FIfF-Konferenz 2014

Der Fall des Geheimen – Ein Blick unter den eigenen Teppich

Wir haben die Rolle Deutschlands und der deutschen Geheimdienste im Kontext der älteren und jüngeren Erkenntnisse – von Echelon über Prism bis Eikonal – zusammen mit rund 400 Besucherinnen und Besuchern beleuchtet und Handlungsoptionen erarbeitet. Natürlich muss die Bearbeitung nun weitergehen.

Am 7. und 8. November 2014 lud das FIfF – Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung – zur FIfF-Konferenz 2014 ein. Dabei warfen wir den längst überfälligen Blick unter Deutschlands eigenen Geheimdienst-Teppich, denn spätestens nach den jüngsten Enthüllungen zur Rolle Deutschlands im globalen Geheimdienstroulette ist es absurd, nur mit dem Finger über den Atlantik oder auf die Britischen Inseln zu zeigen. Insbesondere Deutschland agiert willentlich als Dreh- und Angelpunkt globaler geheimdienstlicher Aktivitäten und treibt die flächendeckende Überwachung voran.

Wir wollten die Rolle der deutschen Geheimdienste beschreiben und verstehen, wie die Überwachungssysteme gebaut sind, nach welchen Menschen- und Weltbildern sie konzipiert und in welchen Kontexten sie verwendet werden. Mit Experten, Betroffenen, Politikern und der Öffentlichkeit wurden technische, politische, rechtliche, wirtschaftliche und historische Aspekte betrachtet – von Echelon über Prism bis Eikonal. Die Zusammenarbeit von Geheimdiensten, deutschen Telekommunikationsanbietern und Technikern bedarf der besonderen Aufmerksamkeit.

Nötig ist der Blick unter den eigenen Teppich auch, weil die deutsche parlamentarische Aufklärungsarbeit zu den Machenschaften von NSA, GCHQ, BND und Co. nur schleppend vorankommt und angesichts der systematischen Missachtung von Menschenrechten und Grundrechten durch die deutschen Geheimdienste halbherzig wirkt. Zudem sabotiert die Bundesregierung das parlamentarische Unterfangen absichtsvoll und maßgeblich: Sei es durch fast durchgehend geschwärzte oder gänzlich zurückgehaltene Dokumente, durch die Verhinderung von Zeugenvernehmungen oder durch monatelange Verzögerungen. Die Regierung und ihre Geheimdienste haben offenbar aktiv vergessen, dass sie eigentlich vom Parlament kontrolliert werden sollten und nicht andersherum.

Ute Bernhardt, Matthias Bäcker, Wolfgang Coy, Hans-Jörg Kreowski, Constanze Kurz, Wolfgang Nešković, Frank Rieger, Anne Roth, Ingo Ruhmann, Peter Schaar, Erich Schmidt-Eenboom, Patrick Sensburg, Hans-Christian Ströbele, Gregor Wiedemann und Andy Müller-Maguhn trugen mit ihren Vorträgen zum Gelingen der Konferenz bei. Das *Nö-Theater* führte am Samstagabend das Stück *V wie Verfassungsschutz* auf.

Auf den folgenden Seiten dokumentieren wir die Beiträge unserer Referentinnen und Referenten zur Konferenz. Dazu haben wir ihre Vorträge zusammengefasst. Natürlich gilt wie immer das gesprochene Wort: Alle Vorträge wurden aufgezeichnet und sind über die Konferenz-Web-Seite *https://fiffkon.de* unter *https://fiffkon.de/medien.html* zugänglich.

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

wurden und werden. Ziele, die die USA in Deutschland inhaltlich verfolgen, sind *Cyber Attack, Counterespionage, emerging strategic technologies, international trade policy, arms export, arms control and treaty monitoring, foreign policy objectives, economic and financial stability* (Cyber-Angriffe, Auslandsspionage, neue strategische Technik, Außenhandelspolitik, Rüstungsexport, Rüstungskontrolle und Vertragskontrolle, Außenpolitik, Wirtschafts- und Finanzstabilität). Wie auch für andere mitteleuropäische Länder geht aus dieser Aufzählung hervor, dass es überhaupt nicht, wie immer wieder behauptet, um Terrorismus geht!

Hackende Geheimdienste

Die Veröffentlichungen zu *Taylored-Access*-Operationen, die automatisierte Infiltration und Schwächung von kryptographischen Methoden, machen deutli… wachung geht, sondern um off… formationen darüber sind in der … Deutlich wird, dass Firmen wie C… zwungene Maß hinaus mit den … beiten.

RSA und Cisco, die ebenfalls eng mit den Diensten zusammenarbeiteten, erlitten nach den Veröffentlichungen einen entscheidenden Imageverlust und Gewinneinbrüche – vor allem im Ausland. US-Firmen merken nun immer mehr, wie wichtig Sicherheitsaspekte wie z. B. Verschlüsselung sind.

Erfolge der NSA-Überwachung

Präsident Obama setzte im letzten Jahr eine Expertenkommission ein, die prüfen sollte, wie die Erfolge der massenhaften Überwachung einzuschätzen sind. Obwohl die Kommission fast nur aus Geheimdienstlern besteht, wofür sie stark kritisiert wurde, ist der veröffentlichte Bericht sehr bemerkenswert. Nicht nur, weil empfohlen wurde, die Manipulation der Finanzmärkte durch Geheimdienste rechtlich zu regulieren (worüber noch gar nichts veröffentlicht worden war), sondern vor allem, weil die Experten sich mit dem Terrorargument beschäftigten. Es wurde zu Protokoll gegeben, dass die massenhafte Metadatenanalyse nur einen bescheidenen Beitrag für die nationale Sicherheit leistet. Es hätte keinen einzigen Fall gegeben, bei dem die NSA mit Sicherheit sagen könnte, dass das Ergebnis einer Untersuchung zu Terror auf irgendeine Art anders gewesen wäre, wenn keine Metadaten zur Verfügung gestanden hätten. Sie konnten also keinen einzigen Fall anführen, um die zentrale Argumentation für diesen riesenhaften Geheimdienstkomplex zu begründen. In Anbetracht der Gelder, die den Diensten zur Verfügung stehen, haben diese stark an Legitimation verloren.

…sümee

…eine gute Chance, die Geheim… …fentlich geäußerte Kritik, sondern … …ele juristische Prozesse laufen bereits. Constanze Kurz selbst ist Beschwerdeführerin vor dem Europäischen Gerichtshof für Menschenrechte, der die Wichtigkeit erkannt hat und sogar ein Schnellverfahren einleitete. Der *Chaos Computer Club* begab sich außerdem in Großbritannien vor das IPT *(Investigatory Powers Tribunal)* – die innerbritische Geheimdienstkontrolle. Auch in Frankreich und Ungarn laufen Verfahren.

Constanze Kurz zieht ein sehr positives Resümee aus den vergangenen zwei Jahren: „Die Chance, durch Snowden über die Geheimdienstaktivitäten Bescheid zu wissen, ermöglicht es uns, ein informiertes Urteil zu treffen und uns gegen diesen Komplex zu wehren – was wir auch tun sollten. Die Dienste sind nicht sankrosankt. Wir bezahlen sie, also können wir das auch beenden – wir müssen nur einen langen Atem haben."

FIfF-Konferenz 2014

Nachrichtendienstliche Zugriffe und ihre Auswirkungen auf digitale Souveränität

Zusammenfassung des Vortrags von Andy Müller-Maguhn

Zu Beginn erfolgte eine kurze Bestandsaufnahme mit der Entwicklung, dass Paranoia nun durch Gewissheit abgelöst wurde und weitgehende Telekommunikationsüberwachung existiert. Ebenso aber auch freier Informationsfluss, Anonymisierungs- und Verschlüsselungswerkzeuge, welche im Falle der Snowden-Evakuierung ihre Wirkkraft gezeigt haben. Die Politik war darüber freilich nicht erfreut, und gerade die erzwungene Landung der Morales-Maschine unter dem Verdacht, Snowden zu transportieren, war ein Vorfall, dessen Gewicht besonders betont wurde.

Nachrichtendienstliche Arbeit ist unterteilbar nach Überwachungsart. Das Anzapfen von Glasfaserkabeln fällt unter *Global Access Operations*; *Special Collection Service* und HUMINT (*human intelligence*) finden auch mit der CIA statt und enthalten Angriffe wie Verwanzungen; unter *Cryptoanalysis and Exploitation Services* können die Programme gefasst werden, welche darauf abzielen, Verschlüsselung zu brechen (BULLRUN, GENIE, TURBINE, TURMOIL, QUANTUM) oder Datenzugriff zu ermöglichen (PRISM, MARINA, MAINWAY, PINWALE, NUCLEON). Die Betrachtung der *Tailored Access Operations* in dieser unvollständigen Liste macht deutlich, dass auch sie nicht nur Auswirkung auf handverlesene Personenziele haben. Denn durch den Fingerabdruck, den unsere Systeme unaufgefordert anderen mitteilen, sind einerseits automatische Angriffe praktikabel, andererseits bedeutet die Kompromittierung des TK-Anbieters Belgacom neben Zugriff auf Finanztransaktionsdaten per SWIFT und Infrastruktur des Europäischen Parlaments auch Ein-

griffsmöglichkeiten in den Flugverkehr, der auf korrekte Daten der Bodenstellen angewiesen ist.

Dass Provider statt des kürzesten den billigsten Weg für Daten wählen, erlaubt es staatlichen Stellen, ihren Machtbereich durch Subventionen auszuweiten, sodass mehr Verkehr durch ihr Zugriffsgebiet läuft. Weniger implizit ist die Installation von über 50.000 fernsteuerbaren Implantaten in Stellen anderer Staaten, von denen auf einer NSA-Folie berichtet wird. Gar an Allmachtsphantasien stößt das Programm TREASUREMAP, mit dem Endgeräte im Internet in Echtzeit inklusive verknüpfter Informationen visualisiert werden.

Doch auch auf andere Staaten wurde der Blick gelenkt. *Lawful Interception*, das Abgreifen der Daten direkt bei den Betreibern, geschieht ohne deren Wissen – da sie sonst Hinweise an das Opfer geben könnten –, und vor allem sind diese Systeme frei konfigurierbar. Durch die breite Einführung in den verschiedenen Ländern ergibt sich als Unterschied, egal ob Monarchie, Faschismus oder parlamentarische Demokratie, nur noch die Konfigurationsdatei. Die Grundlagen sind schon vorhanden und somit wurde vor der Gefahr einer intensiveren Nutzung unter anderen politischen Rahmenbedingungen gewarnt.

Anbieter von Überwachungstechnologie werben damit, erst einmal alles zu speichern und später die genaueren Kriterien der Durchmusterung zu setzen. Sie spezialisieren sich darauf, auch in rechtlich eingeschränkten Umgebungen kreative Dienstleistungen zu finden, wie es bei der Kurzumleitung in ein Rechenzentrum hinter der Grenze geschieht, um Abhörbefugnisse für Auslandskommunikation zu erreichen.

Angesichts der Souveränitätsverletzungen persönlicher und staatlicher Art muss jedoch die aus den Snowden-Dokumenten fokussierte Sicht auf die Beschafferebene geweitet werden hin zu der Fragestellung, warum und für wen all dies getan wird. Die NSA arbeitet nicht zum Selbstzweck, sondern für eine lange Liste von Kunden wie staatliche und militärische Stellen. Als gängiges Verwendungsmittel wurde an das Kompromat erinnert, ein Begriff des MfS, der definierbar ist als „Sachverhalt aus dem Leben einer Person, der im Widerspruch zu gesellschaftlichen […] Normen und Anschauungen steht, bei seinem Bekanntwerden zu rechtlichen oder disziplinarischen Sanktionen, zu Presigeverlusten, zur öffentlichen Bloßstellung, zur Gefährdung des Rufes im Bekannten- und Umgangskreis […] führen würde". Neben klassischen Gehemdienstmethoden des geschaffenen Problems für eine Zielperson inklusive Rettung, um an einen geschuldeten Gefallen anknüpfen zu können, sei der psychologische Trick *Greymailing* genannt. Statt einer harten Erpressung führt die Andeutung einer Erpressung, von der bezeugt wird, sie nicht zu wollen, zu viel besseren Resultaten.

Durch Daten werden Menschen verwundbar und einteilbar. Wir handeln fahrlässig mit Daten, die wir über uns und andere ins Netz geben. Könnte schon von Datenverbrechen und Beihilfe gesprochen werden? Zugriff auf Cloud-Services findet statt, und wenn Personen in Facebooks Datenbanken als Targets geführt werden, braucht nicht viel uminterpretiert zu werden im Angesicht der Drohnenmorde. Dass Ministerin Aigner damals Facebook verbieten wollte, lässt sich durchaus nachvollziehen, auch wenn Auslöser nur der Fall eines Psychotherapeuten war, dessen Telefonbuchdaten sein Telefon verließen und dessen Patienten gegenseitig als Freunde vorgeschlagen wurden. Sicherheit ist vielseitig, und somit verstehen wir unter einer informatischen IT-Sicherheit etwas anderes als Staatssicherheit. Und für einen Geheimdienst wie die NSA hat sie die Bedeutung, dass nur er selbst Zugriff hat.

Kryptologie funktioniert nicht im luftleeren Raum, sondern vielmehr in unsicheren Umgebungen. Verfahren werden geschwächt und umgangen, Schlüssel erbeutet. Der Markt für Schwachstellen, in dem nun auch die Dienste mitspielen, und die Verzögerung von Fehlerbehebungen aufgrund von PR-Abwägungen werfen kein gutes Licht auf den Stand der Technik. Den Aussagen von Industrie und Behörden kann kein Vertrauen entgegengebracht werden. Am Beispiel *RSA Security* wird dies besonders deutlich; im Austausch gegen 10 Mio. Dollar erreichte die NSA, dass Schwachstellen in Produkte eingebaut wurden. Auch Microsoft schließt den Einbau von *Back Doors* nicht aus, und beim Stichwort *Trusted Computing* müssen wir uns fragen, wem zu vertrauen ist. Freie Software bietet in vielerlei Hinsicht Vorteile. Die Einschränkung von Kryptotechnologie bringt eine Einschränkung der digitalen Souveränität. Um nachprüfen zu können, ob der Code unterwandert wurde, stand die Forderung nach einer offenen Kryptoanalyse im Raum, die durch Festangestellte einer gut aufgestellten Institution durchgeführt wird.

Informationen zur Überwachungstechnologie und deren Anbietern lässt sich im *Bugged-Planet-Wiki* finden, einer Gegenkartographie der Überwachungserkenntnisse, die durch Andy Müller-Maguhn betrieben wird.

Andy Müller-Maguhn

Andy Müller-Maguhn ist Bürgerrechtsaktivist im digitalen Bereich. Er arbeitete als *at-large director* bei der *Internet Corporation for Assigned Names and Numbers* (ICANN) und bekleidete Positionen in verschiedenen NGOs wie der *European Digital Rights* (EDRi) oder dem *Chaos Computer Club* (CCC). Aktuell beschäftigt er sich mit Unternehmen, die Überwachungssoftware verkaufen.