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

Sylvia Johnigk

Bürgerrechte nach dem NSA-Skandal

Geheimdienste und Militär nutzen die Verpflichtung von Telekommunikationsunternehmen zur Lawful Interception *und die Kollaborationsbereitschaft von Unternehmen aus, um flächendeckend Informationen abzuschnorcheln. Somit dienen die Informations- und Kommunikationstechnik und insbesondere das Internet und die Online-Dienste zur massenhaften und flächendeckenden Ausforschung und Überwachung.*

Geheimdienste und Militär wollen unsere Metadaten

Dabei stehen Netzknotenpunkte im Fokus, wie zum Beispiel der weltweit größte Internetknotenpunkt DE-CIX, der in Frankfurt betrieben wird. Dieser wird von verschiedenen Betreibern unterhalten, unter anderem ist auch *Level(3)* dabei, ein Kollaborateur des britischen Geheimdienstes GCHQ. Ferner werden Glasfaserkabel an zentralen Orten wie den transatlantischen Unterseekabeln nahezu vollständig auf Metadaten und partiell auf Inhaltsdaten abgeschnorchelt.

Insbesondere interessieren sich die Geheimdienste für die Metadaten. Es scheint so, als wappneten sie sich schon jetzt für die Zukunft. In den nächsten Jahren werden immer mehr Metadaten erzeugt, *Smart Phone*, *Smart Pad*, *Smart TV*, *Smart Grid*, *Smart Fridge*, *Smart Power*, *Smart Car*, *Smart App*. Das sind unfassbar viele Informationen, die die Geheimdienste zu einem gigantischen Verhaltensprofil zusammen führen wollen.

Geheimdienste und Militär schwächen unsere IT

Geheimdienste und Militär schwächen aktiv Software-, Krypto- und Hardwareprodukte, indem sie bei den herstellenden Unternehmen bewusst Schwachstellen einbauen lassen, die sie für ihre Zwecke nutzen.

Zusätzlich werden gezielt Endgeräte, Netzwerkgeräte, Server, Tastatur, Monitor, USB, Smartphone, etc. von Nutzern durch die Geheimdienste mit Wanzen und anderem Ungeziefer ausgestattet. Der Bestellvorgang im Online-Shop und die Bezahlung per Kreditkarte erleichtern es den Geheimdiensten, gezielt die bestellte Ware einer bestimmten Person auf dem Versandweg abzufangen und zu infiltrieren.

Sylvia Johnigk bei ihrem engaierten Referat, Foto: Sven Lüders

Hierfür gibt es für Geheimdienste einen Bestellkatalog[1], aus dem sie die richtigen Tools für ein bestimmtes Gerät auswählen können. Eine weitere Möglichkeit ist das Erzeugen von *Windows*-Fehlermeldungen und so das potenzielle Abgreifen von privaten Informationen über die Versendeoptionen *Melden des Fehlers* an den Provider.

Die aktuelle Konzeption und Implementierung von IuK-Netzwerken und IuK-Technik sind offen für das Ausspähen von Daten. Viele Endgeräte sind aktuell nicht sicher, so dass es schwierig ist, auf diesen Endgeräten Krypto- und andere Sicherheitsanwendungen sicher zu installieren und zu benutzen.

Geheimdienste und Militär betreiben *Bot-Netze* und infizieren 100.000 private Rechner, um sie im Ernstfall für einen Cyberangriff nutzen zu können.[2]

Fälschen, Täuschen und Propaganda sind ihre Kernkompetenzen

Geheimdienste und Militär betreiben gezielt Desinformation und Propaganda. Hierzu gehört es, Informationen zu Bedrohungen oder Schwachstellen einseitig zu färben, zu fälschen oder irreführend, verharmlosend oder übertrieben darzustellen. Hier stehen nicht nur die Geheimdienste in der Kritik, sondern auch die Regierung und andere exekutive Organe der Bundesrepublik.

Zum Beispiel proklamiert die Bundesregierung per Gesetz, dass *DE-Mail* sicher ist. Fakt ist, dass es sich bei DE-Mail lediglich um eine Transport-Verschlüsselung handelt. Auf den Servern der TK-Anbieter liegen die Mails unverschlüsselt. Da TK-Anbieter dem Staat *Lawful-Interception*-Schnittstellen zur Verfügung stellen müssen, können die Geheimdienste bei Bedarf die E-Mail unverschlüsselt absaugen.

Teilweise verbreiten kollaborierende (Sicherheits-) Unternehmen diese Informationen, um ihnen in dieser Tarnung mehr Glaubwürdigkeit zu verleihen.

Geheimdienste verbreiten zudem Desinformation und Propaganda, um Aktivisten und Kritiker zu diskreditieren. Im Rahmen der Veröffentlichungen von Snowden tauchte ein Dokument auf, welches einen Plan des britischen Geheimdienstes offenbarte, dem zu Folge unliebsame Personen diskreditiert werden sollten. Es ist nicht bekannt, ob diese Pläne jemals ausgeführt wurden.[3]

Bundesregierung glänzt im Kleinreden

Bundesregierung und andere Exekutivorgane lassen die Bevölkerung (und die Unternehmen) im Regen stehen. Sie boykottieren eine Aufklärung und schweigen zur Affäre. Ausdrücklich befürworten sie dagegen eine Kooperation mit der NSA. Die NSA unterhält in Deutschland unter anderem den wichtigsten Knotenpunkt für ihre Aktivitäten auf dem alten Kontinent. Zudem genießen Geheimdienstmitarbeiter Diplomatenstatus und sind somit nahezu unantastbar.

Unsere Bundesregierung befürwortet die massenhafte und flächendeckende Ausspähung. Sie spricht bei der Vorratsdatenspeicherung von Erfolgen bei Ermittlungen, von Verstößen gegen das Grundgesetz dagegen gar nicht.

Das Grundrecht auf *Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* dient dem Schutz von persönlichen Daten, die in informationstechnischen Systemen gespeichert oder verarbeitet werden. Dieses Recht wird im Grundgesetz zwar nicht explizit genannt. Es wurde allerdings 2008 durch das Bundesverfassungsgericht als spezielle Ausprägung des allgemeinen Persönlichkeitsrechts (Art. 1 Abs. 1 GG, Art. 2 Abs. 1 i.V.m.) aus den vorhandenen Grundrechtsbestimmungen abgeleitet. Nach dem Urteil des Bundesverfassungsgerichts ist zudem die heimliche Infiltration informationstechnischer Systeme nur dann zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Diese Infiltration kann nur durch einen richterlichen Beschluss herbeigeführt werden.

Mit diesem Urteil sollte klar geworden sein, dass das massenhafte, anlasslose Ausspähen in vielerlei Hinsicht einen massiven Bruch der Grundrechte in Deutschland darstellt, der mit nichts zu rechtfertigen ist.

Die Bundesregierung leistet Beihilfe zu Menschenrechtsverletzungen

Die Bundesregierung und andere Organe der Exekutive leisten Beihilfe bei geheimdienstlichen Aktionen, die sowohl gegen internationale Menschenrechte als auch die deutsche Verfassung verstoßen, indem Menschen in Menschen und Terroristen/Terrorverdächtigte eingeteilt werden. Dabei wird akzeptiert, dass geheime Algorithmen/Analyseverfahren (z. B. X-Keyscore) darüber bestimmen, wer Terrorist oder Terrorverdächtigter ist.

Terroristen und Terrorverdächtige können festgesetzt und in einen Staat verschleppt werden, in dem sie ihre Menschenrechte verlieren – auch wenn nur ein Verdacht vorliegt. Kann man Terrorverdächtige gleich (durch Drohnen) töten, ohne ein Recht auf einem fairen Prozess? Kann man sie in Foltergefängnisse wegsperren, ohne dass sie jemals ein Recht auf einen fairen Prozess haben? Darf man sie foltern, *waterboarden*, stundenlang, tagelang mit lauter Musik beschallen und grellem Licht bestrahlen, auf dem nackten Boden schlafen lassen, in kalten nassen Räumen unterbringen oder ohne Schatten im Freien? Alles ohne eine Chance auf Verteidigung? Ohne einen fairen, offenen Prozess? Lebenslang verdächtig weggesperrt? Wenn das heimlich geschieht, verschwindet man einfach vom Erdboden und oft erfahren Angehörige nichts davon.

Die CIA hat in Deutschland mit Hilfe des Unternehmens CSC den deutschen Staatsbürger *al Masri* in ein Foltergefängnis verschleppen lassen. Nachdem bekannt wurde, dass einige Regierungsmitglieder darüber informiert gewesen waren, gerieten

Sylvia Johnigk

Sylvia Johnigk studierte Informatik an der TU-Berlin und befasste sich schon im Studium mit Themen wie Datenschutz und Informationssicherheit, arbeitete fünf Jahre in der Forschung am Thema Informationssicherheit und acht Jahre bei einem Finanzdienstleister als IT-Security Consultant in Frankfurt am Main. Seit Mitte des Jahres 2009 ist sie selbständig und leitet ein kleines Unternehmen in München, das sich auf Beratung von Unternehmen zum Thema Informationssicherheitsmanagement mit dem Schwerpunkt Mitarbeitersensiblisierung spezialisiert hat.

diese in Kritik. Wegen des Drucks von Außen und der erwiesenen Unschuld kam *al Masri* nach mehreren Monaten wieder frei. Man hat ihn übrigens, nachdem der Fehler bemerkt wurde, nicht zurück nach Deutschland geflogen, sondern in einem Wald nahe der albanischen Grenze ausgesetzt.

Wir lassen uns von Menschen, von Geheimdienstmitarbeitern mittels nicht überprüfbarer Algorithmen und Verfahren die Menschenrechte absprechen.

Die flächendeckende Ausspähung wird zwar mit dem weltweiten Terror begründet, doch lediglich 35 % des Budgets ist für die Terrorbekämpfung vorgesehen. Ein Schelm, wer Böses dabei denkt.

Wichtige Fragen, die wir uns im Zusammenhang mit dem NSA Skandal stellen müssen

Wie dehnbar wird der Begriff des Terroristen/Terrorverdächtigten in der Zukunft werden?

Wollen wir in einer Gesellschaft mit zwei Klassen von Menschen leben, Menschen mit Menschenrechten und Menschen ohne Menschenrechte?

Wollen wir akzeptieren, dass Geheimdienste diese Entscheidungen im Verborgenen und nahezu ohne transparente Kontrolle treffen?

Wollen wir akzeptieren, dass ausländische Geheimdienste auf dem Boden von Deutschland/Europa unsere/andere Daten abziehen?

Wollen wir akzeptieren, dass wir keine Antworten aus den USA bekommen, obwohl sie in die Autonomie der BRD eingreifen (falls die Regierungen dies nicht schon über Geheimverträge abgetreten haben)?

Wollen wir akzeptieren, dass wir unter dem Deckmäntelchen des Terrorismus massenhaft und flächendeckend ausgespäht werden?

Anmerkungen

1 *http://www.spiegel.de/netzwelt/netzpolitik/interaktive-grafik-hier-sitzen-die-spaeh-werkzeuge-der-nsa-a-941030.html*

2 *http://www.chip.de/news/NSA-Geheimdienst-nutzt-infizierte-PCs-als-Botnetz_66586085.html*

3 *http://www.spiegel.de/netzwelt/netzpolitik/gchq-greenwald-veroeffentlicht-weitere-snowden-dokumente-a-955488.html*

Dietrich Meyer-Ebrecht

Besteht die Chance einer demokratischen Gestaltung und Kontrolle unserer Kommunikationsnetze?

If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.
Bruce Schneier[1]

Edward Snowden hat uns mit seinen Enthüllungen gelehrt: Geheimdienste, allen voran die NSA, sind mit der Massivität ihrer personellen und finanziellen Mittel, mit ihrer Aggregation an Expertise und Kreativität in der Lage, jeden Datenstrom anzuzapfen, sich Zugang zu jeder Datensammlung zu verschaffen. Nur mit einem unverhältnismäßig hohen Aufwand und mit erheblichen Einschränkungen könnten wir uns dagegen schützen, und es bleibt offen, ob ein 100 %iger Schutz überhaupt erreicht werden kann. Bürgerrechte im Digitalen – so können wir Bruce Schneiers Statement interpretieren – sind nicht technisch zu haben, sie sind zwischen Politik und Gesellschaft auszuhandeln.

Nicht verhandelbar in einer freiheitlichen Gesellschaft ist die Privatsphäre. Der Schutz der informationellen Privatsphäre stellt jedoch eine ganz besondere Herausforderung dar. Anders als im Physischen gibt es im Digitalen zwischen öffentlichem Raum und privatem Raum keine Türen, die verriegelt werden können. Die Abgrenzung ist eher eine Art semipermeable Membran, vergleichbar mit der Hülle einer biologischen Zelle. Denn für den Informationsaustausch bedarf es einer selektiven Durchlässigkeit, wenn die Optionen der Kommunikationsnetze sowohl einen individuellen als auch einen gesellschaftlichen Nutzen haben sollen. Schutz und Nutzen zugleich können jedoch nur gewährt werden, wenn die digitale Außenwelt demokratischen Spielregeln folgt, einer demokratischen Kontrolle unterzogen wird. Dies fordert den Staat. Der Schutz seiner Bürger muss durch eine angemessene Gesetzgebung – und ihre Durchsetzung! – garantiert sein. Dazu gehört ein politischer Wille. Unverzichtbar ist aber auch das gesellschaftliche Engagement. Beides ist derzeit schwer zu haben. Wollen wir die Chancen für eine demokratische Gestaltung und Kontrolle der Netze abwägen und Lösungswege skizzieren, müssen wir uns mit den Problemen und Missverständnissen auseinander setzen, die diesem Ziel im Wege stehen, die gleichsam als *Bedrohung von innen* wirken.

Die Politik – handlungsunfähig?

Hier treffen wir auf drei Komplexe. Der erste ist die innen- und außenpolitische Dimension: das Thema betrifft die Sicherheits-