen IT-Befugnisse in Bezug auf die im Entwurf benannten terroristischen Ereignisse also höchst kritisch. Auch wenn der Zweck *Terrorismusbekämpfung* die volle Unterstützung verdient, schießen die technischen Infiltrationsbefugnisse doch über das Ziel hinaus. Gerade bei den im Entwurf genannten Ereignissen lohnt es sich, detailliert zu durchdenken, inwiefern eine QTKÜ/OD jeweils hilfreich und zwingend notwendig gewesen wäre. Denn in einigen Fällen waren die Täter schon vorher bekannt und etwa der Anschlag am Breitscheidplatz in Berlin wurde offenbar sogar mit Involvierung von V-Leuten durchgeführt.[14] Gleiches gilt für den NSU-Fall um Andreas Temme.

Kurzzusammenfassung unserer Position zum vorliegenden Gesetzentwurf

- Speziell die Paragraphen § 6 (Quellen-TKÜ) und § 8 (Online-Durchsuchung) beziehen sich auf eine technische Ermächtigung, mit der ein informationstechnisches System infiltriert werden kann. Welche Daten letztendlich ausgeleitet werden – Kommunikation oder nicht –, ist technisch nicht automatisiert unterscheidbar und dementsprechend auch nicht sinnvoll einzuhegen. Quellen-TKÜ und OD müssen daher die gleichen Eingriffshürden und Berichtspflichten haben.

- Des weiteren gibt es technisch begründet wesentliche Zweifel an einer vertrauenswürdigen Protokollierbarkeit der Aktivitäten und Funde einer Quellen-TKÜ/OD auf einem infiltrierten Zielsystem. Die technischen Grundvoraussetzungen für verlässliches Logging und Signierung sind auf einem fremden System nicht gegeben. Eine detaillierte Dokumentation jedes Zugriffs, mindestens in Form von kompletter Quellcodevorlage und -Auditierung, ist ebenso nötig wie die rechtliche Eingrenzung auf bestimmte Zielsystemarten.

- Die heimliche Installation einer Quellen-TKÜ/OD-Software verlangt die Nutzung von Sicherheitslücken. Die dadurch entstehenden Anreize für Dritte, Sicherheitslücken nicht mehr zu melden, sondern zu verkaufen oder derartige Dienste anzubieten, schadet der allgemeinen IT-Sicherheit weltweit. Das greift langfristig die Grundlagen der vernetzten Gesellschaft an und korrodiert die digitale Infrastruktur. Zusätzlich vertreiben diese Dritten die gleichen Sicherheitslücken üblicherweise auch an Diktaturen weltweit, die damit ihre BürgerInnen kontrollieren, DissidentInnen sowie MenschenrechtsverteidigerInnen ausspähen und verfolgen. Um auf eine sichere und menschenfreundliche IT-Landschaft hinzuwirken, dürfen keine Sicherheitslücken verwendet, gehandelt oder zurückgehalten werden – insbesondere keine bislang unbekannten Lücken.

- Die These eines „Blindwerdens von Behörden“ durch Kryptographienutzung (*Going dark*) lässt sich nicht erhärten, physische Interaktionen von Kriminellen und allgemeine Effekte der Digitalisierung bieten nach wie vor hinreichende Ansatzpunkte für eine effektive Gefahrenabwehr.

- Der Verfassungsschutz ist ein Geheimdienst und per Definition ungleich intransparenter und schwerer demokratisch zu kontrollieren als etwa Polizeien. Derartig eingriffstiefe und folgenschwere Ermächtigungen wie § 6 und § 8 dürfen ihm demnach grundsätzlich nicht erteilt werden.

In der Konsequenz raten wir nachdrücklich dazu, die Paragraphen § 6 (Quellen-TKÜ) und § 8 (Online-Durchsuchung) ersatzlos zu streichen.

Material

FIfF-Sachverständigenauskunft, (PDF, 19 Seiten) https://www.fiff.de/presse/pressemitteilungen/FIfF_Stellungnahme_HVSG_Hessentrojaner.pdf

Gesetzentwurf zum Hessischen Verfassungsschutzgesetz, Drucksache 19/5412 (PDF, 57 Seiten)
http://starweb.hessen.de/cache/DRS/19/2/05412.pdf

Webseite der öffentlichen Anhörung im Innenausschuss
https://hessischer-landtag.de/node/2490

Webseite des kritischen Projekts Hessentrojaner (wir sind Unterstützer)
https://www.hessentrojaner.de

Abendveranstaltung bzw. Morgenkundgebung am 7.2. bzw. 8.2.2018
https://www.hessentrojaner.de/aufruf/

FIfF-Pressemitteilung zum Trojanereinsatz laut Strafprozessordnung (StPO)
https://www.fiff.de/presse/pressemitteilungen/entfesselter-trojaner-grosse-koalition-verhoehnt-it-sicherheit-und-demokratie

Referenzen

1 *https://netzpolitik.org/2015/strategische-initiative-technik-wir-enthuellen-wie-der-bnd-fuer-300-millionen-euro-seine-technik-aufruesten-will/*
2 *http://www.spiegel.de/politik/deutschland/bundeswehr-ursula-von-der-leyen-ruestet-an-der-cyber-front-auf-a-1042985.html*
3 *https://www.dfki.de/web/forschung/projekte?pid=945*
4 *https://www.heise.de/newsticker/meldung/WannaCry-Angriff-mit-Ransomware-legt-weltweit-Zehntausende-Rechner-lahm-3713235.html*
5 *https://netzpolitik.org/2017/geheimes-dokument-das-bka-will-schon-dieses-jahr-messenger-apps-wie-whatsapp-hacken/*
6 *https://netzpolitik.org/2014/gamma-finfisher-ueberwachungstechnologie-made-in-germany-gegen-arabischen-fruehling-in-bahrain-eingesetzt/*
7 *https://netzpolitik.org/2012/gamma-finfisher-neue-analyse-des-staatstrojaners-deutet-auf-weitere-kunden-hin/*
8 *https://netzpolitik.org/2014/gamma-finfisher-gehackt-werbe-videos-von-exploits-und-quelltext-von-finfly-web-veroeffentlicht/*
9 *https://www.wired.com/story/vulnerability-equity-process-charter-transparency-concerns/*
10 *https://www.amnesty.org/en/get-involved/take-action/free-ahmed-mansoor/*
11 *https://www.blaetter.de/archiv/jahrgaenge/2018/januar/von-aufklaerung-keine-spur-20-jahre-nsu-komplex*
12 *https://netzpolitik.org/2016/bundeskriminalamt-knackt-telegram-accounts/*
13 *https://www.washingtonpost.com/world/national-security/comey-defends-fbis-purchase-of-iphone-hacking-tool/2016/05/11/ce7eae54-1616-11e6-924d-838753295f9a_story.html*
14 *https://www.rbb24.de/politik/beitrag/2017/10/amri-von-v-mann-angestachelt-anschlag-berlin-breitscheidplatz.html*