H 7625

FIfF Kommunikation

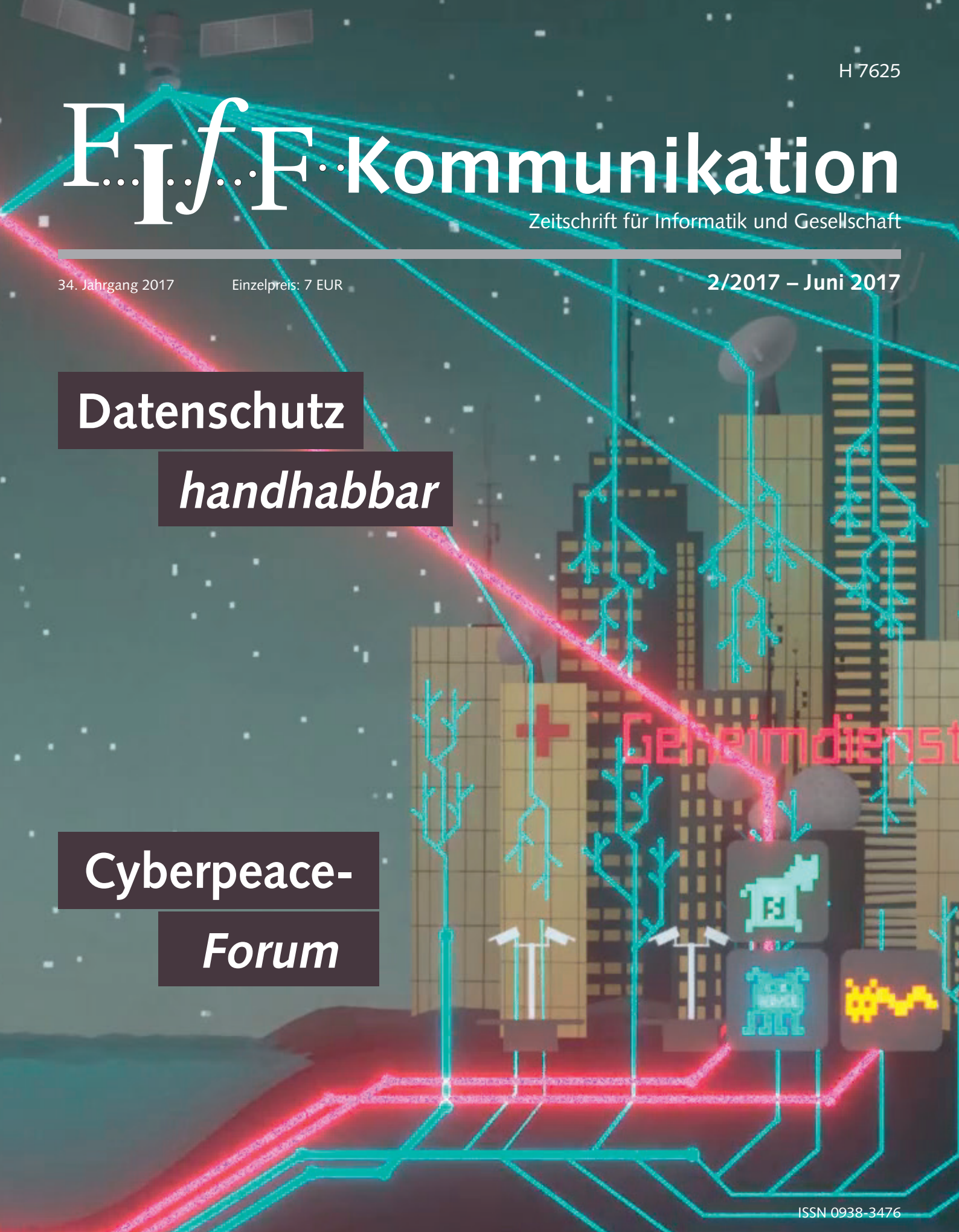
Zeitschrift für Informatik und Gesellschaft

34. Jahrgang 2017 Einzelpreis: 7 EUR

2/2017 – Juni 2017

Datenschutz *handhabbar*

Cyberpeace-*Forum*



ISSN 0938-3476

• Staatliche Spähsoftware • Algorithmen sind nicht schuld • Netzwerkdurchsetzungsgesetz •

FIfF Kommunikation

Zeitschrift für Informatik und Gesellschaft

Titelbild: Videostill, Motion Ensemble, Alexander Lehmann

inhalt

Inhalt

Ausgabe 2/2017

03 Editorial
- Stefan Hügel

Forum

04 *Der Brief:* Zum Heulen
- Stefan Hügel

05 Algorithmen sind nicht schuld, aber wer oder was ist es dann?
- Britta Schinzel

09 Die Manipulation von Denken und Handeln ist zur treibenden Kraft der IT-Entwicklung geworden
- Rainer Rehak, Jens Wernicke

14 Deklaration für die Meinungsfreiheit
- Reaktion auf das Netzwerkdurchsetzungsgesetz

16 Kurzfilm: Cyberpeace statt Cyberwar
- FIfF e. V. – Pressemitteilung

18 Überblick über staatliche Spähsoftware
- Sebastian Nemetz

FIfF intern

15 Ankündigung 33. FIfF-Konferenz (#FIfFKon17)
TRUST – Wem kann ich trauen im Netz und warum?

15 Einladung zur Mitgliederversammlung 2017 in Jena

Lesen & Sehen

75 Grundrechte-Report 2017 „Sicherheit bedeutet Gefahr – jedenfalls für die Grundrechte“
- Humanistische Union u. a.

76 Neuauflage: „Naturwissenschaft – Rüstung – Frieden. Basiswissen für die Friedensforschung“
- Ute Bernhardt

76 Wissenschaft & Frieden 2/2017 „Flucht und Konflikt“

Schwerpunkt „Datenschutz – handhabbar“

29 Editorial zum Schwerpunkt
- Eberhard Zehendner

30 Beurteilung des Datenschutzes anhand ausgewählter Kriterien
- Nicole Tornow

35 Roboter im Alltag: Wer trägt Verantwortung bei Schutzbefohlenen?
- Sarah Schott und Claudia Sichting

39 Eine Spieler-orientierte Kritik an (mobilen) Free-to-Play-Spielen
- Felix Baral-Weber

42 Darf Google mein Profilbild verkaufen?
- Maximilian Katzmann

47 Der Wert unserer Daten
- Maike Küper

52 Schöne neue Bücherwelt
- Anja Grunert

56 Auf der Spur digital terrestrischer Fußabdrücke
- Peter Wohlgenannt

Schwerpunkt „Cyberpeace-Forum“

64 Einleitung
- Hans-Jörg Kreowski

65 Cyberkrieg und Völkerrecht
- Rolf Gössner

69 Onlineoffensive: Die Bundeswehr im Cyber- und Informationsraum
- Thomas Gruber

71 Techniken und Möglichkeiten digitaler Kriegsführung am Beispiel Stuxnet
- Aaron Lye

Rubriken

79 Impressum/Aktuelle Ankündigungen

80 SchlussFIfF

Editorial

Auch diese Ausgabe der *FIfF-Kommunikation* hat zwei Schwerpunkte: einen großen und einen kleinen. *Datenschutz handhabbar*, so der Titel des ersten Schwerpunkts, der von Eberhard Zehendner und Stefanie Jäckel zusammengestellt wurde, und in den im Schwerpunkteditorial auf Seite 29 ausführlich eingeleitet wird. Die Beiträge des Schwerpunkts sind überwiegend aus Seminaren an der Friedrich-Schiller-Universität Jena heraus entstanden und decken ein breites Spektrum von Themen im Umfeld des Datenschutzes ab – Richtlinien des Datenschutzes, Tracking des Leseverhaltens durch E-Book-Reader und der Umgang mit digital terrestrischen Fußabdrücken sind nur einige davon.

Der zweite, kleinere Schwerpunkt ist aus einer Veranstaltung in Bremen im Rahmen unserer Kampagne *Cyberpeace* entstanden, die am 11./12. November 2016 stattfand. Sie war konzipiert als ein Bremer Beitrag im Rahmen der Cyberpeace-Kampagne zur Diskussion aktueller Entwicklungen zum Thema Cyberkrieg. Dazu wurden Entwicklungen und Gegenentwürfe zum Thema Cyber- und Drohnenkrieg vorgestellt und diskutiert. Ab Seite 64 leitet Hans-Jörg Kreowski in einem weiteren Schwerpunkteditorial in diesen Schwerpunkt ein.

Die Schwerpunkte ergänzen unsere aktuellen Beiträge in der Rubrik *Forum*: *Algorithmus* ist vielleicht der erste neue Begriff, der Studierenden im Informatikstudium beigebracht wird. Legt man dieses erlernte Verständnis zugrunde, scheint dieser Begriff gerade einen Bedeutungswandel zu erfahren. Doch der metaphorische Gebrauch von Alltagssprache in der Informatik ist nicht nur ein Hilfsmittel zur Erschließung von Abstraktem, sondern bekanntermaßen auch ein Problem der moralhaltigen Vermischung von Bedeutungen: beispielsweise Intelligenz, Ontologie etc. Auch umgekehrt führt die metaphorische Verwendung informatischer Begriffe in sozialen Zusammenhängen zu verschmierten Semantiken, die ebenfalls zur Verschiebung von Verantwortung führen können. *Algorithmus* ist das jüngste Beispiel dafür. Britta Schinzel appelliert an die Informatik-Community, sich ihre Begriffe nicht bis zur Unkenntlichkeit erweitern und verwässern zu lassen. Lässt sie nämlich zu, dass der Algorithmus-Begriff auf alle Arten von Software, Maschinisierung und KI ausgedehnt wird, so verliert sie ihre Kritikfähigkeit.

In diesem Sinne irritieren Formulierungen wie „Gefährdungen der Menschenwürde ergeben sich … durch … Einsatz von Algorithmen“, wie sie im Entwurf einer Digitalcharta (*digitalcharta.eu*) zu finden sind. Nicht zuletzt George Orwell hat uns gezeigt, welche politische Bedeutung Sprache hat – das sollten gerade wir nicht vergessen. In ihrem Beitrag zielt Britta Schinzel darauf ab, die Semantik des Begriffs *Algorithmus* – und die damit verbundene Diskussion – vom Kopf auf die Füße zu stellen.

Im Vorfeld der letztjährigen FIfF-Konferenz wurde auf dem Nachrichtenportal *nachdenkseiten.de* ein Interview mit Rainer Rehak veröffentlicht, in dem er die Beweggründe und Ziele des FIfF und der Konferenz darstellte. Er erläuterte, wie „… die Manipulation von Denken und Handeln längst zur treibenden Kraft der IT-Entwicklung geworden [ist] und … die Technik, die uns das Leben erleichtern sollte, mehr und mehr zur Instanz der totalen Kontrolle über uns [verkommt].“ Es lohnt sich immer noch, das Interview zu lesen.

Unsere von der *Stiftung Bridge* geförderte Kampagne *Cyberpeace* ist im letzten Jahr zu Ende gegangen. Unsere Arbeit an diesem Thema werden wir selbstverständlich fortsetzen. Dank der Förderung konnten wir die Problematik und unsere Ziele in einem Kurzfilm darstellen, den Alexander Lehmann und Motion Ensemble für uns erstellt haben und der auf der Konferenz *re:publica* vorgestellt wurde. Davon handelt ein kurzer Beitrag in dieser Ausgabe: *Cyberpeace statt Cyberwar*. Wir empfehlen natürlich, den gesamten Film anzusehen, der über unsere Homepage *fiff.de* zu erreichen ist.

Hate Speech ist ein weiteres Problem, mit dem wir uns angesichts des Internets und der sich verbreitenden Kommunikationsmedien beschäftigen müssen. Dass das ein Problem ist, steht außer Zweifel – verstörend, zu welchen verbalen Angriffen sich manche Menschen hinreißen lassen. Für völlig ungeeignet halten wir allerdings die Initiative des Bundesjustizministeriums, das durch das *Netzwerkdurchsetzungsgesetz* (NetzDG) beabsichtigt, die Verantwortung für die Regulierung auf die Betreiber der Plattformen wie *Facebook* abzuwälzen. Strafbare Beleidigungen und Hetze müssen mit den Mitteln des Strafrechts verfolgt werden, für nicht strafbare Aussagen – und sind sie noch so schwer zu ertragen – muss die Community andere Wege finden. Die postulierte „offensichtliche Rechtswidrigkeit“ kann es in einem Rechtsstaat nicht geben. Der Verdacht drängt sich auf, dass das Gesetz, im Sinne des *Nudging*, seine Ziele durch vorauseilende Maßnahmen erreichen will – um das Risiko strafrechtlicher Verfolgung im Vorfeld bereits zu vermeiden. Das FIfF hat sich mit vielen weiteren Organisationen der *Deklaration für die Meinungsfreiheit* angeschlossen, die das Gesetz kritisiert und deren Text wir in dieser Ausgabe abdrucken.

Einen Eindruck von dem Schaden, den Angriffswerkzeuge von Militär und Geheimdiensten verursachen können, erhalten wir gerade durch die weltweite Cyberattacke des Trojaners *WannaCry* – der *Brief* in dieser Ausgabe setzt sich damit und den Konsequenzen auseinander: *Zum Heulen*. Doch worum geht es, wenn wir über Cyberwaffen und Schadsoftware sprechen? Sebastian Nemetz gibt in seinem ebenso umfangreichen wie lesenswerten Beitrag einen *Überblick über staatliche Spähsoftware*. Der Beitrag schlägt den Bogen sowohl zum Cyberpeace-Forum, wo Aaron Lye über *Techniken und Möglichkeiten digitaler Kriegsführung am Beispiel Stuxnet* referierte, als auch zum Erpressungstrojaner *WannaCry*.

Wir wünschen unseren Leserinnen und Lesern eine interessante und anregende Lektüre – und viele neue Erkenntnisse und Einsichten.

Stefan Hügel
für die Redaktion

Der Brief

Zum Heulen

Liebe Leserinnen und Leser, liebe Mitglieder des FIfF,

sollte es jemand angesichts der Überschrift erwartet haben: Nein, es geht nicht um das erneut wenig erfolgreiche Abschneiden der deutschen Starterin beim *Eurovision Song Contest* – auch wenn dieser *Brief* am Vormittag des Sonntag, 14. Mai 2017 entsteht und auch deswegen einigen vielleicht zum Heulen zumute ist.

Die ersten Nachrichten kamen aus Großbritannien: Ein *Ransomware*-Trojaner, genannt *WannaCry*, hatte zunächst Rechner des britischen *National Health Service* befallen und damit die staatliche Gesundheitsversorgung erheblich beeinträchtigt. Nach und nach wurden weitere Störungen bekannt; für die Öffentlichkeit vielleicht am deutlichsten erkennbar an den Anzeigetafeln der *Deutschen Bahn*, auf denen das Anzeigefenster des Trojaners sichtbar wurde. Ursache für die Störungen war offenbar ein Angriffswerkzeug des US-Geheimdiensts NSA, das auf unveröffentlichten Schwachstellen unterschiedlicher Versionen des Betriebssystems *Windows* basierte. Nachdem diese Schwachstellen geleakt wurden, gab es im März einen Patch von Microsoft für die aktuell noch unterstützten Versionen – weitere Patches für nicht mehr unterstützte Versionen, darunter das immer noch häufig eingesetzte *Windows XP*, wurden hastig nachgeschoben.

Der Trojaner wurde dann zunächst gestoppt, nachdem ein britischer Sicherheitsexperte – „durch Zufall" – einen *Kill Switch* entdeckt hat. Man lehnt sich aber sicherlich nicht zu weit aus dem Fenster mit der Vorhersage, dass das nicht der letzte derartige Angriff gewesen sein wird.

„Told you so!", könnte man nun ausrufen, auf unseren Film (siehe dazu den Beitrag in diesem Heft, Seite 16) und viele weitere Artikel und Erklärungen (nicht nur des FIfF) verweisen und sich überlegen zurücklehnen. Doch das hilft natürlich nicht weiter. Im Gegenteil, es führt sogar in die Irre.

Es ist nicht plausibel, anzunehmen, dass einer Geheimdienstbehörde wie der NSA (oder dem BND) die Problematik nicht bekannt war und ist. Geheimdienste schaffen Schwachstellen in Systemen oder halten bestehende Schwachstellen geheim, um ihrer weltweiten Spionagetätigkeit nachzugehen – das muss uns nicht erst seit Edward Snowden klar sein. Die einzige sinnvolle Erklärung ist, dass solche Cyberangriffe und die daraus resultierenden Schäden als *Kollateralschäden* bewusst in Kauf genommen werden. Weltweit werden Computersysteme gefährdet, weil die eigenen Aktivitäten und Ziele höher priorisiert werden als ein tatsächlicher Schutz der Rechnersysteme vor Angriffen. Vielleicht hofft man dort, dass – wenn einmal alle Systeme unter der Kontrolle der jeweiligen Behörde stehen – alle Angriffe im Vorfeld verhindert werden können. Doch das wäre eine trügerische Erwartung – von den menschenrechtlichen Implikationen einer solchen Totalüberwachung ganz zu schweigen. Das hindert die politisch Verantwortlichen aber nicht daran, stakkatoartig den weiteren Ausbau von Überwachungsbefugnissen zu fordern. Die Hoffnung, dass die Veröffentlichungen von Edward Snowden zu einem Abbau der Überwachung führen würden, haben sich längst zerschlagen, ja teilweise eher ins Gegenteil verkehrt.

Es ist übrigens billig, die Verantwortung für die Schäden einfach den Anwendern in die Schuhe zu schieben. Sicher, oberflächlich betrachtet ist es bemerkenswert, dass heute immer noch eine signifikante Zahl von Systemen unter dem veralteten *Windows XP* betrieben wird, dessen Support bereits 2014 eingestellt wurde, oder dass häufig Patches nicht kurzfristig nach Veröffentlichung eingespielt werden. Doch dafür kann es im Einzelfall gute Gründe geben – und auch das dürfte Geheimdiensten wie der NSA bekannt sein, erlegt aber auch denjenigen, die die Angriffswerkzeuge und Schwachstellen *leaken*, eine besondere Verantwortung auf.

Der Vorfall weist aber auch noch auf eine andere Problematik hin: Weltweit wird ein erheblicher Anteil von – auch kritischen – Systemen unter *Windows* betrieben. Egal, wie man dieses System sonst beurteilt: Es ist dadurch eine Monokultur entstanden, die uns alle in die Abhängigkeit von einem einzelnen Anbieter (und dessen Produktzyklen) zwingt. Es gibt richtige Ansätze – die Umstellung der Software in den Großstädten Wien und München („LiMux") ist einer davon. Umso verstörender sind die Überlegungen, dies nun auch in München wieder rückgängig zu machen, nachdem die Initiative in Wien bereits vor längerer Zeit gescheitert ist. Wirtschaftliche Aspekte mögen eine Rolle spielen – den munteren Spekulationen über die Beweggründe der in München politisch Verantwortlichen mag ich mich hier nicht anschließen.

Welche Konsequenzen sind nun zu ziehen?

1. Die Praxis der Schaffung und Geheimhaltung von Angriffswerkzeugen und Schwachstellen in – insbesondere kritischen – Systemen muss ein Ende haben. Staatliche Behörden sind auf eine verantwortungsvolle Information über Schwachstellen zu verpflichten – zuerst der Systemersteller und -betreiber, dann der Öffentlichkeit. Keinesfalls dürfen staatliche Mittel für den Ankauf von *Exploits* bereitgestellt werden.

2. Die politische Doktrin der Totalüberwachung muss aufgegeben werden. Sie schafft keine Sicherheit, sondern neue Gefährdungen. Politisch Verantwortliche sind dringend aufgefordert, zur Verbesserung der Sicherheit beizutragen, anstatt eine gefährliche Symbolpolitik zu betreiben und fortzusetzen.

3. Besonders bei kritischen Systemen ist *Open Source* zu fördern. Öffentliche Zertifizierungsstellen müssen für die Überprüfung der Systeme sorgen und dabei die Fachöffentlichkeit einbinden. Die Zertifizierung muss praxisorientiert gestaltet werden, so dass sie die technische Sicherheit wirklich erhöht und keine Bürokratie der Scheinsicherheit schafft.

Schnell hingeschrieben, schwierig umzusetzen, klar. Aber es gibt keine vernünftige Alternative.

Mit FIfFigen Grüßen

Stefan Hügel

Britta Schinzel

Algorithmen sind nicht schuld, aber wer oder was ist es dann?

1. Einleitung

Algorithmen sind ein zunehmend in den Medien, auch den seriösen und wissenschaftlichen Medien, aufgeworfener Hype. Man fühlt sich von ihnen versorgt, umhegt, gesteuert, überwacht, betrogen, bedrängt usw. Es wird ihnen Handlungs- oder Entscheidungsmacht zugebilligt, sie werden für organisatorische, institutionelle und politische Steuerungen, ja auch für Wahlausgänge verantwortlich gemacht. Doch werden dabei die Begriffe Computerprogramme/Software, Maschinen, Künstliche Intelligenz (KI), Big Data etc., auch wenn dort überall Algorithmen benutzt werden, mit Algorithmen unzulässig identifiziert. Es ist, als wollte man von der Addition Moral verlangen. Algorithmen sind Rechenvorschriften, also formale Anweisungen zur Ausführung mathematischer Funktionen, denen all diese sozialen Funktionen und Zuschreibungen fremd sind. Sie können korrekt, effizient, sparsam, schnell, auch adaptiv bzw. „lernfähig" sein, aber sie sind weder objektiv noch intelligent, weder gut noch böse. Warum werden ihnen fälschlich soziale oder ethische Qualitäten zugebilligt? Weil sie sozusagen den Kern der sehr wohl werthaltigen Automatisierung ausmachen? Weil „Algorithmus" bedeutsamer oder auch sexier klingt als Software?

Computer haben den Weg für den massenhaften Einsatz von Algorithmen eröffnet. Damit werden sie, in Datenstrukturen und Software gerahmt, mit Datenmassen gefüttert, „unsichtbare" Technologie, ja mental, methodisch und physisch unsichtbare Technologie, die wir benutzen, fast ohne sie in Frage zu stellen.[1] Es sind immer menschliche Entscheidungen, wie Software spezifiziert wird, welche Algorithmen dafür ausgewählt und kombiniert werden, welche Datenangebote ihnen zukommen, und die so die Technologie zu etwas sozial, politisch und ethisch Relevantem machen. Leider wird in der Regel nicht demokratisch entschieden, ob und wie welche Technologie eingesetzt wird. Die meisten Menschen können auch nicht selbst bestimmen, welche Technik sie benutzen, um mit ihr etwa Software-Produkte herzustellen. Der soziale Druck zwingt ja vor allem viele junge Menschen, Nutzende zu werden, um sich nicht selbst ins Abseits zu stellen.

Die rasante Entwicklung der Automatisierung wird zu Recht als Bedrohung empfunden. Doch Schaden, Diskriminierungen und Katastrophen entstehen durch die Rahmung der Algorithmen in Software, mit Design, Interfaces und ihrer Amalgamierung mit kontingenten Daten anstelle der Algorithmen eigenen Universalität, mit den dabei vielfältig verfolgten Absichten. Dieser Text versucht, die Begriffe Algorithmus, Programm, Software und Daten klarer auseinander zu halten, und dabei die Orte aufzuzeigen, wo und wie mittels Computer-Software Wertsetzungen, Priorisierungen, Ausschlüsse und Diskriminierungen für Menschen und soziale Systeme in die Welt gesetzt werden (können). Dabei erscheint die Forderung nach ethischen und sozialen Algorithmen als grundlegendes Missverständnis und problematisch, weil so die Verantwortung auf formal Mathematisches verlagert wird, als unveränderlich erscheint und die menschliche Beteiligung verschleiert.

2. Algorithmen

Algorithmen sind dem Menschen „zuhandenes" Werkzeug. Softwareprozesse organisieren eine Kombination von Algorithmen. Dabei wird bestimmt, welche Algorithmen in welcher Reihenfolge genutzt und mit welchen Argumenten aufgerufen werden sollen. Das legen Menschen fest, die ein Ziel haben. Dabei muss hinterfragt werden, wer mit der zu erstellenden Software welchen Zweck verfolgt, ob, wo, wie und in welchem Kontext diese Algorithmen als Werkzeug eingesetzt werden und ob das gebilligt werden kann. Algorithmen sind nicht fähig moralische oder politische Ziele zu erwägen oder zu beachten. Sehr wohl kann dies alles aber unsere Instandsetzung von Softwaresystemen und unser Umgang mit Automatisierung. Softwareprogramme mitsamt den in ihnen organisierten Algorithmen sind, wie die Informatikerin und Genderforscherin Cecile Crutzen schreibt, Werkzeuge, die zum Handeln bereitliegen, unsere Hand führen, (Arten der) Nutzung nahelegen, Handlungen beeinflussen oder insbesondere als *Gadgets* sogar zum Handeln auffordern. Diese zweckbestimmte Organisation in Software kann natürlich moralische Fragen aufwerfen, ja sie tut dies mit der für die informationstechnische Modellierung notwendigen Abstraktion sogar notwendigerweise. Abstraktion impliziert immer auch Weglassen, und dieses Ausschließen ist subjektiv. Ebenso wenig lassen sich die Ergebnisse des Ablaufs von Software und durch sie bedingte Veränderungen der Umgebungen eindeutig vorhersehen. Dies auch deshalb, weil sich die Anforderungen und Einsatzumgebungen ändern oder Software umgenutzt wird für Verwendungszwecke, für die sie ursprünglich nicht gedacht war.

Ein Beispiel: Angenommen, man kann an jedem Tag zwei Leute retten, wie viele sind das in drei Wochen? Antwort: 42. Ein Al-

Britta Schinzel

Britta Schinzel promovierte in Mathematik, arbeitete in der Computerindustrie und habilitierte sich in der Informatik. Im Rahmen ihrer Professur für Theoretische Informatik an der RWTH Aachen arbeitete sie zunehmend interdisziplinär. Sie war von 1991 bis 2008 Professorin für *Informatik und Gesellschaft und Gender Studies in Informatik und Naturwissenschaft* an der Universität Freiburg.

gorithmus wird die Eingaben zwei und drei variabel halten, er ist so universell auf allen natürlichen Zahlen. Um einen Algorithmus anwenden zu können, muss man erklären, dass eine Woche 7 Tage hat, aber nicht, was *retten* heißt. Wenn etwa *retten* durch *ertrinken lassen* ersetzt wird, führt das auf den gleichen Algorithmus. Algorithmen können also für ganz verschiedene Zwecke eingesetzt werden. Wenn man die Namensgebung in einem Softwareprogramm ändert, wie im Beispiel, so erscheint das Programm für die Nutzer in einem ganz anderen Licht. Das Programm selbst und der Algorithmus aber haben auf diese Sichten keinen Einfluss.

Algorithmen operierten historisch gesehen zuerst auf Zahlen; sie wurden benannt nach dem persischen Mathematiker Al Chwarizmi aus dem 9. Jhdt. nach Chr., der auch die 0 erfunden hat. Später wurden sie auf viele andere Gebiete erweitert, die einer mathematischen Manipulation zugänglich waren, u. a. auf Worte, auf Sätze einer Sprache, auf Musiknotate und Musik, auf Graphiken etc. Präzisierungen des Algorithmusbegriffs wurden in Anschluss an Hilberts Versuch der Formalisierung der Mathematik von Kurt Gödel mit der Formalisierung des Berechenbarkeitsbegriffs getroffen. Das hat sehr umfangreiche mathematische Folgerungen und Theorien zur Folge gehabt, die sich u. a. mit den Fragen, was man überhaupt, und dann mit welchem Aufwand an Zeit und Speicherplatz, berechnen kann.

Für schnelle Abläufe im Inneren von Rechnern, wie etwa für Compiler, Betriebssystem und BIOS, bedarf es dabei spezieller Algorithmen, die rasche Antwortzeiten auf Eingaben garantieren. Ähnliches gilt für Sortier- und Suchalgorithmen, wie sie etwa von Suchmaschinen verwendet werden, und für manche Arten von Datenanalyse-Algorithmen.

Algorithmen finden sich mit den verschiedensten Eigenschaften in allen Computerprogrammen und Software-Anwendungen. Wichtige und effiziente Standardalgorithmen werden aus Algorithmenbanken gezogen. Betriebssysteme benötigen Warteschlangen-Algorithmen für die Abwicklung von Daten-Paketen. Compiler und – besonders wichtig für Software-Anwendungen – Sortier- und Such-Algorithmen operieren auf Zeichenketten, und letztere über hierarchisierte Anordnungen in Bäumen oder Graphen. Kürzeste Wege in Graphen sind grundlegend für unsere Navigationssysteme. Geometrische Algorithmen operieren auf diskretisierten Kurven, Flächen oder 3D-Körpern. Approximationsalgorithmen, wie Archimedes' Algorithmus zur Berechnung beliebig vieler Stellen von π, nähern sich in der Genauigkeit *irrationalen* Zahlen. Kompressionsalgorithmen wie MP3 verkleinern Bilder- oder Musikdatenmengen. Kryptografische Algorithmen verschlüsseln Daten, heute meist auf der Basis der komplex zu berechnenden Primzahlfaktorisierung zweier zuvor miteinander multiplizierter Primzahlen. Es gibt biometrische Algorithmen zur Analyse von DNA- oder Protein-Sequenzen, Clusteralgorithmen klassifizieren Mengen oder Muster. Es gibt genetische und evolutionäre Algorithmen, die nicht in gleicher Weise determiniert sind wie die zuvor erwähnten geschlossenen Algorithmen. Künstliche Neuronale Netze klassifizieren oder simulieren natürliche Systeme und werden für Lernalgorithmen, und in geschichteten Kaskaden für „Deep Learning" verwendet. Zufallsalgorithmen arbeiten mit Zufallszahlen aus Zufallszahlengeneratoren zur Bearbeitung unterschiedlichster Probleme, am bekanntesten die Las-Vegas- und Monte-Carlo-Algorithmen. *Data-Mining-* und *Data-Analytics-*Algorithmen durchforsten einen nicht endenden Strom von Big Data und ziehen aus diesen Schlüsse, bereiten Entscheidungen vor, Entscheidungshilfen treffen solche sogar. Und natürlich kann man darin indirekt Meinungen unterbringen und bestimmte Absichten verfolgen. Bei heutigen Suchmaschinen, Big Data, Data Mining, Machine Learning, Social Bots etc. erscheinen oft Daten mit Algorithmen untrennbar verschmolzen, sodass leicht begriffliche Verwechslungen entstehender Softwaresysteme mit Algorithmen entstehen können. Doch die Verschmelzungsprodukte sind nicht mehr universell, keine Algorithmen mehr, sondern Software.

3. Wie entstehen Bias, Ungleichgewichte, Wertsetzungen, diskriminierende Hierarchien oder Auslassungen in Software?

3.1 Das Entwerfen von Software

Wenn man einen diskriminierenden Text hat, so schreibt man die Ursache dafür nicht der Verwendung von Buchstaben oder Zahlen zu. Nicht anders verhält es sich mit der Verwendung von Algorithmen. Sie definieren mathematische Funktionen, die weder der Moral, der Diskriminierung noch der Klugheit oder analoger ethischer, emphatischer oder auch intelligenter Eigenschaften fähig sind. Jedoch werden sie über die Software-Anwendungen zur Ausführung an Computern in unsere Lebenswelt eingebettet. Menschen mit ihren Vorverständnissen, blinden Flecken und den beschränkten Möglichkeiten, das Feld zu verstehen, in dem ihre Software-Programme leben und einwirken werden, müssen den zu bearbeitenden Problembereich spezifizieren, „rational rekonstruieren". Sodann entwickeln sie solche, das rekonstruierte Feld verändernde Problemlösungen, mit Design, Modellierung, Implementierung, Benutzungsschnittstelle, Testen und Dokumentation. Für „geschlossene" Programmlösungen wurden solche Mechanismen bei der Software-Entwicklung während der 1980er- und 1990er-Jahre in den Bereichen von Informatik und Gesellschaft, den Arbeits- und Organisationswissenschaften ausgiebigst diskutiert und erforscht. Nebst dem Zeit- und Kostendruck, unter dem die Spezifikation des zu erstellenden Programms in Zusammenarbeit zwischen Auftraggebern, prospektiven Nutzenden und Entwickelnden definiert wird, ist oft der von Gerhard Wohland u. a. so genannte „ego-approach"[2] von Programm-Entwicklern ein Fehler und Bias erzeugendes Problem.

Die Spezifikation oder das Pflichtenheft für eine solche Software in einer Software-Umgebung wird von Menschen über das Requirements Engineering hergestellt. Damit wird die Aufgabe oder die Problemstellung eruiert, d. h. der Weltausschnitt, in dem das prospektive Programm operieren soll, abgegrenzt und, soweit für die Lösung nötig, definiert. Dabei muss die Komplexität unserer Lebenswelt reduziert werden, durch Dekontextualisierung, Vereinfachung und Abstraktion. Auch ist es nicht gleichgültig, mit welchen Zielen Software spezifiziert und modelliert wird. Wissen und Software-Handeln sind immer situiert.[3] So sind bei klassischer Softwareentwicklung für geschlossene Lösungen vorwiegend die Auftraggebenden, die beschränkten Ressourcen und die meist unter Zeitdruck stehenden Entwickelnden für zuweilen problematische Problemlösungen verantwortlich. Ein-

fluss haben aber auch die Software-Engineering-Modelle, wie das klassische Wasserfallmodell oder die inkrementelle Entwicklung, oder die agile Softwareentwicklung, die nicht mehr von geschlossenen Lösungen ausgeht, sondern auf veränderliche Anforderungen durch adaptive Methoden reagiert.

3.2 Programmiersprachen

Nicht ganz so „unschuldig" wie Algorithmen sind auch die Programmiersprachen, Programmierumgebungen und integrierten Rechner-Software-Systeme, die nicht mehr (oder nur mehr mühsam) frei programmierbar sind. Sie können unsere Vorstellungen vom Aufbau von Algorithmen, über den intendierten Ablauf im Rechner, oder sogar die Möglichkeiten universeller Programmierung einschränken. In Programmiersprachen sind Strukturmodelle eingebaut, bei der Objektorientierung beispielsweise *hierarchische Objektklassen*, dieses Modell wird dann auch in der Analyse verwendet. So werden die Analyse und die Repräsentation der Welt beeinflusst durch die Programmiersprache, die man wählt. Weglassen (abstrahieren) und Sichtbarmachen stehen in direkter Relation mit der Programmierumgebung (-sprache). Sie alle lenken die (menschliche) Vorstellung vom Ablauf eines Algorithmus in unterschiedlicher Weise, sind für das eine oder andere mehr oder weniger geeignet, und „erziehen" das lösungsorientierte Denken der Programmierenden. Mehr noch schränken die Programmierumgebungen und viele Programmierhilfen die Möglichkeiten der Benutzenden ein, indem sie Hilfestellungen geben, die allerdings nicht mehr alle Möglichkeiten offenlassen. So wirken etwa die *Application Programming Interfaces* (APIs), die von Entwickelnden als Aufbaublöcke für Anwendungssoftware, Web-basierte Systeme, Betriebssysteme, Datenbanksysteme, Plattformen für soziale Medien oder Software-Bibliotheken benutzt werden, als *Black Boxes*, weil man nur ihre Schnittstellen sehen kann.

Sukzessive wurde die Software-Entwicklung, aber mit der Interaktivität auch die Anwendung, offener gestaltet. Dabei wurde die Kontrollierbarkeit entsprechend reduziert.

Software, die statistische Methoden und stochastische Optimierungsverfahren verwendet, ist teilweise nur mehr empirisch zu beurteilen. Dies trifft auch für evolutionäre Ansätze und genetische Algorithmen zu, die gleichermaßen die Evolution natürlicher Lebewesen als Metapher verwenden.

3.3 Verteiltes Rechnen auf Netzen

Für die Kooperation und das *Resource Sharing* in Netzwerken von Computern im Grid- und Cloud-Computing, Fog- und Dew-Computing werden verteilte Algorithmen benötigt. Mit ihren spezifischen Paradigmen stellen sie für Verifikation und Sicherheit oft unlösbare Aufgaben dar, und sie bieten der kommerziellen Datengewinnung ein nahezu unerschöpfliches Feld problematischer Analysen.

Eine spezielle Form des Distributed Computing stellen *Künstliche Neuronale Netze* (KNNs) dar. Sie orientieren sich auf grob vereinfachte Weise an den Organisations- und Verarbeitungsprinzipien lebendiger neuronaler Systeme. Mit ihnen kann man u. a. Bilder klassifizieren, Muster erkennen oder motorische Aufgaben lösen, und sie werden zum Machine Learning verwendet. Sie können sehr unterschiedliche Netzwerktopologien haben. Sie bestehen aus statischen Elementen, den Knoten, und Kanten zwischen ihnen, die je mit Eingabewerten initialisiert werden, sowie Regeln über die Verarbeitung all dieser Werte im Netz, die die Informationsverarbeitung in den KNNs beschreiben. Diese stellen den Netzwerkalgorithmus dar. Oft wird die Dynamik des Netzes in eine Lernphase und eine Einsatzphase unterschieden, wobei das Netz in der Lernphase Beispiele präsentiert bekommt, die es nachher zu erkennen oder als Aufgaben zu lösen gilt. Dabei ist der Trainings-Datensatz in der Lernphase entscheidend. So zeigen KNNs, die auf die Erkennung von Hunden oder auch von Türmen und Autos trainiert sind, augenfällig, dass sie am Ende alle Bilder in Hunde oder in Türme und Autos transformieren.[4]

Natürlich ist auch die Auswahl der Netzwerktopologie und des Propagierungsalgorithmus für ein gegebenes Problem ebenso entscheidend für das Ergebnis[5] wie die (nicht zum Algorithmus selbst gehörenden) Anfangsgewichte der Netzvariablen vor dem Training. Von menschlicher Bewertung ebenso abhängig ist der Zeitpunkt des Auslesens der Ergebnisse, denn das Netz pulsiert immer weiter, es sei denn, es erreicht einen stabilen Zustand.

3.4 Big Data, Data Mining und Machine Learning

Datafication soll alles mittels IT Vorfindliche, Welt und Leben, in Daten transformieren. Big Data aggregiert, ordnet und verdaut in von Umfang, Heterogenität und Geschwindigkeit nie zuvor erreichten Dimensionen die von Digitalen Medien, wie Smartphones, Internet, dem Internet der Dinge und sozialen Medien gelieferten ungeheuren Datenmassen zu sozial, ökonomisch und kulturell relevantem Wissen. *Data Mining* und Datenanalyse benutzen u. a. statistische Modelle, probabilistische Methoden, Lernverfahren und Entscheidungsmodelle, um aus Datenmengen unterschiedlichster Art Korrelationen und Schlüsse zu ziehen. Die Auswahl der Daten und der Kriterien, nach denen de- und induziert wird, sind immer diskutierbar. Dieser in multiplen Bereichen angewandte „digitale empirische *Turn*" erhebt den Anspruch von Rationalität und Faktizität, obgleich nicht nur die Daten oft defizient, einseitig vorfindlich oder erhoben und inkompatibel sind, sondern auch methodisch Unsicherheit einzieht. findet. Der empirische Turn nimmt jedoch normativen Charakter an, die Behauptung von Objektivität und Zurechenbarkeit durch die Automatisierung lässt sich konkret nur schwer widerlegen. Doch treffen die folgenden Profilanalysen Menschen u. U. gravierend, von ihrer Kreditwürdigkeit über die Jobchancen. Viel schlimmer noch als Opfer tödlicher Drohnenangriffe.

Machine Learning versucht, aus vorhandenen Beispielen ein allgemeines Gesetz (welches man aber nicht hat) zu erhalten, welches die Beispiele erklärt. Dazu gibt es sehr unterschiedliche Methoden, die sich im Wesentlichen an der Struktur der Domäne orientieren, aus der die Beispiele kommen. Diese Methoden und Algorithmen werden durch die Inhalte nicht berührt. Man kann sie nach Belieben einsetzen, wie sonstige mathematische Methoden auch.

Beim Machine Learning bleiben die Lernalgorithmen zwar statisch, doch die entstehende Software erweitert und spezifiziert sich mit den Trainingsdaten. Die Selektivität solcher Daten wird insbesondere in der *Künstlichen Intelligenz* problematisch, wenn es um die Modellierung menschlicher Eigenschaften und Fähigkeiten durch Training von Daten einer eingeschränkten Bevölkerungsgruppe geht.

Folgen der Verbreitung all dieser Methoden sind statistische *Bias* (Ungleichgewichte) und Diskriminierungen.[6] So zeigen sich Rassen- und Geschlechter-Diskriminierungen beispielsweise beim Anzeigenangebot.[7]

3.5 Suchmaschinen

Suchmaschinen suchen nach Schlüsselwörtern durch die Webseiten im Internet und sortieren die Ergebnisse nach unterschiedlichen Rangfolgen. Die Organisation der Rangfolgen ist dabei zufällig und priorisiert somit Einträge unterschiedlich. Eine Suchmaschine erstellt ein Netz von Verlinkungen, das die *Beliebtheit* einer Seite beurteilt. Google zeichnet dafür im *PageRank* die gewichteten Verweise auf eine Webseite aus, die Linkpopularität, und erstellt eine Ergebnisreihenfolge. Bei einer Suchabfrage werden die Links je nach Gewicht sortiert. Ein anderes Kriterium ist *Hubs und Authorities* von Kleinberg, wo jede Seite zwei Bewertungen erhält. Beim *TrustRank* hingegen wird eine kleine Anzahl von vertrauenswürdigen Seiten manuell ausgewählt. Diese vererben dann Vertrauen auf verlinkte Webseiten weiter.

Bei Google werden Suchergebnisse anhand der gespeicherten individuellen Suchhistorie, dem lokalen Aufenthaltsort und weiteren Faktoren personalisiert ausgegeben. Weitere Adaptionen werden wegen der schnellen Veränderungen im Netz vorgenommen, um Manipulationen der Suchergebnisse auszuschließen und um Werbung geeignet zu platzieren. Seit einiger Zeit sind auch semantische Suchverfahren im Einsatz, Google setzte 2013 das neue Verfahren *Hummingbird* auf, um die Absicht der Suchanfrage besser zu verstehen. Werden auch Gruppenprofile und Bildanalysen für Antworten auf Suchanfragen verwendet, kommt es zu Ungleichheiten und Benachteiligungen für unterschiedliche Nutzende, etwa für Frauen bei der Jobsuche: wenn vorwiegend Männer nach hoch bezahlten Jobs suchen und dies bildlich unterstützt wird, werden Männer eher lukrative Jobs angeboten bekommen, während eine Frau, die das Gleiche sucht, ihrer Gruppe und den verzerrenden Bildangeboten entsprechend weniger gute Angebote erhält.[8] Hier wirkt die Automatisierung als Verstärkung bestehender Ungleichheiten.

3.6 Soziale Netzwerke

Soziale Netzwerke sind Online-Dienste, die auf Plattformen eingehegte Gemeinschaften mit von ihnen selbst erzeugten Inhalten beherbergen, und die ihren Gewinn i. d. R.[9] ebenso wie Suchmaschinen aus der Werbung ziehen. Nutzende können hier mit diversen Einstellungen und Kontaktlisten in von ihnen definierten Gruppen kommunizieren, Daten austauschen und ihre eigenen Profile erstellen. Natürlich sind weder die verwendeten Algorithmen noch die dafür erstellte Software für die in diesen Netzen kursierenden Inhalte verantwortlich. Aber die Software liefert Möglichkeiten, Inhalte zu verstärken, Gruppen-Profile zu erstellen und Nutzer zu beeinflussen. So entstehen Echokammern von Nutzenden, die sich wechselweise bestätigen. *Bots* (autonome mobile Softwareprozesse), wie z. B. *Webcrawler*, arbeiten automatisch Aufgaben ab. *Social Bots* operieren in sozialen Medien, geben dort aus bisherigen Äußerungen generierte Antworten oder setzen mit realistisch wirkenden Fake-Accounts und Profilen vorbereitete Informationen ab. Sie werden nicht nur zur Werbung, sondern auch zum *Nudging* und zu Propaganda und Wahlbeeinflussung eingesetzt und unterhöhlen so die Demokratie. Solches ist sowohl beim *Brexit* wie auch im letzten Wahlkampf in den USA bekannt geworden.[10] Chatbots werden in Messengerdiensten eingesetzt, um die Nutzungsfrequenz zu erhöhen und Nutzende in einem sozialen Netz festzuhalten. Leider lassen sich reale aber kaum von *Fake News* unterscheiden. Mit Bots sind haarsträubende Bias bekannt geworden, etwa Googles Bilderkennungs-Anwendung, die schwarze Menschen als Gorillas identifizierte.[11] Dies, weil ihr als Trainingsdaten vorwiegend weiße Menschen angeboten worden waren. Die Wahl eines unvollständigen Datensatzes ist bei solchen Effekten für die Diskriminierung verantwortlich. Microsofts Chatbot *Tay*, der nach 24 Stunden Aufnahme von Konversationsdaten aus Twitter eine unglaublich rassistische, sexistische, homophobe Persönlichkeit annahm, wiederholte und verstärkte leider entsprechend gepostete Tweets.[12]

4. Resümee

Die Frage, ob Algorithmen verantwortlich gemacht werden können, wird durch Darstellung ihrer Beschaffenheit obsolet. Hingegen ermöglichen Softwaresysteme und Automatisierung, die Algorithmen verwenden, Diskriminierungen oder Manipulationen etc. Wo ist die Grenze zu ziehen, ab wann können aus Algorithmen bestehende Programme soziale, moralische, diskriminierende Eigenschaften aufnehmen? Dies ist dann der Fall, wenn dafür mehr oder weniger passende oder gute Algorithmen ausgewählt werden, wenn, wie für Software üblich, Gestaltungsaspekte mit *Likeability* und *Seducability* dazu kommen, Anforderungsermittung getätigt wird, Datenstrukturen, Schnittstellen, der Zugang und Interfaces definiert werden, die die Möglichkeiten zur Interaktion bieten, sei es für Mensch oder Sensoren, und auch wenn Sicherheitsaspekten Genüge geleistet wird; und weiter wenn kontingente Daten(-mengen) in die Software integriert werden. Beim Entwerfen von Software, für die Entwicklung und Benutzung von Programmiersprachen, für verteiltes Rechnen auf Netzen zeichnen vor allem Auftraggebende und Entwickelnde verantwortlich, für Big Data, Data Mining und Machine Learning, Suchmaschinen und Soziale Netzwerke überdies, und sehr viel mehr, die großen Internet-Firmen, die Nutzenden und Textgebenden. Immer sind es letztlich Menschen, die entscheiden, welche Algorithmen wo und in welchen Zusammenhängen wie kombiniert und verwendet werden. Es sind Menschen, die etwa unvollständige Datensätze in Programme füttern oder dies an Automaten delegieren; die trotz aller bekannt gewordenen politischen Wirkungen von Hassbotschaften, Echokammern und Fake News *Bots* damit füttern. Für die Wirkung sind weder die Algorithmen noch die benutzten Buchstaben verantwortlich.

Software wirkt immer als Verstärker, von Besonderheiten in Organisationen, hinsichtlich eventueller Bias, Einbindungen oder Auslassungen. Sie vergrößert alle Effekte, die aus den sozialen Zusammenhängen gezogen werden, sie bestätigt und zementiert nicht nur Verhältnisse, sondern reifiziert und vertieft gesellschaftliche Ungleichgewichte. Dies noch unvergleichlich mehr, wenn die Datenprodukte in iterierte und rekursive Prozeduren gefüttert werden, wie dies beispielsweise für Big Data der Fall ist. Zudem werden sie durch die Virtualisierung oft unsichtbar und verfestigen sich. Dringender denn je ist deshalb zu fragen, wieweit es zuträglich ist, unsere Arbeits- und Lebenswelt weiter zu automatisieren. Es ist ein Fehler zu glauben, mit KI, Big Data, Handlungsplänen und Optimierungsverfahren die Welt steuern zu können. Der Menschen zugängliche Umgang mit dem Unerwarteten wird mit der Automatisierung darauf beschränkt, das Mögliche als aufzählbar zu betrachten. Die Zukunft wird dabei auf die De- oder Induktion aus Vergangenem reduziert.

Wir sind es, die wir Daten an soziale Netzwerke liefern und dort Profile erstellen, bestimmte Ansichten durch *liken*, *sharen* etc. verstärken, während wir gleichzeitig Internetdienste umsonst nutzen (wollen); wir, die wir als Informatik-Profession eine ahistorische und angeblich neutrale, vermeintlich objektive Haltung einnehmen. Die Verantwortung bleibt jedoch immer bei uns, auch wenn wir gern die Schuld an andere oder etwas anderes abschieben. Erweitert man aber den Algorithmusbegriff auf jegliche Automatisierung, so weist man individuelle und kollektive Verantwortung als Objektives und Unveränderliches ab.

Ich danke Cecile Crutzen für Anregungen und Verbesserungen an diesem Text, und Jörg Pflüger und Wolfgang Coy für klärende Gespräche darüber.

Anmerkungen

1 *Crutzen CKM (2013) Masks between the Visible and the Invisible. In: Ernst W, Horwath I (eds) Gender in Science and Technology. Interdisciplinary Approaches. Transcript, Bielefeld, pp 79–110*

2 *Im Bereich der Gender Studies wurde später der „ego-approach" von Madeline Akrich in The De-Scription of Technical Objects (1992) Bijker W, Law J (eds) Shaping Technology / Building Society. MIT Press, Cambridge, pp 205–224 als sogenannte „I-methodology" neu entdeckt und wird heute so bezeichnet. Dort betrifft sie allerdings vorzugsweise die Benutzung, die sich Entwickelnde gemäß ihren eigenen Bedürfnissen vorstellen.*

3 *Suchman, L (1987) Plans and Situated Action. The Problem of Human-Machine Communication. Cambridge University Press, Cambridge*

4 *http://www.zeit.de/digital/internet/2015-07/neuronale-netzwerke-google-inception*

5 *Ein anderes KNN hätte u. U. die Differenzierung nicht nach der Hautfarbe treffen können, sondern nach der Kopfform, oder aber auch gar keine für Menschen erkennbare Unterscheidungen.*

6 *Sweeney, L (2013) Discrimination in Online Ad Delivery. CACM 56(5): 44–54*

7 *Custers B, et al. (2013) Discrimination and Privacy in the Information Society. Springer, Berlin*

8 *http://www.washington.edu/news/2015/04/09/whos-a-ceo-google-image-results-can-shift-gender-biases/*

9 *Freie dezentrale verteilte soziale Netzwerke wie Diaspora oder firendica finanzieren sich durch Spenden, ebenso freie Suchmaschinen, wie DuckDuckGo, Wegtam, DeuSu, MetaGer, Unbubble oder ixquick.eu, die jeweils auch Datenschutzaspekte berücksichtigen*

10 *http://www.spektrum.de/kolumne/die-macht-der-algorithmen/1429137, https://www.theguardian.com/politics/2017/feb/26/robert-mercer-breitbart-war-on-media-steve-bannon-donald-trump-nigel-farage*

11 *http://www.theverge.com/2015/7/1/8880363/google-apologizes-photos-app-tags-two-black-people-gorillas*

12 *https://qz.com/653084/microsofts-disastrous-tay-experiment-shows-the-hidden-dangers-of-ai/*

Rainer Rehak und Jens Wernicke

Die Manipulation von Denken und Handeln ist zur treibenden Kraft der IT-Entwicklung geworden

Jens Wernicke interviewt Rainer Rehak, erstveröffentlicht auf dem Nachrichtenportal *nachdenkseiten.de*

In unserer technologisierten Gesellschaft untergraben unsichtbare Systeme zunehmend die individuelle Selbst- und demokratische Mitbestimmung. Das ist kein Zufall, sondern explizit so gewollt: Die Wirtschaft „erzieht" sich ihre Kunden, der Staat sich seine Bürger. So ist die Manipulation von Denken und Handeln längst zur treibenden Kraft der IT-Entwicklung geworden und verkommt die Technik, die uns das Leben erleichtern sollte, mehr und mehr zur Instanz der totalen Kontrolle über uns. Eine Entwicklung, die die Informatikerinnen und Informatiker für Frieden und gesellschaftliche Verantwortung nicht hinnehmen wollen. „Versteckte Informationstechnik ist nicht diskutierbar", kritisiert Rainer Rehak*, einer der Organisatoren der diesbezüglichen Jahreskonferenz[1], im Interview mit* Jens Wernicke*.*

Jens Wernicke (JW): *Herr Rehak, Sie sind im Vorstand des FIfF, dem Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung, und dieses Jahr Mit-Organisator der 32. FIfF-Konferenz, die vom 25. bis 27.11. in Berlin stattfindet und die Gefahren sogenannter „unsichtbarer Systeme" behandeln wird. Als Informatiker und Informatikerinnen, die sich für Frieden engagieren, postulieren Sie im FIfF: „Die Manipulation von Denken und Handeln ist zur treibenden Kraft der IT-Entwicklung geworden." Was bitte sind „unsichtbare Systeme"? Und wer bemüht sich um Kontrolle unseres Denkens und Handelns?*

Rainer Rehak (RR): Das lässt sich am besten anhand eines technischen Beispiels erklären: Früher bestand ein Auto aus Motor, Fahrgestell, Getriebe, Reifen usw. Die komplexesten Dinge waren viel-

leicht der Motor und das Getriebe, aber die waren von der Funktion her eher auch noch verständlich. Der Motor dreht eine Antriebswelle und das Getriebe bringt diese Drehung über die Räder auf die Straße – das Auto fährt. Heutzutage bestehen Autos aus Hunderten von Minicomputern, die den Motor steuern und überwachen, Abgase messen oder die Reifenlage kontrollieren, den Airbag checken und so weiter. Das sind alles hochkomplexe Systeme geworden. Ab 2018 ist es sogar gesetzlich vorgeschrieben, dass neue Autos ein Mobilfunkmodul eingebaut haben müssen.[2]

Tatsächlich sind Autos also fahrende Computer geworden – und das merkt man kaum, was Vor- wie Nachteile hat. Aber damit ist auch erklärbar, wie VW den Diesel-Abgasbetrug durchführen konnte: Die Autosoftware war einfach so „schlau" gebaut, dass sie selbst analysieren konnte, wann das Auto im staatlichen Labor getestet wurde. Dann, und nur dann, hat sie das Auto auf „gesetzeskonform" geschaltet. Damit ist aber der VW kein Einzelfall – solche Entwicklungen betreffen immer mehr Geräte, vom „smarten" Fernseher,[3] der kontinuierlich die Umgebungsgeräusche mitschneidet oder die Sehgewohnheiten aufzeichnet und diese per Internet an seinen Hersteller sendet, über elektronische Fahrkarten, die unsere Wege festhalten[4] bis hin zu raffinierten Methoden programmierter „Selbstzerstörung"[5], die nach einiger Zeit die Nutzer und Nutzerinnen zum Kauf eines neuen Gerätes zwingen. Wir wissen einfach nicht mehr, was diese Dinge wirklich – meist im Hintergrund – tun und für wen sie arbeiten. Darum nennen wir sie „unsichtbare Systeme".

JW: *Das ist durchaus beunruhigend, aber wie beeinflusst das unser Denken und Handeln?*

RR: Deutlich wird der Einfluss dieser „unsichtbaren Systeme", wenn man sich aktuelle Entwicklungen im Internet einmal genauer ansieht. Da bekommt man auf Webseiten etwa individuelle Preise[6] serviert, je nachdem, welche Eigenschaften die Big-Data-Analysen[7] über einen errechnet haben, zum Beispiel ob man aus einer reichen oder armen Gegend die Shop-Seite ansurft oder was ähnliche Konsumenten auch gekauft haben. In der Konsequenz wird einem dann bei Einkäufen beispielsweise immer das nächstteurere Produkt so weit heruntergesetzt, dass man es sich gerade noch leisten kann. Beim Kauf wird dann also jeweils mehr Geld ausgegeben als ursprünglich gewollt. Das heißt, hier ermöglichen es diese Systeme, dass jahrelange Forschung aus Betriebswirtschaft, Informatik und Psychologie direkt auf den nichtsahnenden Kunden angewendet wird. Das funktioniert ziemlich gut, weswegen sich inzwischen auch die Verbraucherzentrale Bundesverband e. V. mit solchen Mechanismen intensiv beschäftigen[8] muss.

Richtig problematisch wird es dann, wenn Menschen Angebote bekommen, die exakt auf sie zugeschnitten sind – sie also nicht nur Informationen enthalten, die beim Empfänger auf Zustimmung stoßen, sondern explizit auch andere Informationen nicht enthalten, die die Person abschrecken würde. Oder sie eben auch ganz explizit für bestimmte Produkte keine Kaufvorschläge bekommen.

JW: *Das verstehe ich nicht. Wieso ist das besonders problematisch?*

RR: Nun, genauso wie man auf diese Art sehr individuell für ein Produkt werben kann, kann man natürlich auch für politische Kandidatinnen und Kandidaten werben. Das Stichwort hier ist „Microtargeting",[9] also das Unterteilen der wahlfähigen Bevölkerung in sehr kleine, teilweise individualisierte Zielgruppen. So kann man einerseits schon gefestigte Personen einfach ignorieren, andererseits sich aber auch speziell auf unentschiedene Wähler stürzen und diese ganz individualisiert ansprechen, beispielsweise explizit jene Positionen eines Kandidaten herausheben, die auch im Interessensbereich des Wählers liegen, oder gezielt Positionen nicht erwähnen, die er kritisch finden würde. Und das bedeutet dann eine gewollt einseitige Informationsweitergabe, abgestimmt auf die individualisierten Datensätze der wählenden Person.

Im Wahlkampf von Obama im Jahre 2008 beruhte die Wahlstrategie unter anderem auf diesem Microtargeting: Es wurden millionenfach Wählerdaten gekauft oder erhoben und auf deren Basis dann individuelle Kontaktstrategien erstellt. Jemand, der also seinem Datensatz nach grün denkt, aber gegen eine allgemeine Krankenversicherung ist und lieber telefoniert als E-Mail zu lesen, bekam daher telefonisch Werbung für Obama, in der wiederum dezidiert von erneuerbaren Energien die Rede war, aber tunlichst nicht von Obamas Versicherungsreformen. Meiner Ansicht nach ist das Manipulation, wenn es wie in diesem Beispiel systematisch betrieben wird. Und wenn es darüber hinaus in solch großem Maßstab erfolgt, finde ich das auch aus demokratischer Sicht hochproblematisch. Man kann an diesem Fall wunderbar sehen, dass diese Technologien bestehende Machtverhältnisse weiter festigen. Unabhängige Kandidaten können sich das nämlich nicht unbedingt leisten.

Gleiches gilt übrigens auch ganz allgemein für Suchergebnisse im Internet. Aktuell wird viel über Facebook und Co. diskutiert, also welche Artikel und Posts wie dargestellt werden, aber der eigentliche Megaplayer Google wird selten erwähnt, dabei erstellt er buchstäblich unsere Sicht auf das Internet. Webseiten, die Google nicht findet, gibt es für uns nicht – so wie wir ein Buch im Regal einer Bibliothek nicht finden, wenn es nicht im Bibliothekskatalog geführt wird. Seiten, die Google besser bewertet und als erste anzeigt, werden nicht nur maßgeblich öfter angeklickt, sondern schon ab Seite 2 sind die Suchergebnisse im Grunde irrelevant. Dahinter steckt eine große unsichtbare Macht.

Das ist auch überhaupt nicht hypothetisch, denn wenn bestimmte Webseiten und Informationen aus dem Google-Index verschwinden sollen, kann man sich mit seiner Begründung einfach direkt an die Suchmaschinenbetreiber wenden.[10] Diese Möglichkeit zu haben ist sicherlich eine gute Idee, denn so lassen sich die vielzitierten bildgewordenen Jugendsünden im Nachhinein unauffindbar machen. Doch damit trifft Google aktuell eine Entscheidung, die eine Abwägung zwischen dem Recht auf Privatheit und dem Interesse der Öffentlichkeit an umfassender Information voraussetzen sollte. Eine Firma fällt demzufolge mitunter rechtsrelevante Entscheidungen nach internen, geheimen Kriterien.

Und selbst wenn alle Informationen im Google-Index zu finden wären, ist die Anzeigereihenfolge immer noch ganz bedeutend. US-amerikanische Wissenschaftler haben – in der Tat! – herausgefunden, dass wir weiter oben stehenden Suchergebnissen unbewusst mehr Wahrheitsgehalt zuschreiben. Das ist sogar dann noch wirksam, wenn zuvor deutlich darauf hingewiesen worden ist.[11]

Drastisch formuliert: Google und Co. bestimmen also maßgeblich, was wir für wichtig und relevant, für glaubwürdig und un-

glaubwürdig halten. Dabei wird sehr deutlich, welche Macht diejenigen haben, die Informationen – vermeintlich in unserem Sinne – vorstrukturieren. Es ist meiner Ansicht nach auch eher zweitrangig, ob sie die Macht aktuell bewusst einsetzen oder nicht – von Softwarefehlern dabei ganz zu schweigen. Allein die Möglichkeit einer solchen Einflussnahme ist Gift für eine Demokratie.

Übrigens sind das auch gar keine abstrakten Gedankenspiele. Suchen Sie mal mit derselben Suchmaschine nach demselben Begriff auf zwei verschiedenen Computern – und Sie werden überrascht sein, wie unterschiedlich die Ergebnisse sind.

JW: *Es ist doch aber, ganz pragmatisch gedacht, andererseits zugleich notwendig, dass die unüberschaubar vielen Informationen auf irgendeine Art und Weise vorsortiert werden, weil sie uns völlig unaufbereitet heillos überfordern würden.*

RR: Natürlich ist das grundsätzlich nützlich und daher auch wünschenswert. Aber es kommt eben darauf an, *wie* solche Prozesse erfolgen und wer sie steuert, mit welchem Ziel und wie nachvollziehbar das geschieht. Diejenigen, die das heute für uns übernehmen, sind ja mächtige internationale Konzerne, die damit ganz eigene Interessen verfolgen – und diese wiederum stehen unseren teilweise durchaus diametral entgegen.

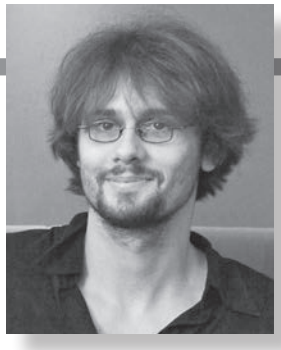
Da sich die NachDenkSeiten viel mit Medienkritik beschäftigen, nehme ich hier mal ein Beispiel aus diesem Bereich: Google und Facebook haben jeweils Funktionen, die den Nutzern und Nutzerinnen zum Beispiel Nachrichten präsentieren. Natürlich müssen diese ausgewählt werden, egal ob von Menschen oder von Algorithmen. Die tatsächlichen Mechanismen, die hier dahinterstehen, sind uns zunächst einmal unbekannt, aber sie sorgen dafür, welche Artikel und Informationen sichtbar oder unsichtbar, weiterverteilt oder vergessen werden. Weder Menschen noch Algorithmen sind dabei übrigens neutral, zweitere tragen ja auch immer die Werte und Wertungen ihrer Software-Entwickler in sich. Dabei kann es sich um eher greifbare Wertungen handeln, wieviel nackte Haut auf Fotos zu sehen sein „darf" zum Beispiel, aber auch um sehr komplexe Einschätzungen, etwa welche politischen Ansichten als „zu extrem" gelten. Und bestimmt werden die Parameter, die diesen Wertungen zu Grunde liegen, letztlich von genau den Medien, deren Nachrichtenauswahl wir lesen.

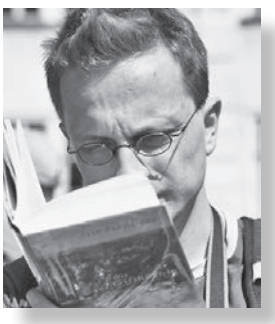
Über die traditionellen Medien wissen wir mittlerweile genug, um in Machtkonzentrationen, wie sie ja Google und Facebook wiederum im digitalen Gefüge verkörpern, immer auch eine Gefahr zu erkennen, weil diese leicht in interessengesteuerte Berichte münden können[12] und leider auch genug dazu geführt haben, dass etwa Kriege erst durch die mediale Steuerung die Akzeptanz der Bevölkerung erhalten haben und so überhaupt nur möglich wurden[13]. Diese Grundprobleme müssen wir gerade bei den Medienakteuren im Internet dringend angehen, denn unregulierte und intransparente Informationstechnik begünstigt noch einmal in ganz anderem Ausmaß das Recht des Stärkeren, seien das „die Märkte" oder politische Kräfte mit „alternativlosen" Lösungen. Aktuell lässt sich sogar eine „Refeudalisierung" des vormals sehr bunten und vielfältigen Internets feststellen. Wenn man sich die weltweiten Nutzungsstatistiken anschaut, besteht das Internet für sehr viele Menschen der westlichen Welt mittlerweile nur noch aus Facebook, Google und YouTube, also hochgradig monopolistischen und vermachteten Webseiten.

JW: *Müsste die folgerichtige Konsequenz also sein, keine Computer mehr für wichtige und persönliche Aktivitäten zu nutzen, besonders als Nachrichtenfilter?*

RR: Natürlich nicht, das wäre ja auch eine merkwürdige Position für einen Informatiker. Aber, Scherz beiseite, die Frage ist doch schon lange nicht mehr, ob wir diese Technik überhaupt nutzen wollen. Es geht darum, wie wir diese Technik gestalten, was sie versteckt oder sogar aktiv verhindert und was sie wiederum offenlegt. Die Frage ist, wie wir dafür sorgen können, dass sie im Dienste der Demokratie und Pluralität wirkt. Für ein besseres Verständnis dieser bisher angesprochenen Probleme und die Entwicklung möglicher Lösungsansätze müssen wir den Blick wieder etwas erweitern.

Rainer Rehak und Jens Wernicke





Rainer Rehak beschäftigt sich seit rund zehn Jahren mit dem Themenfeld *Informatik und Gesellschaft*. Er studierte Informatik und Philosophie in Berlin, Hong Kong und Peking. Während des Studiums arbeitete er am Lehrstuhl für *Informatik in Bildung und Gesellschaft* von Wolfgang Coy. Aktuell lehrt er an der HTW Berlin in den Bereichen *Datenschutz und Datensicherheit, Informatik und Gesellschaft sowie Netzwerke*. In der Wirtschaft ist er als IT-Sicherheits- und Datenschutzberater sowie Unix-Server-Administrator tätig.

Jens Wernicke, Jahrgang 1977, arbeitete lange als Gewerkschaftssekretär und in der Politik. Inzwischen ist er freier Journalist und Geschäftsführer der *Initiative zur Demokratisierung der Meinungsbildung gGmbH*, der Trägergesellschaft des *Rubikon – Magazin für die kritische Masse*. Zuletzt erschien von ihm *Netzwerk der Macht – Bertelsmann. Der medialpolitische Komplex aus Gütersloh* im BdWi-Verlag. In 2017 erscheinen von ihm *Lügen die Medien? Propaganda, Rudeljournalismus und der Kampf um die öffentliche Meinung* im *Westend-Verlag* sowie *Fassadendemokratie und Tiefer Staat* als Mitherausgeber im *Promedia-Verlag*.

Ganz allgemein gesprochen haben wir Menschen ja aus dem Grunde technische Geräte konstruiert, dass wir nicht mehr alles selbst machen und im Detail verstehen müssen. Ich wüsste auch nicht auf Anhieb, wie ich einen Fernseher bauen sollte. Ich möchte einfach, dass er den ersten Sender zeigt, wenn ich die „1" auf der Fernbedienung drücke. Dafür muss ich nichts von Schwingkreisen und Kondensatoren verstehen. Allerdings möchte ich auch nicht, dass die Gerätehersteller ohne mein Wissen Funktionen einbauen, die nur ihnen selbst nutzen, ja, die mir vielleicht sogar schaden, weil sie mich ausspionieren oder meine Handlungsmöglichkeiten unbemerkt einschränken.[14]

Die Snowden-Dokumente haben wunderbar belegt, wie die Geheimdienste der USA technische Geräte präpariert haben, um an Kompromat, also für Erpressungen verwendbares Material über bestimmte wichtige Personen, zu gelangen.[15] Man weiß nie, wann so ein Wissen einmal nützlich sein kann. Das hat ja sogar Angela Merkel selbst zu spüren bekommen, als sie bemerkte, dass sie abgehört wurde.

All diese Dinge haben gemeinsam, dass wir solche hochkomplexen Geräte immer näher in unser persönliches, wirtschaftliches und gesellschaftliches Leben einbinden. Das ist aus meiner Sicht gut so, weil es viele Arbeiten erleichtert. Diese Entwicklung muss aber kritisch begleitet werden, sowohl von Fachleuten in etwa der IT-Branche oder von den Rechtswissenschaften, aber auch von der Gesellschaft als solcher, also auch jedem Einzelnen, damit nicht nur Firmen oder Geheimdienste diese „digitale Welt" gestalten. Daher ist der Untertitel unserer Konferenz auch „Versteckte Informationstechnik ist nicht diskutierbar", denn das ist nicht akzeptabel, wir müssen sie dringend diskutieren.

JW: *Nun geht es bei den Vorträgen auf Ihrer Konferenz unter anderem auch um das Thema „Der Staat als Krimineller" – eine Vorstellung, die vielen sicher abgeht, dass die Obrigkeit demnach aktiv gegen statt für uns arbeitet. Was genau dürfen wir uns unter einem „kriminellen Staat" vorstellen?*

RR: Sie spielen auf unseren Eröffnungsvortrag von Erich Möchel an. Darin wird es um staatliches Hacking gehen, also darum, dass sich Staaten wie selbstverständlich technischer Methoden bedienen, die eigentlich ins Instrumentarium von Kriminellen gehören. Konkret reden wir hier beispielsweise von der Infiltration fremder Computersysteme zum Zwecke der Sabotage von Industrieanlagen, von Energienetzen oder anderen Infrastrukturen. Rechtlich sind diese Aktivitäten auch noch nicht eindeutig interpretiert, denn auf so etwas war das Völkerrecht natürlich nicht direkt vorbereitet; die NATO wiederum hat dazu ebenfalls eine ganz eigene Position, aber das würde hier den Rahmen sprengen.

Jedenfalls haben wir inzwischen mehr oder weniger detaillierte Beschreibungen, was hinter den Kulissen der Staatsmächte passiert, zum Beispiel aus den diversen Dokumenten, die Edward Snowden und andere Whistleblower „befreit" haben. Staaten setzen demzufolge diese hochentwickelte Schadsoftware gegeneinander ein und überbieten sich jeweils mit ihren aggressiven Offensivfähigkeiten. Ein bekanntes Beispiel war das Stuxnet-Virus vor einigen Jahren. Und dabei mischen auch alle großen Staaten gemäß ihren Fähigkeiten mit, egal ob Deutschland, Russland, Israel, die USA oder China.

Es geht also um einen neuartigen, fatalen IT-Rüstungswettlauf, der außer Kontrolle geraten ist und der unsere Geräte im Endeffekt unsicherer macht statt sicherer. Wir alle werden dadurch verwundbarer, durch diesen Machtkampf einiger weniger Akteure. Solche Methoden müssen natürlich dringend gesellschaftlich diskutiert werden, denn sie haben auch schwerwiegende gesellschaftliche Folgen, und genau zu dieser Debatte wollen wir etwas beitragen. Für die Details dazu würde ich Sie allerdings zu Erich Möchels Vortrag einladen, denn auf diesem Gebiet ist er der Experte. Es wird von den Vorträgen übrigens auch einen Live-Stream und danach die Videoaufzeichnung geben.

JW: *Da Sie von Kompromat sprachen … Ich frage mich schon lange, ob der sogenannte „Staatstrojaner", dessen Einsatz sich jedweder demokratischen Kontrolle entzieht, nicht auch dazu genutzt werden kann, Rechner überhaupt erst durch seinen Einsatz so zu manipulieren, dass man dem Besitzer nachfolgend eine Straftat vorwerfen und ihn dafür belangen kann. Was meinen Sie? Ich denke dabei an Folgendes: Wir leben in Zeiten, wo immer klarer wird, dass der NSU offenbar von Dutzenden V-Leuten über Jahre beschützt und abgeschirmt wurde; und in Zeiten, in denen Menschen wie etwa Gustl Mollath, die wichtigen Banken gefährlich werden könnten, mal eben ihrer Bürgerrechte beraubt und psychiatrisiert werden können …*

RR: Grundsätzlich ist der Staatstrojaner im informatischen Sinne erstmal ein normaler Trojaner, der von Behörden eingesetzt werden soll, um Informationen zu sammeln. Ein Trojaner ist eine Software, die beispielsweise über Sicherheitslücken in ein System gelangt und dann dort einprogrammierte Aktivitäten ausführt. Das kann, wie eben erwähnt, eine Informationssuche sein oder aber auch ganz andere Funktionen umfassen. Ich habe vor einiger Zeit selbst zu der grundsätzlichen Beschränkbarkeit solcher Software geforscht und bin zu dem Ergebnis gekommen, dass das, also ihre Beschränkung, effektiv gar nicht möglich ist.[16] Dementsprechend ist gut vorstellbar, dass eine Software wie diese auch bestimmte neue Dateien auf Systemen hinterlegt – dabei ist es auch erst einmal egal, ob das absichtlich, durch Fehler oder aber Dritte erfolgt, die ihre ganz eigenen Interessen verfolgen.

Es gab ja auch schon Viren, die genau das getan haben: beispielsweise Videos von Kindesmisshandlungen auf die Computer von ahnungslosen Personen aufzuspielen,[17] leider sehr folgenreich, wie man sich denken kann. Deswegen ist es so wichtig, dass Computersysteme gut gesichert sind, und zwar gegenüber allen Angreifern.

Aus den USA wissen wir von noch tiefergreifenden Aktivitäten, da erfahren wir von IT-gestützter Spionage der politischen Opposition oder von NSA-Programmen zur Zerstörung der Reputation von prominenten Gegnern der jeweils herrschenden Meinung.[18] Von anderen Ländern wie Russland oder China ist dazu noch wenig bekannt, aber warum sollte es dort anders sein?

Und man muss natürlich auch sehen, dass staatliche Stellen wie die jeweilige Polizei mitunter sicherlich auch gerechtfertigt bestimmte Informationen erlangen sollten, zum Beispiel zur klassischen Verbrechensbekämpfung. Auch darum ist das ein sehr schwieriges Thema, denn ganz ohne polizeiliche Rechtsdurchsetzung geht es ja vielleicht auch nicht in einem Rechtsstaat. Wichtig bleibt dabei, dass die rechtlichen Hürden für solche Methoden

sehr, sehr hoch und klar definiert sein müssen, schließlich haben wir in Deutschland seit dem Urteil des Bundesverfassungsgerichts im Jahre 2008 zur heimlichen Online-Durchsuchung explizit ein „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme". Das interessiert ausländische Geheimdienste natürlich genauso wenig wie sich der BND bei seinen Aktivitäten um die Gesetze anderer Länder schert. Ein Zustand, der schnellstmöglich behoben werden muss.

Aber um auf Ihre Frage zurückzukommen: Natürlich wäre es technisch möglich, inkriminierende Daten auf den Computern von unliebsamen Personen zu platzieren. Ich sehe allerdings ein ganz anderes Problem im Vordergrund. Ich postuliere mal ganz frei, dass jeder Mensch direkt oder indirekt in Aktivitäten verstrickt ist, die – wenn auch nicht unbedingt strafbewehrt – doch mindestens in Teilen der Gesellschaft verpönt oder geächtet sind. Das können kreative Steuermodelle, unübliche Bekanntschaften oder seltene Sexualvorlieben sein. Wenn die staatlichen Stellen und ihre Trojaner nun gut arbeiten, bekommen Sie diese Art von Informationen über alle relevanten Personen heraus und können sich dann bequem aussuchen, wen Sie wie loswerden wollen. Das Perfide daran ist, dass die Dinge, die man dann bei Bedarf an die Öffentlichkeit „gelangen" lässt, alle vollkommen richtig sind und die betroffene Person keine Chance auf Verteidigung hat. Wissen ist Macht!

Und wie bei den zuvor diskutierten Sachverhalten ist auch das keine abstrakte Möglichkeit, sondern bereits heute belegbare Realität. So sammelte[19] die NSA etwa die Erotikvorlieben US-amerikanischer Muslime, natürlich nur für alle Fälle, ohne jede böse Ansicht und so, Sie verstehen schon …

JW: *Gibt es etwas, das Sie „normalen Verbrauchern" wie mir, die wenig IT-Kenntnisse haben, raten? Etwas, womit wir die eigene Manipulierbarkeit ggf. reduzieren können?*

RR: Ein paar Dinge kann man schon tun. Einerseits kann man Software und Internetservices ein wenig so behandeln wie Lebensmittel, die man für sich kaufen würde. Damit meine ich, nicht einfach nur nach der bunten Verpackung einzukaufen, sondern ab und zu einen Blick auf die „Inhaltsstoffe" und „Produktionsbedingungen" zu werfen. Auf die IT-Welt übertragen bedeutet das, nicht nur die Anbieterwerbung zu lesen, sondern auch mal Hintergrundinformationen zur Firma zu recherchieren und mehr über deren Reputation zu erfahren. Wenn das Ergebnis nicht zufriedenstellend ist, kann man nach Alternativen suchen – oder weiß zumindest, woran man eigentlich ist. Und es gibt durchaus Anbieter, die eine kritische Haltung haben, sich fair und transparent ihren Anwendern gegenüber verhalten und offen kommunizieren, wie ihr Geschäftsmodell wirklich funktioniert. Posteo.de für E-Mails oder Uberspace.de für Hosting sind zwei Beispiele dafür. Als Einstieg in die Thematik empfehle ich die Erklärfilme[20] von Alexander Lehmann und das Buch „Die Datenfresser"[21] von Constanze Kurz und Frank Rieger.

Grundsätzlich geht es – wie auch im Medienbereich – vor allem darum, eine kritische Sicht auf IT-Systeme und Internetservices zu entwickeln, diese zu diskutieren und letztlich auf politische Lösungen im Daten- und Verbraucherschutz oder bei der Geheimdienstkontrolle hinzuwirken, damit die digitale Revolution nicht unsere Grundrechte und -freiheiten zerstört, sondern diese sichert.

JW: *Noch ein letztes Wort?*

RR: Wissen Sie, wer kürzlich in einer wesentlichen Datenschutzfrage das mächtige Facebook in die Knie gezwungen hat und damit einen lange bestehenden Vertrag zur Datenweitergabe zwischen Europa und den USA gesprengt hat? Ein österreichischer Jurastudent!

Max Schrems hat letztes Jahr in einer Klage unter Bezugnahme auf die Enthüllungen Edward Snowdens quasi im Alleingang das EU-US-Safe-Harbour-Abkommen zu Fall gebracht, weil er dem Europäischen Gerichtshof schlüssig darlegen konnte, dass die NSA stets und ständig ganz bewusst europäische Datenschutzgesetze missachtet.

Was ich damit sagen will? Wir sind den oben beschriebenen Problemen nicht machtlos ausgeliefert, ganz im Gegenteil. Wir müssen unsere Hausaufgaben machen, dann können wir wirksame öffentliche Diskurse starten, denn die unsichtbaren Systeme können ihre Macht nur entfalten, solange sie unsichtbar bleiben.

JW: *Ich bedanke mich für das Gespräch.*

Vielen Dank auch an Juliane Krüger für ein schlaues Lektorat mit klarem Blick und spitzem Stift.

Links/Verweise

1 *https://www.youtube.com/embed/zDqxA1P4HXg*
2 *http://www.zeit.de/mobilitaet/2015-04/auto-notruf-ecall-verkehrsunfall*
3 *http://www.planet-wissen.de/video-smarte-spione---wie-uns-fernseher-und-co-ueberwachen-100.html*
4 *http://www.golem.de/news/vbb-fahrcard-busse-speichern-seit-mindestens-april-2015-bewegungspunkte-1601-118269.html*
5 *http://www.nachdenkseiten.de/?p=27578*
6 *http://www.tagesspiegel.de/medien/digitale-welt/verbraucherschutz-ein-individueller-preis-fuer-jeden/8353500.html*
7 *https://de.wikipedia.org/wiki/Big_Data*
8 *http://www.vzbv.de/meldung/individuelle-preise-transparent-machen*
9 *https://de.wikipedia.org/wiki/Mikrotargeting*
10 *https://www.verbraucherzentrale.de/recht-auf-vergessen*
11 *https://aeon.co/essays/how-the-internet-flips-elections-and-alters-our-thoughts*
12 *http://www.nachdenkseiten.de/?p=35780*
13 *http://www.nachdenkseiten.de/?p=33071*
14 *https://www.youtube.com/watch?v=OFgQUGTf8BQ*
15 *http://worldnewsdailyreport.com/edward-snowden-the-nsa-steals-and-produces-sex-tapes-to-use-them-for-blackmail/*
16 *https://netzpolitik.org/2012/angezapft-warum-staatstrojaner-mit-gesetzen-nicht-kontrollierbar-und-damit-grundsatzlich-abzulehnen-sind/*
17 *http://www.cbsnews.com/news/viruses-frame-pc-owners-for-child-porn/*
18 *https://theintercept.com/2014/02/24/jtrig-manipulation/*
19 *https://motherboard.vice.com/blog/the-nsa-tracked-porn-habits-to-embarrass-religious-radicals*
20 *https://www.youtube.com/playlist?list=PLQqYRGYVdbVmi3m0kFdLKnHtBwLFEh01N*
21 http://www.fischerverlage.de/buch/die_datenfresser/9783596190331

Deklaration für die Meinungsfreiheit

in Reaktion auf die Verabschiedung des Netzwerkdurchsetzungsgesetzes (NetzDG) durch das Bundeskabinett am 5. April 2017

Meinungsfreiheit hat einen essentiellen und unabdingbaren Stellenwert in einer von demokratischen Werten geprägten Gesellschaft. Das Grundrecht der Meinungsfreiheit ist als Teil der Kommunikationsfreiheiten wie auch die Presse- und die Rundfunkfreiheit in besonderem Maße geschützt. Das Recht auf Meinungsfreiheit findet seine Grenzen erst dort, wo die Rechte und die Würde anderer verletzt werden. Das Recht auf Meinungsfreiheit, aber auch seine Einschränkung, gelten dabei online wie offline.

Zuletzt ist der zulässige Umfang der Meinungsfreiheit in die Diskussion geraten durch den aufgrund zahlreicher Vorkommnisse hervorgerufenen Eindruck, absichtliche Falschmeldungen und Hassrede bestimmten oftmals den öffentlichen Diskurs. Um diesem Phänomen Herr zu werden, hat das Bundeskabinett das Netzwerkdurchsetzungsgesetz (NetzDG) vorgelegt, das vom Deutschen Bundestag noch vor dem Sommer verabschiedet werden soll. Vor diesem Hintergrund möchten die Unterzeichner dieser Deklaration ihre Unterstützung für die folgenden drei Grundsätze zum Ausdruck bringen:

1. Gegen strafrechtlich relevante / rechtswidrige Inhalte muss effektiv vorgegangen werden können. Und zwar mit allen gebotenen und verhältnismäßigen, dem Staat zur Verfügung stehenden Mitteln. Dabei ist es Aufgabe der Justiz, zu entscheiden, was rechtswidrig oder strafbar ist und was nicht. Auch die Durchsetzung solcher Entscheidungen darf nicht an einer mangelnden Ausstattung der Justiz scheitern. Internetdiensteanbietern kommt bei der Bekämpfung rechtswidriger Inhalte eine wichtige Rolle zu, indem sie diese löschen bzw. sperren. Sie sollten jedoch nicht mit der staatlichen Aufgabe betraut werden, Entscheidungen über die Rechtmäßigkeit von Inhalten zu treffen.

2. Die Meinungsfreiheit ist ein kostbares Gut. Sie geht so weit, dass eine Gesellschaft auch Inhalte aushalten muss, die nur schwer erträglich sind, sich aber im Rahmen der gesetzlichen Regelungen bewegen. Die Demokratie nährt sich an einem pluralistischen Meinungsbild.

3. Jede Gesetzgebung sollte sicherstellen, dass der Ausgleich verfassungsrechtlich geschützter Interessen hergestellt wird. Die Meinungsfreiheit jedes Einzelnen und die Informationsfreiheit aller darf nicht darunter leiden, dass gegen rechtswidrige oder strafbare Inhalte vorgegangen wird. Gerade bei solchen Inhalten, bei denen die Rechtswidrigkeit nicht, nicht schnell oder nicht sicher festgestellt werden kann, sollte kein Motto „Im Zweifel löschen/sperren" bestehen, denn ein solches Vorgehen hätte katastrophale Folgen für die Meinungsfreiheit.

Der vom Kabinett beschlossene Entwurf eines NetzDG stellt diese Grundsätze in Frage, weil er staatliche Aufgaben der Rechtsdurchsetzung an Privatunternehmen übertragen würde. Die Androhung hoher Bußgelder in Verbindung mit allzu kurzen Reaktionsfristen verstärkt die Gefahr, dass sich Plattformbetreiber im Zweifel zu Lasten der Meinungsfreiheit und für die Löschung oder Sperrung solcher Inhalte entscheiden, die sich im Graubereich befinden. Die Prüfung der Strafbarkeit oder Rechtswidrigkeit eines Inhalts bedarf zudem regelmäßig einer genauen Betrachtung des Kontexts und der Intention einer Äußerung. Diese Aufgabe muss auch weiterhin von Gerichten übernommen werden.

Wir sind der Auffassung, dass eine politische Gesamtstrategie notwendig ist, um das Aufkommen von Hassrede und absichtlichen Falschmeldungen im Netz einzudämmen. Wir erkennen an, dass Handlungsbedarf besteht, sind zugleich aber der Ansicht, dass der Gesetzentwurf nicht dem Anspruch genügt, die Meinungsfreiheit adäquat zu wahren. Im Gegenteil, er stellt die Grundsätze der Meinungsfreiheit in Frage. Absichtliche Falschmeldungen, Hassrede und menschenfeindliche Hetze sind Probleme der Gesellschaft und können daher auch nicht durch die Internetdiensteanbieter allein angegangen werden – dafür bedarf es der Kooperation von Staat, Zivilgesellschaft und der Anbieter. Wir setzen uns daher für eine gesamtgesellschaftliche Lösung ein, durch die strafwürdiges Verhalten konsequent verfolgt wird, Gegenrede und Medienkompetenz gestärkt werden und ein die Meinungsfreiheit respektierender Rechtsrahmen für die Löschung oder Sperrung rechtswidriger Inhalte erhalten bleibt.

Unterzeichner (Stand: 25. Juni 2017)

Amadeu-Antonio-Stiftung; Bitkom; BIU – Bundesverband Interaktive Unterhaltungssoftware; Bundesverband Deutsche Startups; BVDW – Bundesverband Digitale Wirtschaft; BITMi – Bundesverband IT-Mittelstand; Chaos Computer Club; #C Netz; D64 – Zentrum für Digitalen Fortschritt; Digitale Gesellschaft; DJV – Deutscher Journalisten-Verband; eco – Verband der Internetwirtschaft; FSM – Freiwillige Selbstkontrolle Multimedia-Diensteanbieter; Internet Society – German Chapter; LOAD – Verein für liberale Netzpolitik; Open Knowledge Foundation Deutschland; Reporter ohne Grenzen; Wikimedia Deutschland; Arbeitskreis Zensur; DeutscherAnwaltVerein; Deutscher Kulturrat; DPV – Deutscher Presse-Verband; FITUG – Förderverein Informationstechnik und Gesellschaft; FIfF – Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung; GI – Gesellschaft für Informatik; GMK – Gesellschaft für Medienpädagogik und Kommunikationskultur; HDE - Handelsverband Deutschland; Verbraucherzentrale Sachsen; Dr. Ulf Buermeyer, LL.M., Vorsitzender der GFF – Gesellschaft für Freiheitsrechte; Dr. Frederik Ferreau, Wissenschaftlicher Mitarbeiter, Universität zu Köln; Prof. Dr. Hubertus Gersdorf, Rechtswissenschaftler; Joerg Heidrich, Rechtsanwalt; Prof. Dr. Jeanette Hofmann, Politikwissenschaftlerin; Prof. Dr. Thomas Hoeren, Rechtswissenschaftler; Prof. Niko Härting, Rechtsanwalt; Sabine Leutheusser-Schnarrenberger, Bundesjustizministerin a.D.; Jan Mönikes, Rechtsanwalt; Prof. Dr. Dr. h.c. Ingolf Pernice, Rechtswissenschaftler; Stephan Schmidt, Rechtsanwalt

https://deklaration-fuer-meinungsfreiheit.de/

TRUST – Wem kann ich trauen im Netz und warum?

33. FIfF-Konferenz (#FIfFKon17), 20. bis 22. Oktober 2017, Universität Jena

Vortragende:

- Prof. Dr. *Gabriele Schade* (MDR-Rundfunkrat)
- Prof. Dr. *Dorina Gumm* (Fachhochschule Lübeck)
- Dr. *Lutz Hasse* (Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit)
- *Hannes Mehnert* (University of Cambridge)
- *Thomas Gruber* (Cyberpeace-Kampagne/IMI Tübingen/ Universität Bremen)
- sowie *Felix Baral-Weber*, *Stefan Jäger*, *Sylvia Johnigk*, *Kai Nothdurft, Carlo Schäfer, Sascha Turban*, …

Geplante Workshops:

- *„Algorithmen"*
- *Handys, aber sicher*
- *IANUS-Workshop*
- *IT-Sicherheit barrierefrei*
- *Spielerische Hands-on-Demonstration der Wirkmechanismen und Risiken von F2P-Spielen*
- *Volkszählung – Zensus – Zensus-Vorbereitungs-Gesetz*
- *Wardriving (mit Stadtbegehung)*

Laufend weitere Informationen unter: *https://2017.fiffkon.de*

Einladung zur Mitgliederversammlung 2017

des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF e. V.)

Wir laden fristgerecht und satzungsgemäß zur ordentlichen Mitgliederversammlung 2017 ein.

Sie findet am Sonntag, den 22. November 2017, von 12:30 bis 14:00 Uhr statt.
Adresse: Friedrich-Schiller-Universität Jena, Carl-Zeiss-Str. 3, 07743 Jena
Der betreffende Raum wird rechtzeitig am Eingang angeschlagen sowie auf *www.fiff.de* veröffentlicht.

Vorläufige Tagesordnung

1. Begrüßung, Feststellung der Beschlussfähigkeit und Festlegung der Protokollführung
2. Beschlussfassung über die Tagesordnung, Geschäftsordnung und Wahlordnung
3. Bericht des Vorstands einschließlich Kassenbericht
4. Bericht der Kassenprüfer
5. Diskussion der Berichte
6. Entlastung des Vorstands
7. Neuwahl des Vorstands
8. Neuwahl der Kassenprüfer
9. Diskussion über Ziele und Arbeit des FIfF, aktuelle Themen, Verabschiedung von Stellungnahmen, Berichte aus den Regionalgruppen
10. Anträge an die Mitgliederversammlung
    Anträge müssen schriftlich bis drei Wochen vor der Mitgliederversammlung bei der FIfF-Geschäftsstelle eingegangen sein
11. Verschiedenes

gez. Stefan Hügel
für den Vorstand und die Geschäftsstelle des FIfF

Kurzfilm: Cyberpeace statt Cyberwar

FIfF präsentiert Film gemeinsam mit Motion Ensemble

9. Mai 2017 – Eine besondere Premiere fand am zweiten Tag der re:publica 17 statt: Das FIfF stellte gemeinsam mit dem Animationsfilmduo Motion Ensemble unseren neuen Kurzfilm Cyberpeace statt Cyberwar *vor. Der Film warnt eindringlich vor den Gefahren eines Cyberkriegs und erklärt, wie ein solcher Krieg ablaufen würde. Der Film ist unter* https://vimeo.com/216584485 *sowie* https://youtu.be/St955HBD-7k *abrufbar.*

Durch die Digitalisierung der Gesellschaft sind IT-Systeme heute weit verbreitet. Das „Internet of Things" durchzieht unser gesamtes Alltagsleben. Damit werden wir alle zum Angriffsziel: Computer und Mobiltelefone, aber auch Haustechnik, Automobile oder öffentliche Infrastruktur können durch Schadsoftware in Cyberwaffen verwandelt werden.

Cyberpeace statt Cyberwar

Sylvia Johnigk, Sprecherin der Cyberpeace-Kampagne und Vorstandsmitglied des FIfF, erläutert: „Cyberkriege werden durch Schadprogramme geführt, die Sicherheits-Schwachstellen in digitalen Systemen ausnutzen. Solche Schwachstellen sind in jedem System vorhanden oder werden durch den Angreifer selbst geschaffen. Bekannte Schwachstellen werden nicht beseitigt, sondern geheim gehalten und später für Angriffe ausgenutzt. Diese Praxis bedroht unsere gesamte Gesellschaft."

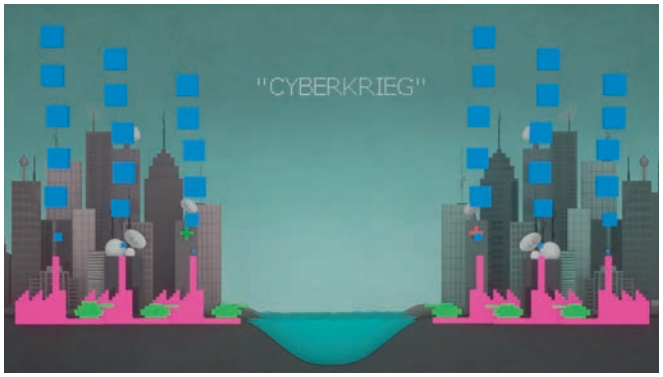
Stefan Hügel, Vorsitzender des FIfF-Vorstands, ergänzt: „Auch deutsche Behörden sind an diesem Spiel beteiligt. Dem Militär und Geheimdiensten werden erhebliche Steuermittel zur Verfügung gestellt, um Schwachstellen auf dem Markt zu kaufen. Anstatt für die Sicherheit der Bevölkerung zu sorgen, indem diese Schwachstellen beseitigt werden, nutzt man sie für spätere Angriffe. Das ist unverantwortlich und gefährlich."

Cyberwaffen können nicht kontrolliert werden, wenn sie erst einmal freigesetzt sind. Ihr Urheber kann nicht ermittelt werden; er bleibt im Anonymen. Letztlich kosten sie große Summen an Steuergeldern und schaden uns mehr als sie uns nutzen.

Das FIfF fordert, dass Cyberwaffen auf rein defensive Zwecke beschränkt bleiben. Sie dürfen weder hergestellt, noch gehandelt, noch für offensive Zwecke eingesetzt werden. Deutschland muss auf eine offensive Cyberstrategie verzichten, sich verpflichten, keine Cyberwaffen zu entwickeln und zu verwenden und internationale Abkommen zu einem weltweiten Bann von Cyberwaffen müssen angestrebt und gefördert werden. Mit seiner Kampagne Cyberpeace setzt sich das FIfF für diese Forderungen ein.

Pressemitteilung: FIfF e. V.; Bilder und Untertitel: Motion Ensemble / Alexander Lehmann im Auftrag des FIfF

Den gewöhnlichen Krieg kennen wir ja …

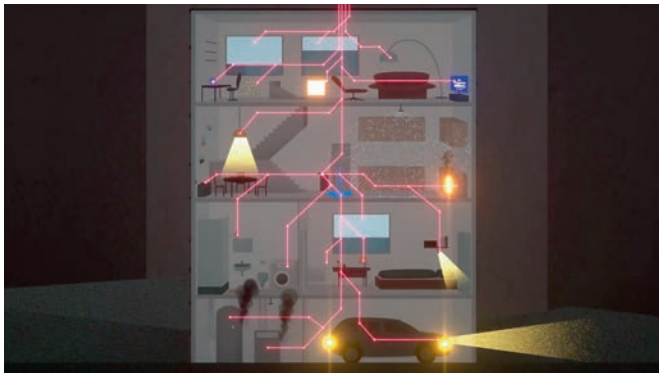


… einfach ein paar Fabriken bauen, und dann am Fließband Cyberwaffen produzieren, funktioniert nämlich nicht …

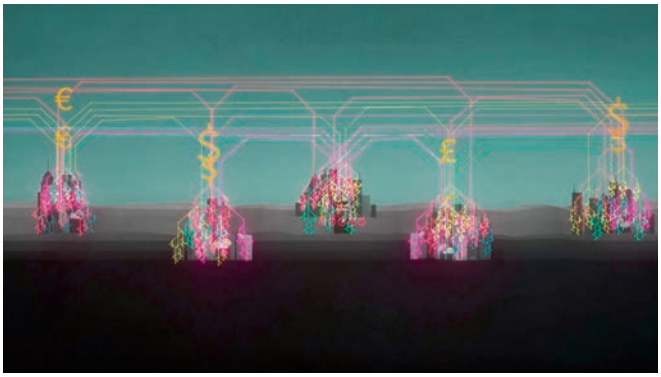
… Cyberkrieg-Aufrüstung besteht also primär darin, bei allen potenziellen Gegnern deren Netze, Einrichtungen und Geräte nach möglichen Schwachstellen zu durchsuchen …

Der Film wurde möglich gemacht durch die Unterstützung der Stiftung Bridge und **Eure Spenden**. Er ist noch nicht vollständig finanziert. Bitte unterstützt uns weiter, damit wir diesen und weitere Filme finanzieren können. Jede Spende hilft uns dabei, uns für eine friedliche Welt und Cyberpeace einzusetzen.

Spendenkonto: Bank für Sozialwirtschaft (BFS) Köln
IBAN: DE79 3702 0500 0001 3828 03; BIC: BFSWDE33XXX



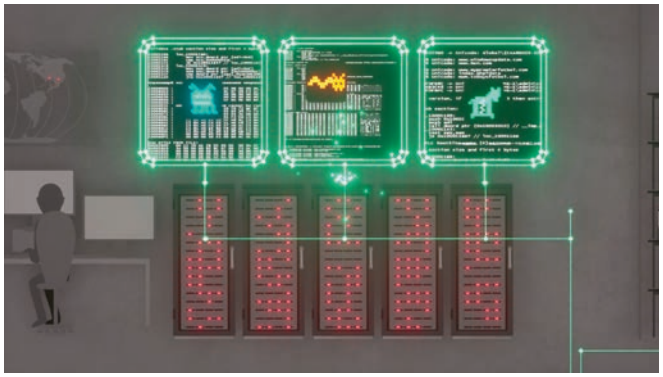
… sich vorzustellen, was passieren kann, wenn jeder PC, jeder Router, jedes Telefon, jede kleine und große Steuerungsanlage und mittlerweile auch Autos, Haushaltsgeräte, und bald sogar unser Zuhause zu einer potenziellen Cyberwaffe werden kann …



… weltweit werden riesige Mengen an Geld dafür ausgegeben, unsere kritische Infrastruktur absichtlich unsicher und verwundbar zu halten …

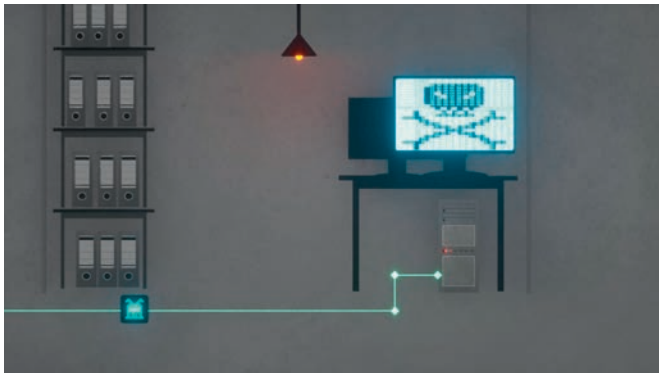
… in einem weltumspannenden virtuellen Netz wie dem Internet lässt sich niemals mit Sicherheit feststellen, wer der wirkliche Verursacher eines Angriffs ist …

… und diese Schwachstellen können natürlich auch von Kriminellen, wie Betrügern und Terroristen, gefunden und gegen uns eingesetzt werden …



… Schadprogramme, wie Würmer, Viren und Trojaner werden in vielen Fällen so programmiert, dass sie ein wehrhaftes Eigenleben führen …

… wir alle würden besser und sicherer leben, wenn unsere Regierungen das Geld zum Schließen der Lücken verwenden würden und nicht zum absichtlichen Offenhalten …



… Waffen dieser Art können sogar für mehrere Jahre unentdeckt in Systemen schlummern, bevor sie Schaden anrichten …

cyberpeace.fiff.de, gefördert durch die Stiftung Bridge

Sebastian Nemetz

Überblick über staatliche Spähsoftware

Stuxnet, Red October, Flame – *von Staaten entwickelte Schadsoftware, auch* Milware *genannt, unterscheidet sich in Aufbau und Funktionalität von nicht staatlicher Malware. Dieser Beitrag beleuchtet Charakteristiken von Milware, anwendbare Analysemethoden sowie Konsequenzen des Einsatzes von Milware und gibt anhand von sieben konkreten Beispielen einen fundierten Überblick über deren Verbreitungsweise, Exploits, technische Funktionsweise und tatsächlich bisher erreichte Fähigkeiten. Der Fokus liegt auf Milware, die durch akademische oder andere zuverlässige Quellen analysiert und dokumentiert wurde. Es werden auch Einsatzzwecke, Urheber und Opfer der jeweiligen Milware behandelt.*

In den letzten zehn Jahren waren Regierungen und Geheimdienste für Entwicklung und Verbreitung vieler hochkomplexer Schadprogramme (Malware) verantwortlich. Nicht nur deren Einsatz ist eine neue Herausforderung für den Bereich der Informationssicherheit, staatliche Schadsoftware stellt auch eine neue Dimension von Malware hinsichtlich ihrer Komplexität und Zielsetzung dar. Sie unterscheidet sich in vielen Punkten von herkömmlicher, nicht staatlicher Malware, weswegen für diese Kategorie der Begriff *Milware* eingeführt wurde[1]. Aufgrund des rechtlichen Status von Regierungen und der zur Verfügung stehenden finanziellen und personellen Ressourcen haben Staaten gegenüber nicht staatlichen Organisationen im Hinblick auf Innovationskraft, Vielfalt und Umfang einen enormen Vorteil bei Entwicklung und Einsatz ihrer Schadsoftware, weswegen Milware auch durch deutlich höheren Entwicklungsaufwand gekennzeichnet ist. Die Einführung des Begriffs vereinfacht eine Kategorisierung der von Sicherheitsfirmen gefundenen Programme zum Zwecke der Spionage (mitunter auch zur Zerstörung), deren Urheber Geheimdienste oder militärische Organisationen sind. Diese Programme werden auch dann als Milware bezeichnet, wenn sie zwar staatlich in Auftrag gegeben und genutzt werden, die Entwicklung aber an private Unternehmen ausgelagert worden ist.[2]

Der Begriff *Cyberwaffe* (*cyber weapon*) wird fälschlicherweise häufig synonym zu Milware gebraucht. Als Cyberwaffen werden nur die Schadprogramme bezeichnet, welche darauf ausgelegt sind, physischen oder logischen Schaden anzurichten. Während etwa Stuxnet eindeutig dazu zählt, gehört die meiste Milware/Malware nicht zu den Cyberwaffen, da sie zur Spionage und für Informationsdiebstahl entworfen wurde[2].

Um Milware ranken sich viele Mythen, staatlicher Schadsoftware werden oftmals enorme Fähigkeiten zugesprochen. In nachfolgenden Analysen wird dargelegt, wie die Quellenlage allgemein für die jeweilige Milware ist, welche Erkenntnisse durch akademische Quellen gesichert und zu welchen Ergebnissen andere Untersuchungen gekommen sind.

Unterschiede zwischen Malware und Milware

Malware versucht nach dem Gießkannenprinzip, eine möglichst große Verbreitung zu erlangen, um möglichst oft ihren Schadcode ausführen zu können.[1] Milware hingegen hat meist eine kleine Zielgruppe und sucht in erster Linie Zugriff auf spezielle Rechner, um zu einem späteren Zeitpunkt ihre Wirkung entfalten zu können. Auch bei Datendiebstahl und anderen nicht zerstörerischen Funktionen ist die Zielsetzung bei Milware eine nicht kommerzielle, während Malware häufig finanziellen Interessen dient.

Christoph Scholz, CC BY-SA 2.0

Bisher versuchte man die Unterschiede zwischen staatlichen und nicht staatlichen Programmen durch Begriffe wie *Codekomplexität* auszudrücken. In einem neuen Ansatz generiert Trey Herr mit Hilfe einiger Metriken einen *MAlicious Software Sophistication Index*, kurz *MASS Index*, mit dem man Code als staatlich oder nicht staatlich klassifizieren können soll.[2] Dieser orientiert sich an funktionalen Gesichtspunkten und es werden High-Level-Charakteristiken wie Architektur und Verhaltensmerkmale der Schadsoftware zu Rate gezogen. Der *MASS Index* ist allerdings nicht als quantifizierendes Tool gedacht, sondern hat das Ziel, von qualitativer und deskriptiver Natur zu sein.

Ferner gilt es natürlich zu beachten, dass nicht nur zwischen staatlicher und nicht staatlicher Software eine Trennlinie verläuft, sondern auch zwischen Staaten: Werkzeuge aus Italien, Pakistan, Nordkorea, den USA oder China unterscheiden sich erheblich in ihrer Qualität. Selbst zwischen verschiedenen Organisationen eines Staates gibt es Unterschiede in der Ziel- und Umsetzung.[2]

Analyse: Propagation, Exploits und Payload

Bei der Analyse von Schadsoftware konzentrierte man sich bisher auf einzelne, funktionale Komponenten im Code. Herrs Vorgehen hingegen ist ein Top-Down-Ansatz: In seinem Framework *PrEP* untersucht er die Verbreitungsmethode (*Pr*opagation method), die *E*xploits und den *P*ayload[3]. Eine ähnliche Aufteilung wird in diesem Beitrag bei der Analyse einiger Exemplare im konkreten Teil vorgenommen.

Bei der *Verbreitungsmethode* werden die Wege aufgezeigt, mit denen die Schadsoftware auf das Zielgerät gelangt. Mögliche Beispiele hierfür sind schadhafte E-Mail-Anhänge, eine kompro-

mittierte Webseite, ein infizierter USB-Stick oder auch die Auslieferung mit Hilfe eines *Droppers* (Schadcode kann gleich zusammen mit einem anderen Programm, dem *Dropper*, auf dem Zielsystem installiert oder darüber zu einem späteren Zeitpunkt nachgeladen werden).

Exploits sind die Codeteile, mit denen Sicherheitslücken ausgenutzt werden und die Schadsoftware sich im Zielgerät einnisten kann.

Der *Payload* bezeichnet das Kernstück der Malware, also das, was ausgeführt werden soll, sobald der entsprechende Rechner unter Kontrolle gebracht wurde. Alles ist denkbar: Datendiebstahl, Erstellen einer *Backdoor*, Überwachung einer angeschlossenen Kamera – bis hin zur Manipulation von Programmen, um Hardware zu zerstören.

Eine Trennung zwischen Exploit und Payload vorzunehmen, ist äußerst sinnvoll, wenn man sich den Entwicklungsprozess vor Augen führt. Exploits können sowohl selbst gefunden als auch von externen Quellen (z. B. im Internet) gekauft werden. Exploits öffnen die Tür für das Ausführen des Payloads – das bloße Erlangen einer Root-Shell an sich hat noch keinen Effekt. Das, was durch den Payload ausgeführt wird, ist der Grund, weswegen man in den Rechner eindringt. Ohne Exploit könnte also der Payload nicht auf den Zielrechner gelangen und seine Schadfunktion ausführen; ohne Payload hingegen wäre ein Exploit noch ohne schadhafte Folgen.

Ausblick und Beispiele für staatliche Schadprogramme

Nun werden einige Beispiele für Milware näher beleuchtet, zunächst *Stuxnet*, der prominenteste Vertreter. Stuxnet erreichte als erste Milware weltweite Aufmerksamkeit, als sie physischen Schaden in Industrieanlagen verursachte, welche scheinbar vom Internet getrennt betrieben wurden.[4] Im Anschluss werden Stuxnets Nachfolger *Duqu* und dessen Nachfolger *Duqu 2.0* betrachtet, ebenso wie *Flame* und *Gauss*, die beide in Verbindung zu Stuxnet stehen und zusammen mit Duqu als *Cousins* von Stuxnet bezeichnet werden[4]. Da bisher nur Milware aus dem angelsächsischen Raum bzw. *dem Westen* behandelt wurde, folgt die Betrachtung einer Milware aus dem osteuropäischen Raum (*Red October)*, ehe der Überblick mit dem erst 2014 entdeckten *Regin* abgerundet wird. Für alle sieben liegen entweder akademische Untersuchungen vor oder sie wurden von Teams analysiert und dokumentiert, die für Hersteller von Anti-Virus-Produkten arbeiten; die Information aller nachfolgenden Besprechungen basiert auf diesen Untersuchungsergebnissen. Sofern Information nicht gesichert oder spekulativer Natur ist, wird dies klar gekennzeichnet. Dateien von Stuxnet stehen außerdem im Internet auf der Plattform *archive.org* zum Download bereit[5] und könnten von jedermann untersucht werden; die Binärdateien anderer Milware sind nicht ohne weiteres im Internet zu finden.

1 Stuxnet

Im Juni 2010 wurde von Mitarbeitern der belarussischen Firma *VirusBlokAda* eine Schadsoftware entdeckt, welche sie als *RootkitTmphider* bezeichneten; wenig später wurde immer mehr über den Computerwurm bekannt, der fortan *Stuxnet* genannt wurde. Am 30. September 2010 veröffentlichte *Symantec* ein – inzwischen mehrfach überarbeitetes – Dossier über Stuxnet, in dem die bisherige Faktenlage aus technischer Sicht zusammengefasst wurde.[6] Dieses Dossier, basierend auf Analysen des Wurms, ist auch im akademischen Bereich die Hauptquelle für die technische Funktionsweise von Stuxnet und dient als Referenz für die technischen Hintergründe, wie sie in diesem Abschnitt skizziert werden. Aufgrund der unzähligen Infektionen im Iran und den dortigen Schäden gilt als gesichert, dass die Angriffsziele von Stuxnet die iranische Urananreicherungsanlage in Natanz und das Kernkraftwerk in Buschehr waren.

Grundlegender Aufbau der Anlagen

Um die Funktionsweise dieses Wurms nachvollziehen zu können, wird zunächst erläutert, wie solche Anlagen grundsätzlich aufgebaut sind. In heutigen Industrieanlagen werden technische Prozesse mittels Computerprogrammen gesteuert und überwacht, sogenannte *SCADA*-Systeme (*Supervisory Control and Data Acquisition*). Klassischerweise bestehen Automatisierungsanwendungen aus folgenden Komponenten: Sensoren und Aktoren messen bzw. manipulieren den technischen Prozess, die Information wird einem Controller zugeführt. Ferner existiert ein *Human Machine Interface* (HMI), das eine Schnittstelle zu Mitarbeitern vor Ort darstellt. Des Weiteren kann eine Schnittstelle zu Fernwartungszwecken bereitstehen, so dass ein externer Zugang zu Sensoren, Aktoren oder Controller vorhanden ist.

Im konkreten Fall war Siemens' System *Simatic* (*Si*emens Auto*matic*) im Einsatz: Dessen Herzstück bildet die Speicherprogrammierbare Steuerung (SPS). Die Software zur Programmierung der SPS heißt *STEP 7* und die Geräte, die zur Programmierung verwendet werden, sind *Field PGs* (SIMATIC Field PG). Siemens verwendet als Prozessleitsystem *SIMATIC PCS 7* und stellt überdies Bedien- und Beobachtungssysteme *SIMATIC HMI* zur Verfügung. Auf diesen ist die Visualisierungssoftware *WinCC* installiert, welche unter Windows läuft.

Vorgeschichte: Stuxnet 0.5

Anfang 2013 tauchte eine weitere Version von Stuxnet auf, welche fortan als *Stuxnet 0.5* bezeichnet wurde. Es handelte sich um die älteste gefundene Version, welche bewies, dass Stuxnet älter war, als man zunächst angenommen hatte. Symantec analysierte die Version und veröffentlichte die neuen Erkenntnisse in einem Whitepaper.[7]

Bereits im November 2005 wurde demnach ein *Command-and-Control-Server* registriert und spätestens seit dem 15. November 2007 war Stuxnet 0.5 in Umlauf. In dieser Vorversion wurden Ventil-Steuerungen sabotiert, um die Verteilung von Uranhexafluorid-Gas zu kontrollieren. Der Druck in den Zentrifugen-Kaskaden wurde um das Fünffache erhöht, um so die Gerätschaften zu zerstören.[8]

Stuxnet 0.5 wurde so programmiert, dass es ab dem 4. Juni 2009 keine weiteren Systeme infizierte, so dass ab Juni 2009 die

Variante 1.001 aktiv werden konnte, die man zunächst für die erste Stuxnet-Version hielt. Im Folgenden geht es nun um die *Hauptversionen* (1.x) von Stuxnet.

Infektionswege und Exploits

Stuxnet hatte mehrere Möglichkeiten, sich einzunisten und zu verbreiten. Insgesamt wurden drei Schichten befallen:

1. Windows-Betriebssystem
2. Siemens PCS-7, WinCC und STEP 7
3. Siemens S7 SPS

Stuxnet wurde ursprünglich durch USB-Sticks in Umlauf gebracht. Hierfür wurde ein erster *Zero-Day-Exploit* verwendet, welcher das fehlertolerante Parsen der *autorun.inf* ausnutzte. Ferner soll im Iran ein Mitarbeiter einen infizierten Stick absichtlich in die Anlage gebracht haben.[9] Nach der Erstinfektion wurde nun – je nach System – ein zweiter Zero-Day-Exploit für eine Privilegeskalation genutzt. Bis zur Version Windows XP SP2 nutzte Stuxnet dazu einen Fehler im Kernel-Mode-Treiber *win32k.sys*, in neueren Versionen eine Lücke im Task-Scheduler. Danach sollte der Schadcode in installierte Antiviren- und Windows-Systemdienste injiziert werden, ehe die eigentliche Installation in einem eigenen, vom kompromittierten System als vertrauenswürdig eingestuften Prozess ausgeführt wurde. Damit das *Rootkit* einen Neustart überleben konnte, wurden Treiber-Dateien mittels gestohlener Zertifikate der Firmen *JMicron* und *Realtek* eingeschleust. Das Betriebssystem prüft die Unterschriften, um zu verhindern, dass sich Schadsoftware im Systeminneren installieren kann. Durch die beiden gestohlenen – aber eben korrekten – Signaturen hielt das Betriebssystem Stuxnet für unschädlich und ließ die Installation zu. Anschließend verbreitete sich Stuxnet im LAN und aktualisierte sich gegenseitig. Dies war auch ohne Internetverbindung möglich. Neben Peer-to-Peer-Updates verbreitete sich Stuxnet auch über Dateifreigaben und einen Zero-Day-Exploit bei Microsofts Druckerfreigaben.

Auf der zweiten Ebene wurden STEP 7-Projektdateien infiziert. Die Schwachstelle lag hierbei in fest einprogrammierten Logins in der WinCC-Datenbank-Software. Hauptaktivität war ein *Hook* der Datei *s7otbxdx.dll*, einer zentralen Bibliothek, mit der die Kopplung einer SPS mit einer Step 7-Anwendung oder einem Field-PG stattfindet. Diese wurde durch die Veränderung eines Buchstabens in *s7otbx**s**x.dll* umbenannt und durch eine eigene *s7otbxdx.dll* ergänzt. Somit konnten Schreib- und Lesezugriffe zur SPS überwacht werden.

Auf dritter Ebene fand nur bei speziellen Hardwarebausteinen eine Manipulation statt, auf die hier nicht näher eingegangen werden muss. Die Stuxnet-Variante A konnte Frequenzumformern der finnischen Firma *Vacon*, die Variante B dem Hersteller *Fararo Paya* (Teheran) zugeordnet werden.[6] Frequenzumrichter regeln unter anderem die Geschwindigkeit von Motoren. Für eine noch detailliertere Analyse wird auf Symantecs Dossier verwiesen.[6]

Payload

Wie konnte Stuxnet nun Schaden anrichten? In unregelmäßigen Abständen zwischen 13 Tagen und drei Monaten wurde die von den bereits angesprochenen Umformern einzustellende Frequenz geändert. Dies war eine grundlegende Neuerung zu Stuxnet 0.5: Anstatt die Zentrifugen durch Manipulation der Rotationsgeschwindigkeit zu zerstören, wurde der Druck in den Zentrifugen erhöht, so dass das Ergebnis nach einem Alterungsprozess aussah und nicht nach einer Zerstörung. Um die Manipulation vor den Mitarbeitern in Natanz zu verbergen, spielte die Milware eine vor der Manipulation aufgezeichnete, 21 Sekunden lange Messwert-Sequenz in einer Schleife in das Kontrollsystem ein. Im Anschluss veränderte Stuxnet nach und nach den Druck in der Anlage.[10]

Folgen

Die internationale Atomenergieorganisation (IAEO) stellte bei Kontrollen im Iran mehrere Produktivitätseinbrüche bei den Zentrifugen-Kaskaden von Januar bis August 2009 fest, obwohl sich die Anzahl an Zentrifugen vergrößerte. Ferner mussten insgesamt knapp 1000 Zentrifugen ausgetauscht werden.[11] Es wird vermutet, dass die Störungen das Werk von Stuxnet und der Vorversion waren. Im November 2010 gab Irans Präsident Mahmoud Ahmadinejad zu, dass das iranische Atomprogramm sabotiert wurde und es bei einer begrenzten Anzahl Zentrifugen zu Problemen kam.[12]

Auch wenn die Mehrzahl der Infektionen im Iran stattfand, breitete sich Stuxnet weltweit aus. In Deutschland waren 59 Prozent der befragten Strom-, Gas- und Wasserversorger von Stuxnet befallen, im internationalen Durchschnitt „nur“ 41 Prozent.[13] Stuxnet richtete aber keinen Schaden in Anlagen an, die nicht Ziel dieser Cyberattacke waren.

Urheber

Mit über 100.000 Zeilen Code, vier Zero-Day-Exploits, einem Windows-Rootkit, der ersten SPS-Schadsoftware, Antivirus-Umgehungstechniken, komplexer Prozessinjektion und Hooking-

Sebastian Nemetz

Sebastian Nemetz absolvierte sein Bachelor- und Masterstudium der Informatik mit dem Schwerpunkt IT-Sicherheit an der Friedrich-Alexander-Universität Erlangen-Nürnberg und arbeitet seit diesem Jahr bei einem Münchner IT-Sicherheitsunternehmen als IT-Berater und Penetrationstester.

code, zwei gestohlenen Signaturen, Netzwerkinfektionsroutinen, Peer-to-Peer-Updates und Command-and-Control-Interface war Stuxnet der bisher komplexeste Wurm, so dass seine Kosten im sieben- bis achtstelligen Bereich lagen und das Projekt in diesem Umfang nur von Staaten zu realisieren war.[14]

Als Urheber gelten die Vereinigten Staaten von Amerika und Israel. Auch wenn beide das nicht offiziell bestätigt haben, gibt es kaum Zweifel daran. Im Jahr 2013 wurde ein Verfahren gegen General James Cartwright (2007 bis 2011 stellvertretender US-Generalstabschef) eingeleitet, da er geheime Informationen über die Stuxnet-Attacke an die *New York Times* weitergegeben haben soll.[15] Dies ist ein weiteres Indiz dafür, dass die Attacke unter Beteiligung der USA ausgeführt wurde.

Dass das Ziel die Sabotage der Atomanlagen im Iran war, ist aufgrund der Vielzahl der Infektionen im Iran und den genauen Angaben über die Hardwarebausteine in den betreffenden Anlagen, auf die Stuxnet exakt zugeschnitten war, unbestritten. Neben diversen Spekulationen ist ein Indiz für die israelische Beteiligung, dass sich in Dimona baugleiche Zentrifugen befinden, an denen der Wurm hätte getestet werden können.[16]

Neue Erkenntnisse 2016: Nitro Zeus

Durch den Dokumentarfilm *Zero Days* kamen Anfang 2016 neue Erkenntnisse über Stuxnet ans Tageslicht. Der Film behauptet, dass Stuxnet Teil eines viele Millionen schweren Programms namens *Nitro Zeus* war, dessen Ziel es war, die komplette zivile Infrastruktur des Irans zum Erliegen bringen zu können.[17] Im Falle eines Krieges hätten so Stromversorgung, Kommunikationsnetze und weitere zentrale Infrastruktur lahmgelegt und der Iran ohne militärisches Eingreifen geschwächt werden können. US-Geheimdienstler geben zudem den Israelis die Schuld an der Aufdeckung von Stuxnet, da diese den Wurm eigenmächtig verändert und eine sich aggressiver verbreitende Variante eingesetzt hätten. Recherchen der New York Times kamen zum gleichen Ergebnis und stützten die Thesen aus Zero Days.[18]

2 Duqu

Nun wird die Milware *Duqu* vorgestellt, welche als ein Nachfolger von Stuxnet gilt. Im September 2011 entdeckten Forscher des *Laboratory of Cryptography and System Security* (CrySyS Lab) am Department für Telekommunikation an der Budapester University of Technology and Economics eine bis dato unbekannte Schadsoftware bei einem europäischen Unternehmen, das sie beauftragt hatte, einen Sicherheitsvorfall in deren IT-Systemen zu untersuchen.[4] Sie tauften die Milware Duqu, da auf infizierten Rechnern Dateien angelegt wurden, deren Dateinamen mit *~DQ* begannen. In Folge analysierte das CrySyS Lab das gefundene Sample und teilte es mit großen Anti-Virus-Herstellern. Mitte Oktober 2011 erschien ein erster Report von *Symantec*. Die Erkenntnisse über die Funktionsweise von Duqu, auf die sich auch dieser Beitrag stützt, stammen aus den Veröffentlichungen des CrySyS Lab[19] und Symantecs Bericht[20].

Allgemeines

Das Ergebnis einer ersten Untersuchung war die Erkenntnis, dass Duqu äußerst ähnlich zu Stuxnet aufgebaut ist, wenn man Designphilosophie, interne Strukturen und Mechanismen sowie Implementierungsdetails miteinander vergleicht. Trotz der frappierenden Ähnlichkeit zeigte sich, dass Duqu ein anderes Ziel verfolgte. Während bei Stuxnet das Erzielen physischen Schadens im Vordergrund stand, handelt es sich bei Duqu um eine informationssammelnde Milware, die zur Cyberspionage verwendet werden kann. Aufgrund der Ähnlichkeit liegt natürlich der Verdacht nahe, dass Duqu von derselben Gruppe von Leuten wie Stuxnet entwickelt wurde und sie Zugang zum Stuxnet-Quellcode hatten.

Verbreitung und Exploits

Als Dropper-Komponente konnte ein Dokument für Microsoft Word ausfindig gemacht werden, welches einen Zero-Day-Kernel-Exploit enthielt. Der Exploit nutzte dabei – nach einer gewissen Wartezeit und sofern bestimmte Randbedingungen auf dem System stimmten – einen unbekannten Bug im Windows-Kernel beim Handling eingebetteter Schriftarten aus, für den im Anschluss an die Veröffentlichung im Dezember 2011 ein Patch bereitgestellt wurde (CVE-2011-3402).

Insgesamt gab es drei Hauptgruppen an Malware-Komponenten: Erstens einen Keylogger, außerdem jeweils eine Gruppe von Objekten, die mit dem Kerneltreiber *jminet7.sys* bzw. dem Kerneltreiber *cmi4432.sys* in Verbindung standen.

Der Keylogger enthielt eine interne, verschlüsselte DLL, welche die Keylogging-Funktionalität zur Verfügung stellte und eine Hauptanwendung, welche den Keylogger injizierte und den Logging-Prozess kontrollierte. Es tauchten zwei Varianten auf, siehe hierzu die Abschnitte über Infostealer 1 und 2, in denen sie näher erläutert werden.

Bei der zweiten Gruppe von Malware-Komponenten wurde in der Registry ein Service erstellt, der den Treiber *jminet7.sys* während des Hochfahrens lädt. Der Kerneltreiber lädt dann die Konfigurationsdaten und injiziert eine DLL namens *netp191.pnf* in einen Systemprozess. Ferner werden Konfigurationsdaten in einer verschlüsselten Datei *netp192.pnf* gespeichert. Die dritte Kategorie verhält sich ähnlich, nutzt aber die Dateien *cmi4432.pnf* und *cmi4464.pnf*.

Diese Verhaltensmuster ähneln dem von Stuxnet, zudem injiziert Duqu auch Code in die *lsass.exe*. Des Weiteren werden dieselben Hooks für *ntdll.dll* verwendet wie bei Stuxnet, und der Treiber *cmi4432.sys* hat eine valide digitale Signatur des taiwanischen Herstellers *C-Media Electronics*, von dem der Treiber aber offenkundig nicht kam – auch bei Stuxnet wurde Code mit kompromittierten taiwanischen Zertifikaten unterschrieben. Während Duqus Initialisierung werden drei Entschlüsselungsoperationen ausgeführt, auch das gleicht Stuxnet. Wie bei Stuxnet sucht auch Duqu zuerst nach bekannten Anti-Virus-Produkten, um dann eine bösartige DLL zu injizieren.

Payload

Während also viele Komponenten von Duqu und Stuxnet gleich aufgebaut waren, war der Payload ein komplett anderer. Es ging nicht um die Zerstörung von Industrieanlagen, sondern die Gewinnung von Information über Systeme, möglicherweise für zukünftige Angriffe.

Duqu verwendet HTTP und HTTPS, um mit Command-and-Control-Servern zu kommunizieren. C&C-Server wurden unter anderem in Indien, Belgien und Vietnam gehostet und leiteten den Traffic an andere Server weiter, um so die Identifizierung und Nachverfolgung zu erschweren.

Duqu konnte ausführbare Dateien herunterladen und eigene Daten hochladen. Dabei wurde vorgegeben, .jpg-Bilder zu übertragen, an deren Ende verschlüsselte Daten angehängt wurden. Die „Verschlüsselung" erfolgte dabei durch eine Komprimierung mit *bzip2* und anschließende XOR-Verschlüsselung. Die ersten 8.192 Bytes des Bildes entsprechen dabei einer Aufnahme des Hubble-Weltraumteleskops.

Duqus Standardeinstellung war, 30 Tage lang aktiv zu sein und sich dann selbst zu deinstallieren; die Dauer konnte aber via C&C-Server verlängert werden. Im Gegensatz zu Stuxnet verbreitete sich Duqu nicht von selbst weiter. Insgesamt konnten vier zusätzlich über den C&C-Server heruntergeladene Binaries beobachtet werden:

Infostealer 1 ist ein *Standalone Executable*, das auf kompromittierten Geräten gefunden wurde, aber in keinem anderen Executable enthalten war (also heruntergeladen wurde). Es hatte neun Hauptroutinen:[20]

- *List of running processes, account details, and domain information*
- *Drive names and information, including those of shared drives*
- *Take a screenshot*
- *Network information (interfaces, routing tables, shares list, etc.)*
- *Keylogger*
- *Window enumeration*
- *Share enumeration*
- *File exploration on all drives, including removable drives*
- *Enumerate computers on the domain through NetServerEnum*

Das Logfile speichert Aufzeichnungen der folgenden Felder: *Type, Size, Flags, Timestamp, Data.*[20]

Infostealer 2 ähnelt der ersten Variante, ist aber eine DLL, aktueller (August vs. Mai 2011) und hat weniger Funktionalität als Infostealer 1. Die sieben Features sind:[20]

- *List of running processes, plus account and domain*
- *List drive names and information, including shared drives*
- *Screenshot*
- *Network information (interfaces, routing tables, and shares list)*
- *Windows enumeration*
- *Share enumeration*
- *Share browse*

Keylogger, File exploration on all drives, including removable drives und *Domain's servers enumeration (using NetServerEnum)* wurden entfernt.[20]

Reconnaissance module, ein *Aufklärungsmodul*, liefert nur einige wenige Informationen über das System (Teil einer Domain?, PID, Session ID, Windows-Ordner, Temp-Ordner, Betriebssystemversion, Architektur, Kontoname, Netzwerkadapter und Zeitinformationen).

Lifespan extender module konnte die *Lebensdauer*, nach der sich Duqu von selbst entfernte, verlängern.

Für eine noch ausführlichere Analyse wird auf die eingangs genannten Berichte[19,20] verwiesen.

3 Duqu 2.0

Auch Duqu wurde weiterentwickelt, und so fand Kaspersky im Jahr 2015 eine überarbeitete Version. *Duqu 2.0* ist Teil einer Spionagekampagne gegen die Kaspersky Labs, Hotels und Konferenzeinrichtungen bei den Verhandlungen der E3+3-Staaten zur Beilegung des Streits um das iranische Nuklearprogramm, an deren Ende im Juli 2015 die Einigung mit dem Iran zum *Joint Comprehensive Plan of Action* stand.[2,21]

Da direkt betroffen, untersuchte Kaspersky die Milware ausgiebig. Kasperskys Analysen und die des CrySyS Labs kommen zu dem Ergebnis, dass die Software eng mit Duqu verwandt ist und sich lediglich der Payload geändert hat, die zugrundeliegende Architektur aber ähnlich geblieben ist.[22,23] Diese Berichte dienen als Quelle für die Aussagen über Duqu 2.0.

Duqu und Duqu 2.0 verwendeten ähnliche Entschlüsselungsroutinen für Strings, die in Zusammenhang mit Anti-Virus-Produkten stehen. Ebenso werden ähnliche Methoden, magische Nummern und Dateiformate für AES-verschlüsselte Dateien verwendet, sogar derselbe Bug tritt auf; der verwendete (Nicht-Standard-)CBC-Modus für die AES-Verschlüsselung war derselbe; das Logging-Modul war äußerst ähnlich mit denselben magischen Konstanten und sogar das C++-ähnliche Coding und die Kompilierungsart ähnelten sich.

Verbreitung und Exploits

Duqu 2.0 wurde u. a. durch gezielte Phishing-E-Mails in Umlauf gebracht. Er verbreitete sich durch Microsoft-Windows-Installer-Pakete, um weitere Maschinen zu infizieren. Außerdem hatte er Module für einen *Pass-the-Hash*-Angriff innerhalb eines lokalen Netzwerks, sodass den Angreifern eine Vielzahl an Verbreitungsmöglichkeiten zur Verfügung stand. Es wurden ähnliche Exploits wie bei Duqu verwendet und eine Schwachstelle bei den Schriftarten (Windows True Type) ausgenutzt, um Administratorrechte zu erlangen.

Payload

Der Payload von Duqu 2.0 hatte viele Möglichkeiten zum Initieren, Einfrieren und Umgehen von Intrusion-Detection-Systemen und Anti-Virus-Produkten sowie über 100 weitere konfigurierbare Module, welche als einzelne Pakte heruntergeladen werden konnten. Auszugsweise werden die Funktionalitäten der Module in Tabelle 1 aufgelistet.

Für eine ausführliche Darstellung aller Funktionen sei hier auf Kasperskys Analyse[23] verwiesen.

4 Flame

Im Mai 2012 analysierte unter anderem das CrySyS Lab eine neu entdeckte Milware, welche zunächst *sKyWIper* getauft und später *Flame* genannt wurde. Erste Versionen tauchten bereits 2007 in Europa, 2008 in den Vereinigten Arabischen Emiraten und 2010 im Iran auf. Flame ist ebenfalls eine informationsstehlende Schadsoftware. Wie auch Stuxnet und Duqu komprimiert und verschlüsselt Flame seine Dateien. Als Quelle für die Fähigkeiten dieser Milware dienen insbesondere die Analysen vom CrySyS Lab[24], sowie Untersuchungen des Kaspersky Labs, dessen Ergebnisse ebenfalls in das Werk des CrySyS Labs eingeflossen sind.

Verbreitung und Exploits

Das CrySyS Lab konnte keine Dropper nachweisen, auch ist unklar, wie die Erstinfektion vonstattenging. Sobald Flame jedoch einen Rechner infiziert hatte, gab es viele Möglichkeiten, sich zu verbreiten: Es nutzt dieselben Drucker- (MS10-061) und LNK-Exploits (MS10-046) wie Stuxnet. Ferner kann es sich als Proxy für Windows Update ausgeben, so dass Rechner im Netzwerk, die Updates erhalten wollen, vom infizierten Rechner Malware geliefert bekommen. Damit dies funktionieren kann, ist eine gültige digitale Signatur notwendig. Für die Erstellung des Zertifikats wurde unter anderem ein MD5-Kollisionsangriff durchgeführt; eine detaillierte Erklärung dieses Angriffs findet sich im Bericht der CrySyS Labs.[4]

Payload

Um einen Überblick über die Funktionalitäten zu geben, werden in Tabelle 2 die aus der Milware extrahierten Codenamen mitsamt ihrer Bedeutung aufgelistet, wie sie vom Kaspersky Lab dokumentiert und vom CrySyS Lab publiziert wurden[4,25].

Bezüglich der C&C-Kommunikation (siehe *Gator*) hat das CrySyS Lab Informationen über mehr als 50 Domainnamen und mehr als 15 IP-Adressen, die für die Kommunikation verwendet wurden; die C&C-Server wurden dabei sehr häufig gewechselt.

Urheber

In der ersten groben Analyse kam das CrySyS Lab beim Vergleichen von Duqu und sKyWIper/Flame zu dem Schluss, dass es wohl nicht vom selben Team entwickelt wurde. Vielmehr vermuteten sie, dass die Angreifer verschiedene, unabhängige Entwicklungsteams für denselben Zweck beauftragt hatten und es sich somit um zwei verschiedene Implementierungen derselben Anforderungsspezifikation handeln könnte. Wenig später gelang dem Kaspersky Lab der Nachweis, dass in Flame und Stuxnet derselbe Code verwendet wurde, sodass man davon ausgehen kann, dass es sich um parallele Projekte derselben Gruppe handelte.[26] Die *Washington Post* zitiert Roel Schouwenberg, Senior Researcher des Kaspersky Labs:[27]

> *„We are now 100 percent sure that the Stuxnet and Flame groups worked together."*

Gegenüber der Washington Post bestätigten ehemalige hochrangige Geheimdienstoffizielle, dass die NSA, CIA und das israelische Militär bei der Entwicklung von Flame beteiligt waren. Aber weder die USA noch Israel gaben hierzu eine offizielle Stellungnahme ab.[27]

Funktion des Moduls	Details
Password Stealer	Login-Daten (Passwörter) aus Google Chrome, Firefox, POP3/HTTP/IMAP, TightVNC, RealVNC, WinVNC3/4, Outlook, SAM, LSASS-Cache, Windows Live, .Net Passport
Remote Desktop Administration	Macht Screenshots, bewegt die Maus, sendet Input an den Desktop
Erkennung von Netzwerk-Sniffern	Erkennt z. B. Wireshark, tcpview, dumpcap und weitere
Umfangreiche Sammlung von System- und Userinformationen	Liste laufender Prozesse, Geräte, Userliste, TCP-Tabellen, SQL-Server-Information, verbundene Drucker, PuTTY Host-Keys und Sessions, u. v. m.
Pipe-Backdoor	Global sichtbare Windows-Pipe
Sammlung von System- und Netzwerkinformationen	Task-Scheduler-Logs, Firewall-Policies, Liste aller Systemdienste etc.
Erzeugen eines XML-Reports über das System (benutzt eigenes Schema)	Computername, Windows-Verzeichnisse, Liste logischer Geräte, Liste aller Dateien, Betriebssystem-Seriennummer, Domainname, Netzwerkadapter-Konfiguration (IP-Adressen, MAC, MTU, Adapterliste)
Vollzugriff auf Dateien	Lesen, Schreiben, Metadaten

Tabelle 1: Payload von Duqu 2.0 (Auszug)

Codename	Bedeutung
Beetlejuice	Listet Bluetooth-Geräte um die infizierte Maschine auf, kann Maschine in *Beacon* verwandeln
Microbe	Audioaufnahme von bereits existierenden Hardwarequellen, listet alle Multimediageräte auf, speichert Gerätekonfiguration, versucht passendes Aufnahmegerät auszuwählen
Infectmedia	Wählt eine Methode (Autorun_infector, Euphoria) zum Infizieren von Medien aus
Autorun_infector	Erzeugt malwareverseuchte *autorun.inf* und startet mit einem Open-Kommando; dieselbe Methode wurde von Stuxnet benutzt, bevor es den LNK-Exploit gab
Euphoria	Erzeugt ein als Verbindungspunkt fungierendes Verzeichnis mit *desktop.ini* und *target.link*; dient als Shortcut, um Flame zu starten
Limbo	Erzeugt Backdoorkonten mit dem Login *HelpAssistant* auf den Maschinen in der Netzwerkdomäne, sofern entsprechende Rechte vorhanden sind
Frog	Infiziert Maschinen mittels vordefinierter Benutzerkonten; einziger spezifizierter Account ist *HelpAssistant* aus der Limbo-Attacke
Snack	Überwachung der Netzwerk-Interfaces, empfängt und speichert NBNS-Pakete in einem Logfile
Boot_dll_loader	Konfiguration, die eine Liste aller zusätzlichen Module enthält, die geladen und gestartet werden sollen
Weasel	Erstellt eine Verzeichnisliste
Boost	Erstellt eine Liste „interessanter" Dateien anhand verschiedener Dateinamenmasken
Telemetry	Logging
Gator	Sobald eine Internetverbindung besteht: Verbindungsaufbau zu C&C-Server, um neue Module herunter- sowie gesammelte Daten hochzuladen
Security	Identifiziert Programme, die Flame behindern könnten (Anti-Virus-Programme, Firewalls, …)

Tabelle 2: Payload von Flame (Auszug)

5 Gauss

Forscher des Kaspersky Labs entdeckten im Juni 2012 bei der Suche nach neuen, unentdeckten Komponenten von Flame eine Schadsoftware, welche viele Module enthält, die nach bekannten Mathematikern benannt worden sind. Das Modul, in dem die sensibelsten Daten gestohlen werden, ist das Gauss-Modul, sodass man die komplette Schadsoftware als *Gauss* bezeichnet hat. Die Erkenntnisse über Gauss stammen hauptsächlich aus den Untersuchungen des Kaspersky Labs[28], unabhängige akademische Untersuchungen gibt es nicht.

Verbreitung und Exploits

Über die Ausbreitung ist wenig bekannt; Wurm-Eigenschaften, also das eigenständige Verbreiten, konnten nicht beobachtet werden. Das Späh-Modul auf USB-Sticks nutzt – wie Stuxnet – einen .LNK-Exploit (CVE-2010-2568). Gauss infizierte Rechner im Nahen Osten; im Gegensatz zu Flame, das sich hauptsächlich im Iran verbreitet hat, fand man die meisten (1.660 von ca. 2.500) Gauss-Infektionen allerdings im Libanon.

Payload

Gauss nutzt eine ähnliche Codebasis wie Flame und kommuniziert über C&C-Server. Wie auch Flame ist Gauss dazu entwickelt, möglichst viel Information vom infizierten Rechner zu stehlen. Gauss entwendet dabei Zugangsdaten für verschiedene Banksysteme, soziale Netzwerke, Email-Clients und von Instant-Messaging-Accounts, indem eigene Module in verschiedene Browser injiziert werden. Dadurch werden Session Data, Cookies, Passwörter und der Browserverlauf abgefangen. Gauss hat zudem spezielle Kommandos, um Daten von libanesischen Banken (z. B. Bank of Beirut und Byblos Bank) abzufangen.[4]

Die identifizierten Module von Gauss sind in Tabelle 3 mit Codenamen und Bedeutung aufgelistet. Für ein Modul gibt es mehrere Bezeichnungen (sowohl *Kurt* als auch *Godel*).

Modulname	Bedeutung
Cosmos	Sammelt Informationen über CMOS, BIOS
Kurt, Godel	Infiziert USB-Laufwerke mit Modul, das Daten stiehlt
Tailor	Sammelt Informationen über Netzwerk-Interfaces
McDomain	Sammelt Informationen über Benutzer-Domain
UsbDir	Sammelt Informationen über die Laufwerke des Computers
Lagrange	Installiert eine eigene Schriftart (Palida Narrow)
Gauss	Installiert Browser-Plugins, welche Passwörter, Cookies und weitere Daten sammeln
ShellHW	Loader und Kommunikationsmodul

Tabelle 3: Payload von Gauss

Die Konfiguration einer bestimmten Modulkombination für jedes System ist in einem Registry Key festgehalten. Diese Technik, wie auch die gesamte Konfigurationsstruktur, ist ähnlich zu der aus Stuxnet, Duqu und Flame.

Das Godel-Modul ist besonders interessant, da es mit der Stromchiffre RC4 verschlüsselt ist (im Vergleich zu Stuxnets, Duqus und Flames Verschlüsselung also äußerst stark) und der Schlüssel für die Entschlüsselung nicht in der Milware selbst enthalten ist. Stattdessen wird versucht, das Modul dynamisch zu entschlüsseln und den Schlüssel anhand von Strings in der Path-Variable und einigen Dateinamen zu errechnen. Das lässt darauf schließen, dass das Godel-Modul nur für ganz spezielle Zielrechner entworfen wurde. Auf Rechnern, bei denen der Schlüssel nicht wiederhergestellt werden kann, bleibt das Modul inaktiv.

6 Red October

Die Milware *Red October* ist im Gegensatz zu den vorherigen kein Verwandter von Stuxnet, sondern aus der Feder einer vollkommen anderen Gruppe. Die Spähsoftware, im Oktober 2012 von Kaspersky entdeckt, wurde von russischsprachigen Autoren entwickelt. Red October infizierte Forschungseinrichtungen und diplomatische Organisationen in Zentralasien und Osteuropa.[2] Der Name stammt von Kaspersky und ist eine Anspielung auf den Roman *The Hunt For Red October*.[29] Die Milware war mindestens seit dem Jahr 2007 aktiv.[30] Da keine Analyse von akademischen Institutionen vorliegt, entstammen alle Erkenntnisse ausschließlich Kasperskys Veröffentlichungen.[31]

Verbreitung und Exploits

Für die Verbreitung wurde ein dreistufiges System verwendet. Auf erster Ebene dienten E-Mails mit bösartigen Anhängen und URLs als Türöffner. Bei den Anhängen handelte es sich um Dokumente für Microsoft Word und Excel, welche Sicherheitslücken (CVE-2009-3129, CVE-2010-3333, CVE-2012-0158) ausnutzen, außerdem gab es einen Exploit für Java (*Rhino*-Exploit für CVE-2011-3544). Beide Varianten luden einen Dropper für die zweite Stufe nach. Über den Dropper konnten wiederum verschiedene Module nachgeladen werden. Der Wurm konnte sich außerdem über das lokale Netzwerk ausbreiten. Insgesamt wurden vier verschiedene Exploits verwendet. Dabei handelte es sich nicht um Zero-Day-Exploits, sondern um Exploits für bereits bekannte Sicherheitslücken, die jedoch auf den Rechnern nicht gepatcht worden waren.[31]

Payload

Der Payload wurde über den Dropper nachgeladen und von einem Loader entschlüsselt. Es standen mehr als 100 verschiedene Module mit unterschiedlicher Funktionalität zur Verfügung. Für den Download standen ab 2007 zusammengerechnet mindestens 60 C&C-Server bereit. Die Module, die durch die Backdoor installiert werden konnten, lassen sich in zwei Kategorien aufteilen:

- Offline-Module existieren als Dateien auf der lokalen Festplatte, können eigene *Registry Keys* erstellen, haben Logdateien auf der Festplatte und können selbstständig mit den C&C-Servern kommunizieren.

- Online-Module existieren nur im Speicher und werden nie auf die Festplatte gesichert; keine *Registry Keys*, Logs nur im RAM, senden Resultate an die C&C-Server.

Der Hauptzweck der Spähsoftware lag darin, möglichst viel Information zu sammeln. Dies umfasst Information über das infizierte System, Browserversionen, Dateinamen, Verzeichnisbäume, E-Mail-Verläufe, Zugangsdaten, Passwort-Hashes, angeschlossene mobile Geräte und weiteres.

Ein Modul nistete sich in den Adobe Reader und Microsoft-Office-Applikationen ein. Der Hauptzweck dieses Codes war es, eine sichere Methode zu haben, den Zugriff auf das Zielsystem wiedererlangen zu können. Das Modul erwartete ein speziell gefertigtes Dokument, das dem Opfer per E-Mail zugeschickt werden konnte und – da es keinerlei Exploit-Code enthielt – problemlos alle Sicherheitschecks überstand. Das Dokument wurde vom Modul verarbeitet und startete eine bösartige Anwendung, die an das Dokument angehängt war. Dieser Trick ermöglicht einen erneuten Zugriff auf den infizierten Rechner, wenn z. B. die C&C-Server unerwarteterweise offline gegangen sind (shutdown/takeover).

Die Spähsoftware infizierte weltweit die Rechner von Regierungen, Botschaften und Forschungseinrichtungen. Über die Urheber ist nichts weiter bekannt.

7 Regin

Die Spionageplattform *Regin* wurde erst durch im November 2014 veröffentlichte Recherchen und Untersuchungen von *The Intercept*, Symantec und Kaspersky bekannt.[32,33,34] Es ist unklar, seit wann Regin eingesetzt wurde, einige Teile existieren jedoch bereits seit dem Jahr 2003. Die Hauptziele lagen in der Informationsbeschaffung und der Erleichterung anderer Angriffe. Kaspersky weist darauf hin, dass Regin rein als Malware zu bezeichnen nichtzutreffend wäre, Regin sei vielmehr eine ganze Plattform.

Aufbau, Verbreitung und Exploits

Regin ist gekennzeichnet durch seinen mehrstufigen Aufbau. Kaspersky und Symantec unterscheiden sich leicht in der Darstellung der Stufen, beim nachladbaren Payload wird von *Plugins* gesprochen. Symantec gibt sechs Stufen an:[33]

0. Dropper. Installs Regin onto the target computer

1. Loads driver (facilitates the loading of stage 2)

2. Loads driver (kernel driver, runs stage 3)

3. Loads compression, encryption, networking, and handling for an encrypted virtual file system (EVFS)

4. Utilizes the EVFS and loads additional kernel mode drivers, including payloads

5. Main payloads and data files

Ein Großteil des Codes befindet sich in verschlüsseltem Dateispeicher, so genannten Virtual File Systems (VFS). Für eine detaillierte Erklärung der Funktionsweise wird auf die technischen Berichte von Symantec und Kaspersky verwiesen.[33,34]

Über den initialen Infektionsmechanismus ist nur wenig bekannt, ebenso wenig wurden Zero-Day-Exploits gefunden.

Payload

Die Plugins ermöglichten umfangreiche Überwachungsmaßnahmen. Das umfasst das Sammeln verschiedenster Information auf dem infizierten Rechner (Laufwerksnamen, Ordnerstrukturen, angeschlossene USB-Geräte), das Abgreifen von sensiblen Daten (Zugangsdaten, Passwörter, Dokumente, E-Mails), das Überwachen des Netzwerkverkehrs und viele weitere Features (z. B. Mausklicks, Screenshots).

Während oftmals eben dieser Datendiebstahl im Vordergrund stand, gibt es auch Fälle, bei denen Telekommunikationsanbieter angegriffen wurden, um weitere komplexe Angriffe führen zu können. Ein Plugin kann die Aktivitäten eines GSM Base Station Controller mitloggen.

Opfer und Urheber

Laut Kaspersky sind die meisten Opfer in den folgenden Gruppen zu finden:[34]

- Telekommunikationsanbieter
- Regierungseinrichtungen
- Multinationale politische Gremien
- Finanzinstitute
- Forschungsinstitute
- Personen, die in Bereich der fortgeschrittenen Mathematik/ Kryptographie forschen

Regin war in vielen Ländern aktiv, vor allem in Russland und Saudi-Arabien, aber auch in Belgien, Deutschland und Österreich. Bekannte Opfer von Regin sind der belgische Telefonanbieter *Belgacom*, der belgische Kryptograph *Jean-Jacques Quisquater*, die EU-Kommission in Brüssel und eine Referatsleiterin im deutschen Bundeskanzleramt. Die Bundesanwaltschaft hatte wegen letzterer ein Ermittlungsverfahren gegen unbekannt eingeleitet.

Seit Anfang 2015 geht man davon aus, dass Regin ein Werkzeug der NSA und des GCHQ ist, welches von den Geheimdiensten der *Five Eyes* genutzt wird. Weder die NSA noch das GCHQ kommentierten die Veröffentlichungen.

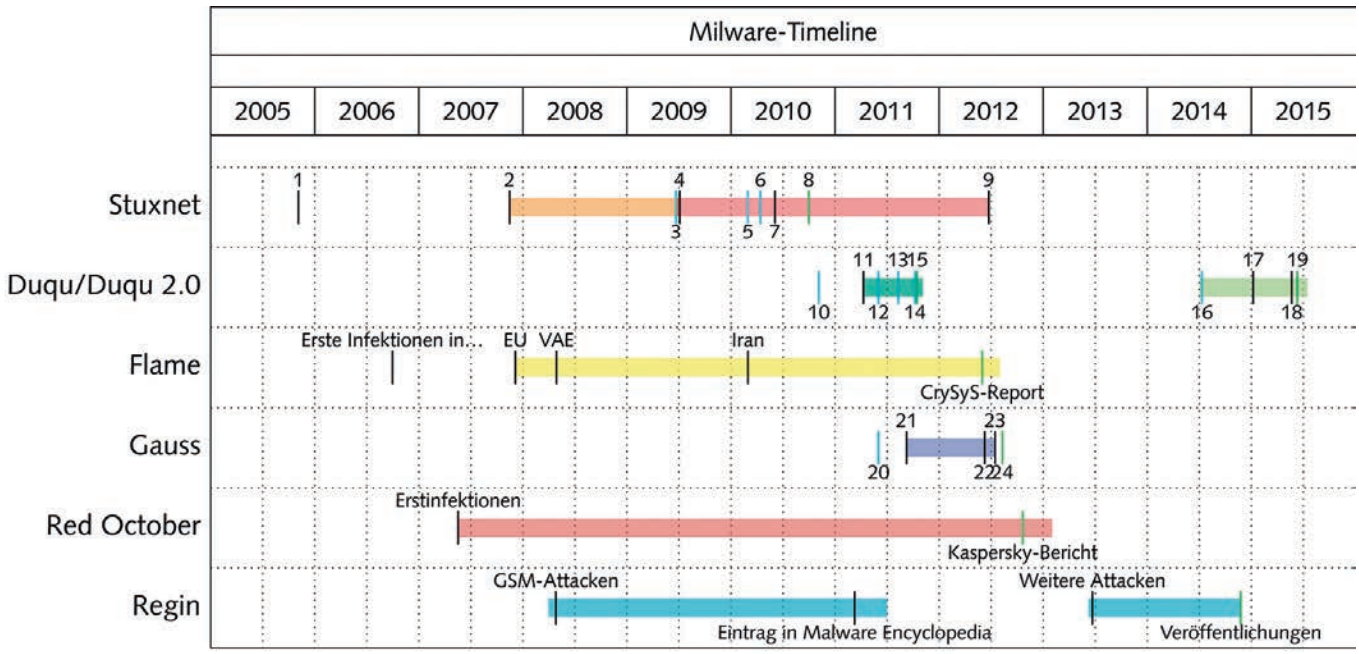
8 Ausblick

Abschließend werden die besprochenen sieben Beispiele für Milware in einen zeitlichen Kontext gesetzt (Abbildung 1). Die Zeitintervalle sind dabei nicht als exakte Anfangs- und Enddaten zu verstehen, sondern dienen als grobe Anhaltspunkte, in welchem Zeitraum die Milware aktiv war. Bei Stuxnet wurde der Anfang auf das Datum gelegt, an dem die Version 0.5 auf die Online-Plattform *VirusTotal* hochgeladen wurde; ab wann Stuxnet nicht mehr eingesetzt wurde, ist nicht bekannt, das Ende wurde daher für die Grafik auf den Zeitpunkt gelegt, an dem sich Stuxnet nicht mehr weiterverbreitete, auch wenn Stuxnet wohl schon früher nicht mehr benutzt wurde. Bei Duqu und Duqu 2.0 beginnt der Zeitraum ab den ersten dokumentierten Angriffen und endet kurze Zeit nach den Veröffentlichungen. Flame war seit 2007 nachgewiesenermaßen in Europa aktiv, bei der Entdeckung 2012 wurde der bisherige Einsatzzeitraum auf fünf bis acht Jahre geschätzt.[24] Gauss' früheste bekannte Infektionen waren im September 2011, im Juli 2012 gingen die C&C-Server offline. Red Octobers Einsatz ist ab Mai 2007 gesichert, Anfang 2013 war die Milware noch immer in Gebrauch.[30] Die Plattform Regin war seit mindestens 2008 im Einsatz, wurde 2011 vom Netz genommen und tauchte 2013 in einer neuen Version wieder auf. Ob Regin auch nach den Veröffentlichungen Ende 2014 noch genutzt wurde, ist nicht bekannt.

Welche Auswirkungen hat nun die Zunahme an Milware? Herr beobachtete *Trickle-down-Effekte* von Milware zu Malware.[2] Propagierungsmethoden und Exploits, die für Milware entwickelt wurden, finden Einzug bei Malware-Autoren.[35] Auch wird Code (z. B. von Duqu und Red October) von kriminellen Vereinigungen in ihrer Malware wiederverwendet. Indem Staaten durch eigene oder ausgelagerte Großprojekte ihre Angriffsstärke erhöhen, finanzieren sie letztlich indirekt auch Forschungs- und Entwicklungseinrichtungen für nicht staatliche Gruppen, was die Schere zwischen den Fähigkeiten der Angreifer und der Verteidiger noch weiter öffnet.

Auf dem Exploit-Markt können die staatlichen finanziellen Mittel die Verteidiger ausstechen. Ferner führt die staatliche Präsenz dazu, dass es mehr und mehr Anbieter für Schwachstellen in weit verbreiteter, kommerzieller Software gibt. Milware kann zur treibenden Kraft werden, was die Komplexität und Vielfalt schadhafter Software und deren Komponenten betrifft. Staaten konkurrieren bereits jetzt um die effektivsten Spionagetools und Cyberwaffen. Bei all diesen Betrachtungen muss man sich stets vor Augen führen, dass Staaten – im Gegensatz zu sonstigen Malware-Autoren – weitgehend immun gegen strafrechtliche Verfolgung sind und somit bei Entwicklung und Einsatz von Milware weitreichende Freiheiten haben, ohne Konsequenzen fürchten zu müssen.

Abschließend lässt sich festhalten, dass Milware eine neue Kategorie von bösartiger Software darstellt, bei der sich aufgrund der staatlichen Entwicklung die Prioritäten (Verwendung bei nationalen Strategien, als taktisches Mittel auf dem „Schlachtfeld" oder zur Spionage) und Komplexität fundamental von denen nicht staatlicher Gruppen unterscheiden. Diese Unterschiede bedingen, dass konventionelle Annahmen aus der Informationssicherheit auf den Prüfstand gehören. Schafft es die IT-Sicherheits-Community nicht, eine Unterscheidung zwischen Milware



1	Registrierung der C&C-Server	9	Infection stop date: v1.x	17	Weitere Attacken
2	v0.5 bei VirusTotal hochgeladen	10	Treiber kompiliert, erste Varianten	18	Analysebeginn
3	Main binary compile timestamp: v1.001	11	Erste Attacken	19	Kaspersky-Report veröffentlicht
4	Infection stop date: v0.5	12	Infostealer 1 kompiliert	20	Einige Dateien kompiliert
5	Main binary compile timestamp: v1.100	13	Infostealer 2 kompiliert	21	Früheste bekannte Infektionen
6	Main binary compile timestamp: v1.101	14	Weitere Module kompiliert	22	Nachforschungen beginnen
7	Entdeckung von Stuxnet	15	CrySyS Report	23	C&C-Server gehen offline
8	Symantec-Dossier	16	Einige Module kompiliert	24	Kaspersky-Bericht

Abbildung 1: Timeline mit den aktiven Zeiträumen und Meilensteinen verschiedener Milware

und Malware zu vollziehen und entsprechende Konsequenzen zu ziehen, wird es schwierig, auf diese neue, andersartige Bedrohung angemessen reagieren zu können.

Nachwort der Redaktion: Kurz vor Übernahme dieses Textes in den Layoutprozess erreichte uns ein Hinweis des Autors auf einen tagesaktuellen Vorgang, der den oben angesprochenen Trickle-down-Effekt plastisch vor Augen führt:

> *Hackers exploiting malicious software stolen from the National Security Agency executed damaging cyberattacks on Friday that hit dozens of countries worldwide […] They then quickly spread through victims' systems using a hacking method that the N.S.A. is believed to have developed as part of its arsenal of cyberweapons. […] The attacks on Friday appeared to be the first time a cyberweapon developed by the N.S.A., funded by American taxpayers and stolen by an adversary had been unleashed by cybercriminals against patients, hospitals, businesses, governments and ordinary citizens. […]*[36]

Referenzen

1 *Herr T (2015) The Rise of Milware. Cyber Security Policy & Research Institute, The George Washington University, 2.3.2015, http://www2.seas.gwu.edu/~cspri/blog/2015/3/2/the-rise-of-milware.html*

2 *Herr T, Armbrust E (2015) Milware: Identification and Implications of State Authored Malicious Software. New Security Paradigms Workshop, Twente, Niederlande, 8.-11.9.2015, S. 29–43. https://ssrn.com/abstract=2569845*

3 *Herr T (2014) PrEP: A Framework for Malware & Cyber Weapons. The Journal of Information Warfare 13(1):87–106. https://ssrn.com/abstract=2343798*

4 *Bencsáth B, Pék G, Buttyán L, Félegyházi M (2012) The Cousins of Stuxnet: Duqu, Flame, and Gauss. Future Internet 4(4):971–1003, http://www.mdpi.com/1999-5903/4/4/971*

5 *Best M (2015) Stuxnet code. archive.org, 12.9.2015, https://archive.org/details/Stuxnet*

6 *Falliere N, O'Murchu L, Chien E (2011) W32.Stuxnet Dossier. Symantec Security Response, Version 1.4, Feb. 2011, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf*

7 *McDonald G, O'Murchu L, Doherty S, Chien E (2013) Stuxnet 0.5: The Missing Link. Symantec Security Response, Version 1.0, 26.2.2013,*

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/stuxnet_0_5_the_missing_link.pdf

8 *Beer K (2013) Stuxnet 0.5: Der Sabotage-Wurm ist älter als gedacht. heise Security, 27.2.2013, http://heise.de/-1812154*

9 *Eikenberg R (2012) Innenangreifer half bei Stuxnet-Infektion. heise Security, 13.4.2012, http://heise.de/-1520408*

10 *Langner R (2013) To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve. The Langner Group, Nov. 2013, https://www.langner.com/wp-content/uploads/2017/04/To-kill-a-centrifuge.pdf*

11 *Albright D, Brannan P, Walrond C (2010) Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Institute for Science und International Security, 22.12.2010, http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf*

12 *BBC News (2010) Iran says nuclear programme was hit by sabotage. BBC online, 29.11.2010, http://www.bbc.co.uk/news/world-middle-east-11868596*

13 *SPIEGEL ONLINE (2011) Deutsche Energieversorger anfällig für Computerwurm Stuxnet. DER SPIEGEL 16/2011, 16.4.2011, http://www.spiegel.de/spiegel/vorab/a-757472.html*

14 *Rieger F (2010) Der digitale Erstschlag ist erfolgt. Frankfurter Allgemeine Zeitung, 22.9.2010, www.faz.net/aktuell/feuilleton/debatten/digitales-denken/t-1578889.html*

15 *Wilkens A (2013) Stuxnet: Berichte über weiteren Geheimnisverrats-Fall in den USA. heise online, 28.6.2013, http://heise.de/-1902235*

16 *Broad WJ, Markoff J, Sanger DE (2011) Israeli Test on Worm Called Crucial in Iran Nuclear Delay. The New York Times, 15.1.2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html*

17 *Binsch J (2016) Codename „Nitro Zeus": Vom Plan, Iran komplett lahmzulegen. Süddeutsche Zeitung, 18.2.2016, http://www.sueddeutsche.de/digital/s-1.2870281*

18 *Sanger DE, Mazzetti M (2016) U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict. The New York Times, 16.2.2016, http://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html*

19 *Bencsáth B, Pék G., Buttyán L, Félegyházi M (2011) Duqu: A Stuxnet-Like Malware Found in the Wild. Technical Report Version 0.93, CrySyS Lab, Budapest, 14.10.2011, https://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf*

20 *Symantec Security Response (2011) W32.Duqu: The precursor to the next Stuxnet. Version 1.4, 23.11.2011, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf*

21 *Auswärtiges Amt (2016) Konflikt um das iranische Atomprogramm. 20.1.2016, http://www.auswaertiges-amt.de/DE/Aussenpolitik/RegionaleSchwerpunkte/NaherMittlererOsten/04_Iran/Iranisches-Nuklearprogramm_node.html*

22 *Bencsáth B, Ács-Kurucz G, Molnár G, Vaspöri G, Buttyán L, Kamarás R (2015) Duqu 2.0: A comparison to Duqu. Technical Report Version 1.0, CrySyS Lab, Budapest, 10.6.2015, http://www.crysys.hu/duqu2/duqu2.pdf*

23 *Kaspersky Lab (2015) The Duqu 2.0: Technical Details. Version 2.1, 11.6.2015. https://securelist.com/files/2015/06/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf*

24 *sKyWIper Analysis Team (2012) sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks. Technical Report Version 1.05, CrySyS Lab, Budapest, 31.5.2012, https://www.crysys.hu/skywiper/skywiper.pdf*

25 *Gostev A (2012) Flame: Bunny, Frog, Munch and Beetlejuice… Kaspersky Lab, 30.5.2012, https://securelist.com/blog/incidents/32855*

26 *Kaspersky Lab (2012) Resource 207: Kaspersky Lab Research proves that Stuxnet and Flame developers are connected. Press Release, 11.6.2012, http://newsroom.kaspersky.eu/fileadmin/user_upload/en/Images/Lifestyle/20120611_Kaspersky_Lab_Press_Release_Flame_Stuxnet_cooperation_final_-_UK.pdf*

27 *Nakashima E, Miller G, Tate J (2012) U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say. The Washington Post, 19.6.2012, www.washingtonpost.com/world/national-security/u/2012/06/19/gJQA6xBPoV_story.html*

28 *Global Research & Analysis Team (GReAT) (2012) Gauss: Abnormal Distribution. Kaspersky Lab, 9.8.2012, https://securelist.com/analysis/publications/36620*

29 *Clancy T (1984) The Hunt for Red October. Naval Institute Press, Annapolis, MD*

30 *Global Research & Analysis Team (GReAT) (2013) "Red October" Diplomatic Cyber Attacks Investigation. Kaspersky Lab, 14.1.2013, https://securelist.com/analysis/publications/36740*

31 *Global Research & Analysis Team (GReAT) (2013) "Red October". Detailed Malware Description 1. First Stage of Attack. Kaspersky Lab, 17.1.2013, https://securelist.com/analysis/publications/36830*

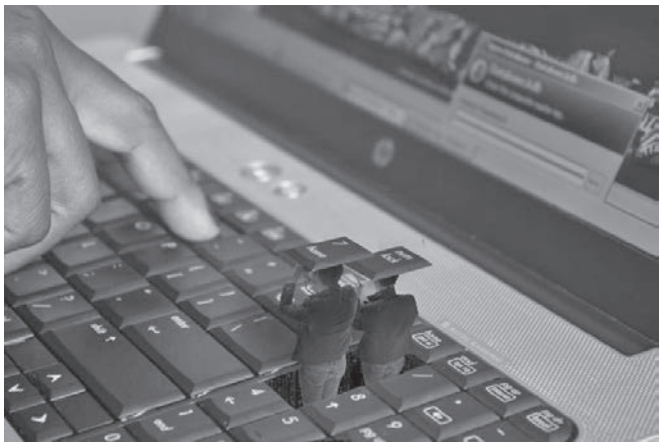
32 *Marquis-Boire M, Guarnieri C, Gallagher R (2014) Secret malware in European Union attack linked to U.S. and British intelligence. The Intercept, 24.11.2014, https://theintercept.com/2014/11/24/secret-regin-malware-belgacom-nsa-gchq/*

33 *Symantec Security Response (2015) Regin: Top-tier espionage tool enables stealthy surveillance. Version 1.1, 27.8.2015, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/regin-analysis.pdf*

34 *Kaspersky Lab (2014) The Regin platform: Nation-state ownage of GSM networks. Version 1.0, 24.11.2014, https://securelist.com/files/2014/11/Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf*

35 *Shamir U (2014) The Case of Gyges, the Invisible Malware: Government-Grade now in the Hands of Cybercriminals. Sentinel Labs Intelligence Report, Juli 2014, https://archive.org/details/pdfy-58MYDOIbvKzM8O1H*

36 *Perlroth N, Sanger DE (2017) Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool. The New York Times, 12.5.2017, https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html*



keyloggers, Foto: Robbert van der Steeg, CC BY-SA 2.0

Stefanie Jäckel und Eberhard Zehendner

Datenschutz handhabbar – Editorial zum Schwerpunkt

Datenschutz handhabbar lautete der Titel des Seminars (im Rahmen unserer jedes Semester stattfindenden Veranstaltung *Informatik und Gesellschaft* an der Friedrich-Schiller-Universität Jena), dem die ersten vier Beiträge des Schwerpunkts entstammen; auch die nächsten beiden Beiträge stammen aus Seminaren dieser Veranstaltung. Die Beiträge von Peter Wohlgenannt und Sebastian Nemetz entstanden im Rahmen eines *Konferenzseminars IT-Sicherheit* an der Friedrich-Alexander-Universität Erlangen-Nürnberg, organisiert vom Lehrstuhl für IT-Sicherheitsinfrastrukturen (Prof. Felix Freiling).

Nicole Tornow erprobt in ihrem Beitrag *Beurteilung des Datenschutzes anhand ausgewählter Kriterien. Guideline zum Umgang mit Datenschutzrichtlinien* ganz praktisch die *Handhabbarkeit von Datenschutz* – ein laut der Autorin leidiges Thema, das jedoch jeden von uns betrifft. Häufig scheitert die Motivation der Nutzer bereits am anfänglichen Durchlesen der Datenschutzrichtlinien. Tornow stellt heraus, dass der Aufwand, der zur detaillierten Einarbeitung in die gesetzlichen Grundlagen nötig wäre, so hoch ist, dass er die meisten Nutzer abschreckt. Aus diesem Grund ist es laut Tornow dringend nötig, ein einfaches kriterienbezogenes System zu schaffen, das für alle Nutzer einen umfassenden Überblick und auch Durchblick zum Schutz der eigenen personenbezogenen Daten ermöglicht.

Sarah Schott und *Claudia Sichting* unterstreichen in ihrem Beitrag *Roboter im Alltag: Wer trägt Verantwortung bei Schutzbefohlenen?*, dass Roboter, die mit Kindern spielen, im Alltag helfen und auf Gefühle reagieren, längst nicht mehr nur Science-Fiction sind. Die Autorinnen zeigen, weshalb es spätestens jetzt Zeit wird, die Fähigkeiten der Roboter auszuloten und bei Bedarf das Datenschutzrecht anzupassen. Gleichzeitig folgt die Warnung: wartet man mit Maßnahmen zur Veränderung des Datenschutzrechts ab, bis sich die beschriebenen Entwicklungen auch in Europa durchsetzen, wird zwischenzeitlich oder auf lange Sicht der Schutz der Privatsphäre riskiert.

Eine Spieler-orientierte Kritik an (mobilen) Free-to-Play-Spielen äußert *Felix Baral-Weber* und betont, dass F2P (Free-to-Play)-Spiele den mobilen Spielemarkt derzeit dominieren. Der Autor analysiert, dass Nutzer im Nachhinein häufig zur Kasse gebeten werden, obwohl F2P-Spiele eigentlich versprechen, kostenlos spielbar zu sein. Hierbei angewendete Monetarisierungs-Methoden sind integraler Teil des Spieldesigns und verändern die Spiele grundlegend. Baral-Weber deckt mit seinem Beitrag typische Muster (Patterns) auf, die hinter F2P-Spielen stecken.

Darf Google mein Profilbild verkaufen?, fragt *Maximilian Katzmann* provokant und stellt heraus, dass mittlerweile die meisten Smartphones eine gebündelte Sammlung an persönlichsten Informationen ihrer Nutzer enthalten. Hierzu gehören private Konversationen, Fotos von Freunden und Familie, ortsbezogene Daten sowie Informationen, die unseren Gesundheitszustand beschreiben. All diese Daten werden mit dem Google-Konto verknüpft. Damit ergibt sich eine große Menge an Information, die Google zur Verfügung gestellt wird. Um zu verstehen, wie das Unternehmen mit diesen Daten umgeht und wie Google seine Einnahmen generiert, erläutert der Autor die Datenschutzbestimmungen des Unternehmens.

Maike Küper fragt in ihrem Beitrag, warum Daten eigentlich ein so begehrtes Gut sind, stellt gängige Metaphern hierzu erfolgreich auf den Prüfstand und nähert sich schließlich schrittweise der bedeutsamen Frage, wie groß er denn nun konkret wirklich ist: *Der Wert unserer Daten.*

Anja Grunert konfrontiert in *Schöne neue Bücherwelt. Was E-Book-Reader über unser Leseverhalten herausfinden und wie Verlage oder Buchhändler dies nutzen können* Komfort und Nutzen des digitalen Buches mit Schattenseiten derzeitiger Ausgestaltung zugehöriger Lesegeräte. Besonderer Dank geht an *John Cuneo* für die Möglichkeit zum Wiederabdruck seiner trefflichen Karikatur der „Gelesenen".

Auf der Spur digital terrestrischer Fußabdrücke befindet sich *Peter Wohlgenannt* im abschließenden Beitrag des Schwerpunkts. Die auf der Ausstrahlung individueller Signaturen mitgeführter Geräte basierende *geografische Lokalisation* einer Person stellt – neben der Erfassung biometrischer Merkmale und dem Online-Tracking über individuelle, digitale Netzwerkspuren – ein weiteres schreckliches Instrument der Ausforschung von Menschen dar.

Nicht direkt Teil des Schwerpunkts, doch in konkretem inhaltlichen Zusammenhang damit stehend (und daher direkt vor dem Schwerpunkt platziert), ist der Überblick über staatliche Spähsoftware von *Sebastian Nemetz.* Er lässt spektakuläre Fälle von *Milware* Revue passieren, die zwar überwiegend zu unmittelbar zerstörerischen Zwecken eingesetzt wird, aber eben auch – wie schon die Bezeichnung *Spähsoftware* erahnen lässt – zur heimlichen und illegalen Erlangung persönlicher, geschäftlicher, wissenschaftlicher, diplomatischer und militärischer Geheimnisse genutzt werden kann.

Nicole Tornow

Beurteilung des Datenschutzes anhand ausgewählter Kriterien

Guideline zum Umgang mit Datenschutzrichtlinien

Die Handhabbarkeit von Datenschutz ist ein leidiges Thema, das jeden von uns betrifft, denn oftmals scheitert unsere Motivation schon zu Beginn beim eigentlichen Durchlesen von Datenschutzrichtlinien. Der Aufwand der Einarbeitung ist meist zu abschreckend, um aufmerksam Richtlinien zu bearbeiten oder rechtliche Grundlagen zu verstehen. Aus diesem Grund ist es umso wichtiger, einen umfassenden Überblick und auch Durchblick im Interesse des Schutzes der eigenen personenbezogenen Daten zu gewähren.

Die folgende Auseinandersetzung mit der Handhabbarkeit von Datenschutz umfasste die Einarbeitung in Datenschutzgesetze sowie Datenschutzerklärungen bekannter Unternehmen. Auf dieser Grundlage wurde ein Beurteilungssystem entworfen, welches es dem Einzelnen ermöglichen soll, Datenschutzrichtlinien nach persönlich gewünschtem Schutz zu verstehen, zu bewerten und schließlich mit diesem Wissen über die Einwilligung zu entscheiden. Damit wird gleichzeitig die Frage evaluiert: *Können Datenschutzrichtlinien durch zielgerichtetes Abarbeiten von gewählten Kriterien umfassend beurteilt werden?*

1. Rechtliche und gesetzliche Grundlagen

Datenschutzrichtlinien (nach aktuellem Stand, die EU-DSGVO wird zu Änderungen führen) verweisen oft auf Gesetze, die ohne Fachwissen nicht interpretierbar sind. Nachfolgend werden Auszüge aus dem Bundesdatenschutzgesetz und der Richtlinie 95/46/EG des Europäischen Parlaments erläutert. Das Recht auf Informationelle Selbstbestimmung, im bundesdeutschen Gesetz (jedoch außerhalb des Grundgesetzes) als Datenschutz-Grundrecht verankert, beschreibt das Recht des Einzelnen, über die Freigabe und Verwendung seiner personenbezogenen Daten selbst zu entscheiden[1].

Bundesdatenschutzgesetz (BDSG)

Im Jahr 1990 wurde das *Bundesdatenschutzgesetz* verabschiedet, welches den Schutz des Einzelnen vor der Beeinträchtigung seiner Persönlichkeitsrechte im Umgang mit den eigenen personenbezogenen Daten festlegt (nach § 1 BDSG). Es umfasst dabei die Aspekte der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten. Besonders die im § 3 BDSG aufgeführten Begriffsbestimmungen sind notwendig, um weitere Gesetzmäßigkeiten zu verstehen. Dazu zählen unter anderem

- *personenbezogene Daten* als „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“ (§ 3 Abs. 1),
- *Löschen* von Daten, d.h. „Unkenntlichmachen gespeicherter personenbezogener Daten“ (§ 3 Abs. 4) und
- *Anonymisieren* personenbezogener Daten, wodurch „Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand [...] einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können“ (§ 3 Abs. 6).

Andere Paragraphen des BDSG betreffen weitere Aspekte des Datenschutzes und verdeutlichen, auf welche konkreten Eigenschaften im Umgang mit persönlichen Daten zu achten ist. Laut § 4 Abs. 1 sind Datenerhebung, -verarbeitung und -nutzung „nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat“. Hierbei gilt im Allgemeinen, dass die personenbezogenen Daten beim Betroffenen erhoben werden müssen. Ausnahmen bilden gegebene Erfordernisse durch eine vorliegende Rechtsvorschrift, eine zu erfüllende Verwaltungsaufgabe oder ein entsprechender Geschäftszweck. Die Einwilligung für Erhebung, Verarbeitung und Nutzung personenbezogener Daten muss nach § 4a immer auf einer freien Entscheidung des Betroffenen beruhen und bedarf der Bereitstellung von ausreichend Information über den Zweck der Datenerhebung.

Werden personenbezogene Daten für eigene Geschäftszwecke erhoben, sind diese Zwecke nach § 28 konkret zu formulieren. Ein Zweck beschreibt eine zur Ausführung bzw. zum Anbieten des Dienstes für den Betroffenen erforderliche Information. § 34 verpflichtet die verantwortliche Stelle, Auskunft über zur eigenen Person gespeicherte Daten, Empfänger, an die entsprechende Daten weitergegeben wurden, und den Zweck der Speicherung zu erteilen. Die Auskunftserteilung kann verweigert werden, wenn damit Geschäftsgeheimnisse gefährdet wären, welche das Informationsinteresse des Betroffenen überwiegen.

Ist die weitere Speicherung erhobener Daten nicht mehr zulässig oder werden diese für den erforderlichen Zweck nicht mehr benötigt, sind sie nach § 35 zu löschen bzw. zu sperren, wenn der Löschung „gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen“.

Die genannten Paragraphen sind keineswegs vollständig wiedergegeben, noch decken sie alle zu beachtenden Gesetze ab. Die Formulierungen wurden gezielt auf die behandelte Thematik zugeschnitten. Für eine umfangreichere Einarbeitung sind daher ebenso § 6 (Rechte des Betroffenen), § 28b (Scoring) sowie § 29 (Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung) zu beachten.

Europäische Richtlinie 95/46/EG

Die *Richtlinie 95/46/EG des Europäischen Parlaments und des Rates*[2] wurde am 24. Oktober 1995 erlassen. Sie bezieht sich auf den Schutz personenbezogener Daten in Europa, genauer: in allen Mitgliedsstaaten des *Europäischen Wirtschaftsraumes* (EWR)[3], der die Staaten der EU sowie die EFTA-Staaten Island, Liechtenstein und Norwegen umfasst. Auch auf europäischer Ebene werden ähnliche Regelungen wie im BDSG festgelegt. So ähnelt die Gesetzgebung der Einwilligung zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten der des BDSG sehr.[4]

Da die Europäische Union ein Zusammenschluss von Staaten ist, wird vor allem die Übermittlung von personenbezogenen Daten geregelt. Die Übermittlung ist unter bestimmten Bedingungen bzw. Voraussetzungen generell zulässig. Gründe dafür sind u.a. die rechtmäßige Erfüllung betroffener, im öffentlichen Interesse liegender Aufgaben (Übermittlung an Dritte) oder eine zweckmäßige Begründung und Beurteilung durch die Europäische Kommission (Übermittlung außerhalb der EU).[5]

Eine weitere Festlegung gilt der allgemeinen Speicherung von Daten und ist vor allem bzgl. Datenclouds für den Betroffenen wichtig. Cloudspeicherdienste legen Nutzerdaten nicht zwingend an einem Standort und darüber hinaus im Wohnsitzstaat des Nutzers ab. Problematisch ist, dass jegliche Speicherung von Daten außerhalb Deutschlands, respektive der EU, einem anderen Datenschutzgesetz und damit auch einem anderen Datenschutzniveau unterliegt. Die Risiken betreffen dabei nicht nur den grundlegenden Schutz vor Datenmissbrauch, sondern vor allem die Auseinandersetzung mit Datenschutzgesetzen des jeweiligen Staats. Meist werden in Verträgen der Anbieter Vereinbarungen zu Erhebung, Verarbeitung und Nutzung der Daten getroffen, die bindend für beide Vertragsseiten sind.[6]

Vom Safe-Harbor-Abkommen zum Privacy Shield Framework

Das Safe-Harbor-Abkommen war eine Vereinbarung zwischen der EU und dem Handelsministerium der USA, welches in der Zeit von 6.7.2000 bis 6.10.2015 bestand.[7] Das Abkommen regelte die Speicherung und Verarbeitung personenbezogener Daten von EU-Bürgern in den USA. Am 6.10.2015 wurde diese Vereinbarung vom Europäischen Gerichtshof für ungültig erklärt, mit der Begründung, dass im Hinblick auf die Angemessenheit des Schutzes von personenbezogenen Daten ein unzureichendes Schutzniveau vorhanden ist.[8]

Im Juli 2016 wurde von der Europäischen Kommission, dem Handelsministerium der USA und der Schweizer Verwaltung das EU-U.S. und Swiss-U.S. *Privacy Shield Framework*[9] ins Leben gerufen, welches als „Nachfolger" für das Safe-Harbor-Abkommen den Schutz personenbezogener Daten zwischen der EU resp. Schweiz und den USA regelt. Unternehmen können sich für das Framework selbst zertifizieren,[10] was bedeutet, dass die Verwendung des Frameworks auf einer freiwilligen Basis beruht und sicherstellt, dass die im Privacy Shield festgelegten Prinzipien eingehalten werden[11].

2. Festlegung der Kriterien

Auf Basis der gegebenen Gesetzesgrundlage wurden ausgewählte Datenschutzrichtlinien betrachtet, aus denen einzelne Faktoren zur Beurteilung des Schutzes personenbezogener Daten abgeleitet wurden. Anhand von Facebook[12], Amazon[13], Valve[14] und DropBox[15] ergaben sich folgende Kriterien:

Auskunftsanforderung – Das Auskunftsrecht wird in § 34 BDSG festgehalten. Die Auskunft informiert den Nutzer nicht nur über persönlich angegebene, sondern auch automatisiert gesammelte Daten. Als Kriterium wird die Erwähnung und Wahrnehmbarkeit dieses Rechts geprüft.

Die **Datenfreigabe** gilt primär dem Schutz und der Verwaltung personenbezogener Daten. Dieses Kriterium bestimmt, wie und in welcher Form die Freigabe personenbezogener Daten vom jeweiligen Dienst oder Nutzer bestimmt werden kann. Diese Vorgehensweise ist stark vom Unternehmen und dessen Geschäftsinhalt abhängig. Es gibt keine gesetzliche Vorgabe, die dieses Kriterium bestimmt. Ein ausführliches Beispiel gibt die Datenschutzrichtlinie von Facebook[12] unter dem Punkt „Wie werden diese Informationen geteilt?" vor.

Die **Einwilligung** ist in § 4a BDSG sowie Richtlinie 95/46/EG[4] verankert. Als Kriterium wird damit vor allem der Zeitpunkt und die explizite Aufforderung zur Einwilligung betrachtet.

Die **Gültigkeit der rechtlichen Grundlage** bezieht sich vor allem auf die Ereignisse des Safe-Harbor-Abkommens. Nachdem das Abkommen für ungültig erklärt wurde, war es stets Bestandteil vieler Datenschutzrichtlinien. Bis zum Zustandekommen des Privacy Shield Frameworks befanden sich daher in einem Zeitraum von acht Monaten sowohl die Betroffenen als auch die Unternehmen im Unklaren und waren aufgrund fehlender Alternativen in ihrem Handlungsspielraum eingeschränkt.

Jugendschutz – Der Schutz personenbezogener Daten von Minderjährigen besitzt eine Sonderstellung bei Erhebung, Verarbeitung und Nutzung von Daten. In den Richtlinien von Valve wird ausdrücklich erwähnt, dass „Valve […] nicht wissentlich personenbezogene Daten von Personen im Alter von 13 Jahren und darunter […]"[14] erhebt, auch Amazon gibt an, „keine Produkte zum Kauf durch Minderjährige an[zubieten]. […] [Kunden, die] das 18. Lebensjahr noch nicht vollendet haben, dürfen […] nur zusammen mit einem Elternteil oder Vormund […]"[13] Produkte erwerben. Aus rechtlicher Sicht werden jedoch innerhalb des BDSG keine Regelungen getroffen. Hierbei sind die Nutzer auf Vorgaben der Datenschutzrichtlinien zur Erhebung, Verarbeitung und Nutzung des jeweiligen Dienstanbieters angewiesen. Etwaige Maßnahmen, die im Bürgerlichen Gesetzbuch (BGB) festgehalten werden und in solchen Situationen Anwendung finden, werden hier nicht betrachtet.

Das **Löschen** personenbezogener Daten wird erforderlich, sobald eine Speicherung bzw. Ablage in irgendeiner Form erfolgt. Sowohl im BDSG als auch in den meisten Richtlinien wird dieses Kriterium thematisiert.

Sprache – Viele der heutigen Dienstleistungen werden international angeboten, daher ist eine Datenschutzrichtlinie in der eigenen Landessprache nicht selbstverständlich oder gesetzlich verankert. Die verwendete Sprache kann zum Nachteil werden, wenn eine Übersetzung nicht aktuell oder inkorrekt ist. Ein charakteristisches Beispiel dafür liefert DropBox; das Unternehmen schreibt ausdrücklich in seiner Datenschutzrichtlinie: „Diese Übersetzung wird nur zu Informationszwecken bereitgestellt. Bei Unstimmigkeiten gilt der englische Ausgangstext."[15]

Die **Transparenz** von Datenschutzrichtlinien begründet sich in einer verständlichen Erläuterung der verwendeten Methoden zur Datenerhebung, -verarbeitung und -speicherung. Im BDSG werden hierbei § 6c (Mobile personenbezogene Speicher- und Verarbeitungsmedien) im Speziellen erfasst, ebenso wird in § 28b das Verfahren des Scorings beschrieben, welches einen

„[…] Wahrscheinlichkeitswert für ein bestimmtes zukünftiges Verhalten des Betroffenen […]“ (§ 28b Abs. 1) ermittelt. In beiden Paragraphen werden sehr spezifische Themen bestimmt. Eine allgemeine Regel für die Auskunft über den Einsatz bestimmter Cookies o.ä. wird nicht festgehalten.

Das **Übermitteln** (Weitergabe der Daten) an Dritte ist sowohl in § 29 BDSG als auch in der Richtlinie 95/46/EG[5] verankert. Das Kriterium soll darauf aufmerksam machen, in welcher Form und aus welchen Gründen Daten weitergegeben werden (dürfen).

Verständnis – Das Verstehen der Datenschutzrichtlinie bezieht sich auf die angestrebten Nutzergruppen, Struktur und Aufbau des Textes, Eindeutigkeit sowie Erläuterungen von Fachbegriffen. Das Kriterium *Verständnis* ist jedoch schwer rechtlich festzuhalten, da eine genaue Definition von Verständnis vom jeweiligen Vorwissen abhängig ist. Es werden indirekte Angaben zur Verständlichkeit gegeben, bspw. „[…] nachvollziehbar in allgemein verständlicher Form“ (§ 34 Abs. 2 BDSG). Facebook nutzt beispielsweise eine persönliche Anrede und verwendet eine übersichtliche Struktur, die vor allem jüngeren Nutzern zu Gute kommt.[12]

Warnhinweise sind zwar kein Bestandteil von Datenschutzrichtlinien oder Datenschutzregelungen, jedoch sehr hilfreich für Nutzer mit wenig oder gar keinem informations- oder medientechnischen Vorwissen. Sie sollen die Sensibilisierung im Umgang mit personenbezogenen Daten fördern.

Zweckbindung – Der Zweck begründet die Erhebung, Verarbeitung und Nutzung von Daten und muss daher vor jeder Einwilligung bekannt sein (§ 28 BDSG). Anhand der Zweckbindung wird sichtbar, aus welchem Grund bestimmte Daten benötigt werden.

Anwendung der Kriterien auf die Datenschutzrichtlinie von Facebook

Facebook ist ein Gigant der sozialen Netzwerke. Die Datenschutzrichtlinie wird anhand der Kriterien *Löschen*, *Datenfreigabe*, *Einwilligung* und *Auskunftsanforderung* untersucht. Alle verwendeten Informationen sind, sofern nicht anders angegeben, der Facebook-Datenschutzrichtlinie[12] entnommen.

Löschen – Facebook ermöglicht jederzeit das Löschen des eigenen Kontos. Dazu gehören alle Inhalte, die mit diesem Konto verbunden sind. Jedoch können jegliche Informationen, die mit anderen Nutzern geteilt wurden, nicht immer direkt gelöscht werden. Personenbezogene Daten, die von anderen Nutzern zur Person bereitgestellt wurden, sind nicht mit dem Konto verbunden und fallen daher nicht darunter.

Datenfreigabe – Die Verwaltung der eigenen Daten wird in Facebook stark durch das Teilen von Informationen mit anderen gesteuert. Einige Informationen sind öffentliche Inhalte, die auch mit Hilfe von Suchmaschinen eingesehen werden können. Dazu gehören alle Inhalte, die mit der öffentlichen Zielgruppe geteilt werden, das *Facebook Forum* und das öffentliche Profil eines Nutzers (beinhaltet u. a. Nutzername, Altersgruppe, Geschlecht). Geteilte Informationen können durch den Nutzer, mit dem sie geteilt wurden, ebenso weiter geteilt werden. Der Nutzer selbst kann dementsprechend keinen direkten weiteren Einfluss darauf nehmen.

Einwilligung – Aufgrund meiner Recherchen habe ich die Webseite der Datenschutzrichtlinie von Facebook mehrfach verwendet. Nach mehrmaligen Aufrufen der Seite wurde ich mit der folgenden Information konfrontiert: „Cookies helfen uns dabei, Facebook-Dienste anzubieten, zu schützen und zu verbessern. Wenn du unsere Webseite weiterhin verwendest, stimmst du unserer Richtlinie zu Cookies zu.“ Damit erhebt das Unternehmen ohne meine explizite Einwilligung oder die Verwendung eines Facebook-Kontos bereits Daten.

Auskunftsanforderung – Eine persönliche Auskunftsanforderung wird von Facebook nicht angeboten. Es gibt jedoch eine automatisierte und im Account bereitgestellte Option „Deine Daten herunterladen“, die mit dem Konto verbundene Information als komprimierte Datei zusammenstellt.

Aufgrund dieser Auszüge wirft der Datenschutz bei Facebook vor allem im Bereich der Datenfreigabe und der Einwilligung einige Bedenken auf. Eine explizite Einwilligung erfolgt nicht aus freien Stücken und ist dem Nutzer unter Umständen bereits bei der Informationssammlung ein Hindernis oder Ablehnungsgrund. Des Weiteren weist die Datenfreigabe aufgrund der *Teilen*-Funktion erhebliche Gefahren für den Schutz der eigenen Daten auf. Unbedachtes Teilen einer Aussage oder eines Bildes kann damit ungeahnte Konsequenzen nach sich ziehen.

3. Beurteilungssystem für Datenschutzrichtlinien

Aufbauend auf den Kriterien habe ich ein Beurteilungssystem entwickelt, welches eine dem Nutzer vorliegende Datenschutzrichtlinie anhand von gewichteten Kriterien bewertet. Das System zielt auf eine motivierende Strategie ab, die den Betroffenen dazu anhalten soll, den Schutz seiner personenbezogenen Daten bewusst zu handhaben.

Als Basis für das Beurteilungssystem habe ich nach möglichen vorhandenen Vorgehensweisen oder Systemen recherchiert. Die meisten Ergebnisse lieferten Bewertungen spezifischer Datenschutzrichtlinien, jedoch kein umfassendes oder einheitliches System zur Bewertung einer beliebigen Richtlinie.

Nicole Tornow

Nicole Tornow hat an der Friedrich-Schiller-Universität Jena (FSU) Informatik studiert. Nach einem erfolgreichen Abschluss des Masterstudiums ist sie nun als Software-Entwicklerin im E-Commerce-Bereich tätig.

Aufbau und Arbeitsweise des Beurteilungssystems

Mein Beurteilungssystem ist dreischrittig aufgebaut: Gewichtung der Kriterien, Bewertung der Kriterien anhand einer gegebenen Datenschutzrichtlinie und Auswertung. Die Auswertung ergibt eine prozentuale Angabe, die durch farbliche Abstufung repräsentiert wird, welche die Richtlinie in ihrer Gesamtheit beurteilt.

Gewichtung der Kriterien

Für das Beurteilungssystem verwende ich nur eine kleine Auswahl der genannten Kriterien. In Tabelle 1 ist eine beispielhafte Darstellung einer benutzerdefinierten Gewichtung angegeben.

Kriterium	Gewicht g[i]	Gewichtungsfaktor w[i] = g[i] / g_max
Auskunftsanforderung	6	0,6
Datenfreigabe	10	1,0
Einwilligung	7	0,7
Löschen	9	0,9

Tabelle 1: Berechnung von Gewichtungsfaktoren

Die Gewichtung der Kriterien erfolgt durch den Nutzer nach eigenem Ermessen und Wünschen. Der maximale Wert *g_max* eines Gewichts *g[i]* beträgt 10, der minimale Wert ist 0. Wird ein Kriterium mit dem Wert 0 belegt, so geht es nicht in die Berechnung und damit nicht in die Beurteilung ein. Je höher eine Gewichtung angegeben wird, desto stärker fließt die erreichte Punktezahl der Bewertung in das Endergebnis ein.

Bewertung der Kriterien

Die Bewertung eines Kriteriums gibt an, wie gut die Datenschutzrichtlinie diesen Aspekt behandelt. Es können je Kriterium zwischen 0 und 5 Punkten vergeben werden, wobei p_max = 5 Punkte die höchste und damit beste Wertung p[i] für ein Kriterium darstellt. Tabelle 2 zeigt die Bewertung von Kriterien. Die Abstufung zwischen den Punkteniveaus könnte folgendermaßen beschrieben werden:

Das Kriterium …

0 – … wird in der Datenschutzrichtlinie nicht erwähnt oder besitzt eine gesetzwidrige oder nicht akzeptable Aussage.

1 – … ist nur unzureichend oder indirekt beschrieben. Die resultierende Aussage ist nur unter expliziter Beachtung seitens des Nutzers vertretbar. Viele Fragen bleiben offen.

2 – … ist direkt beschrieben. Es sind jedoch starke Einschränkungen vorhanden.
Beispiel: Die Datenfreigabe bei Facebook bedarf eines bewussten Vorgehens des Nutzers. Die Teilen-Funktion enthält die Gefahr, dass Daten durch weiteres Teilen öffentlich einsehbar werden und gegebenenfalls nicht vollständig gelöscht werden können.

3 – … ist direkt und ausreichend beschrieben. Es sind Einschränkungen vorhanden.

4 – … ist direkt, ausreichend und akzeptabel beschrieben. Damit verbundene Überprüfungen oder Maßnahmen sind jedoch nicht vollständig aufgezeigt. Kleinere Einschränkungen sind vorhanden.
Beispiel: Der Jugendschutz wird bei Amazon eindeutig in der Richtlinie beschrieben. Maßnahmen zur Überprüfung sind jedoch nur indirekt oder gar nicht genannt.

5 – … ist in der Datenschutzrichtlinie vollständig mit zugehörigen Maßnahmen und Regelungen beschrieben.
Beispiel: Die Auskunftsanforderung der Otto GmbH[16] ist eindeutig auf ihrer Datenschutz-Webseite sichtbar und referenziert entsprechende Paragraphen des BDSG.

Berechnung und Aussage der Bewertung

Tabelle 2 beschreibt beispielhaft die Zusammenführung der Gewichtung der Kriterien mit den für die Kriterien erreichten Punkten. Verwendet werden die Gewichtungen aus Tabelle 1. Die Farbkodierung (Färbung) richtet sich nach Tabelle 3.

Kriterium	Punkte p[i]	Gewicht w[i]	Ergebnisse p[i] × w[i]
Auskunftsanforderung	4	0,6	2,4
Datenfreigabe	2	1,0	2,0
Einwilligung	1	0,7	0,7
Löschen	3	0,9	2,7
Erreichte Punkte S = $\sum$ p[i] × w[i]			7,8
Maximal erreichbar S_max = p_max × $\sum$ w[i]			16,0
Relatives Ergebnis Q = 100 × S / S_max			48,75 %
Färbung			**ausreichend**

Tabelle 2: Gesamtauswertung

4. Bewertung der Datenschutzrichtlinie von Facebook anhand des Beurteilungssystems

Nun bewerte ich die Datenschutzrichtlinie von Facebook im vorgestellten Beurteilungssystem anhand der ausgewählten vier Kriterien. Die Gewichtung der Kriterien wurde in Tabelle 1 bereits dargestellt, die Bewertung der Kriterien in Tabelle 2 begründe ich wie folgt:

Auskunftsanforderung: 4 – Die Auskunftsanforderung wird relativ einfach für den Nutzer innerhalb dessen Accounts gelöst. Der Betroffene kann sich eine Datei mit den Daten, die mit seinem Konto verbunden sind, herunterladen. Inwiefern diese Funktion vollständig ist bzw. welche Resultate geliefert werden, kann hier nicht beurteilt werden.

Datenfreigabe: 2 – Die Datenfreigabe bei Facebook wird vor allem durch die *Teilen*-Funktion sehr unübersichtlich. Facebook beschreibt in seiner Datenschutzrichtlinie ausführlich, in welcher Form und mit welcher Auswirkung das Teilen die Handhabbarkeit der eigenen Daten beeinflusst. Der Nutzer sollte hier keinesfalls gedankenlos Informationen weitergeben.

Einwilligung: 1 – Der Besuch einer Webseite des Unternehmens aktiviert nach bestimmter Zeit Cookies, die automatisch Daten erheben, unabhängig davon, ob der Nutzer ein Facebook-Konto besitzt. Zwar werden Hinweise darauf gegeben, dass bei weiterem Nutzen der Facebook-Seite die Cookies aktiviert werden, jedoch gibt es keine explizite Einwilligung oder Ablehnung.

Löschen: 3 – Facebook ermöglicht jederzeit das Löschen des eigenen Accounts und damit verbundener Daten. Jedoch ist es nicht möglich, alle Daten zur eigenen Person vollständig zu entfernen.

Die erreichte Bewertung der Facebook-Datenschutzrichtlinie beträgt 48,75 % und ist damit im dunkelgrauen Bereich. Das bedeutet in diesem Fall, dass die Datenschutzrichtlinie zwar gut bis sehr gut aufgebaut und geschrieben ist, sich jedoch Einschränkungen für die personenbezogen Daten ergeben, die sehr gravierend sind. Insbesondere die Kriterien der Datenfreigabe und der Einwilligung zeigen aufgrund ihrer hohen Gewichtung und niedrigen Bewertung einen deutlichen Einfluss in der Berechnung.

5. Schlussfolgerung und Ausblick

Rückblickend wird deutlich, dass sowohl die Datenschutzrichtlinien als auch die Datenschutzgesetze unterschiedliche Kriterien hervorgebracht haben. Es gab auf beiden Seiten Übereinstimmungen wie die Auskunftsanforderung und das Löschen von Daten. Jedoch wurden auch Kriterien gefunden, wie der Jugendschutz, die in den Datenschutzgesetzen keine Rückendeckung erhalten. Durch die gesetzliche Vorgabe wurde deutlich, wie wichtig die Einwilligung und Zweckbindung in Bezug auf die Erhebung, Verarbeitung und Nutzung von Daten ist.

Die zu Beginn gestellte Frage kann daher nur hinsichtlich der Wiedergabe der Datenschutzrichtlinie durch den Filter der Kriterien beurteilt werden. Mit den vorgestellten Kriterien können die wichtigsten und datenschutzrechtlich relevanten Aspekte betrachtet werden. Änderungen an der Datenschutzrichtlinie können mit diesem Vorgehen nur durch ein erneutes Abarbeiten der Kriterien erfasst werden (sofern keine eindeutigen Kennzeichnungen über die Änderungen vorgenommen wurden). Zusammenfassend bilden die Kriterien eine gute Abdeckung der betrachteten Datenschutzrichtlinien, müssen jedoch im Einzelfall durch weitere Faktoren erweitert werden.

Letztendlich ermöglicht diese Vorgehensweise, den Berg an heutigen Datenschutzrichtlinien zu bewältigen. Der damit verbundene Aufwand ist für den Betroffenen dennoch sehr hoch. Die gegebenen Bewertungen der Kriterien bedürfen der Erarbeitung eines Vorwissens zumindest in datenschutzrechtlicher Sicht. Die Erfahrung und Expertise im Hinblick auf Datenschutzrichtlinien kann mit der Bearbeitung und damit aktiven Auseinandersetzung der Thematik gewonnen werden. Damit bleibt dennoch das Problem: Die Informationslast bleibt beim Betroffenen.

Das vorgestellte Beurteilungssystem stellt eine mögliche Herangehensweise zur Beurteilung von Datenschutzrichtlinien dar. Das Fokussieren auf einzelne Kriterien kann hierbei den Blick für das Wesentliche erleichtern. Die Wahl und Erweiterung der Kriterien kann sich darüber hinaus speziell an den Eigenschaften des Dienstleisters (bspw. Soziale Netzwerke, Online-Shops) orientieren und somit eine zielgerichtete Beurteilung ermöglichen.

Die Bewertung der Kriterien ist dabei der kritische Aspekt des Systems. Hierbei stellt sich die Herausforderung, entsprechende Textanalysewerkzeuge zur automatischen Beurteilung zu entwickeln. Die Idee basiert hierbei darauf, dem Nutzer möglichst viel der angesprochenen Informationslast abzunehmen und darüber hinaus für den Schutz der eigenen personenbezogenen Daten zu motivieren.

Ein Einsatz des Beurteilungssystems liegt vor allem im App-Anwendungsbereich oder als Browser-Plugin. Mithilfe einer Farbkodierung könnten damit visuelle Empfehlungen in Abhängigkeit der benutzerdefinierten Gewichtung gegeben werden.

Referenzen

1 *Datenschutz-Wiki (2016) Informationelle Selbstbestimmung. 28.4.2016, https://www.datenschutz-wiki.de/Informationelle_Selbstbestimmung*

2 *Europäische Gemeinschaften (1995) Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Abl. L 281, 23.11.1995, S. 31, http://eur-lex.europa.eu/eli/dir/1995/46/oj*

3 *Europäische Gemeinschaften (1999) Beschluss des Gemeinsamen EWR-Ausschusses Nr. 83/1999 vom 25. Juni 1999 zur Änderung des Protokolls 37 und des Anhangs XI (Telekommunikationsdienste) zum EWR-Abkommen. ABl. L 296, 23.11.2000, S. 41, http://eur-lex.europa.eu/eli/dec/1999/83(2)/oj*

Relatives Ergebnis Q	Farbe	Bedeutung
$Q < 40\,\%$	**durchgefallen**	Die Datenschutzrichtlinie weist eindeutige Mängel auf. Von einer Einwilligung wird abgeraten.
$40\,\% \leq Q < 60\,\%$	**ausreichend**	Die Datenschutzrichtlinie ist inhaltlich ausreichend beschrieben und kann unter Beachtung der Einschränkungen akzeptiert werden.
$60\,\% \leq Q < 80\,\%$	**gut**	Die Datenschutzrichtlinie ist inhaltlich gut aufgestellt und kann unter Berücksichtigung kleinerer Einschränkungen akzeptiert werden.
$80\,\% \leq Q$	**sehr gut**	Die Datenschutzrichtlinie ist inhaltlich sehr gut aufgebaut und kann mit bewusstem Umgang akzeptiert werden.

Tabelle 3: Farbkodierung

4 *Der Europäische Datenschutzbeauftragte (2016) Berechtigte Gründe für die Verarbeitung personenbezogener Daten. https://web.archive.org/web/20160621152314/https://secure.edps.europa.eu/EDPSWEB/edps/lang/de/EDPS/Dataprotection/QA/QA6 (27.5.2017)*
5 *Der Europäische Datenschutzbeauftragte (2016) Übermittlung personenbezogener Daten. https://secure.edps.europa.eu/EDPSWEB/edps/lang/de/EDPS/Dataprotection/QA/QA9 (27.5.2017)*
6 *Der Europäische Datenschutzbeauftragte (2016) Cloud-Computing. https://web.archive.org/web/20160621152452/https://secure.edps.europa.eu/EDPSWEB/edps/lang/de/EDPS/Dataprotection/QA/QA10 (27.5.2017)*
7 *Safe Harbor (2017) https://www.datenschutz-wiki.de/Safe_Harbor (27.5.2017)*
8 *Export.gov (2017) U.S.-EU Safe Harbor List. https://safeharbor.export.gov/list.aspx (27.5.2017)*
9 *International Trade Administration (2017) Privacy Shield Overview. https://www.privacyshield.gov/Program-Overview (27.5.2017)*
10 *International Trade Administration (2017) Self-Certification Information. https://www.privacyshield.gov/article?id=Self-Certification-Information (27.5.2017)*
11 *International Trade Administration (2017) Privacy Shield Framework. https://www.privacyshield.gov/EU-US-Framework (27.5.2017)*
12 *Facebook (2017) Datenrichtlinie. https://de-de.facebook.com/privacy/explanation (3.3.2017)*
13 *Amazon.de (2017) Amazon.de-Datenschutzerklärung. http://www.amazon.de/gp/help/customer/display.html?nodeId=3312401 (3.3.2017)*
14 *Valve (2017) Einverständnis zu den Datenschutzrichtlinien. http://store.steampowered.com/privacy_agreement/ (3.3.2017)*
15 *DropBox (2017) Dropbox-Datenschutzrichtlinien. https://www.dropbox.com/privacy (3.3.2017)*
16 *Otto (2017) Datenschutz. https://www.otto.de/shoppages/service/about/datenschutzinformation (4.3.2017)*

Sarah Schott und Claudia Sichting

Roboter im Alltag: Wer trägt Verantwortung bei Schutzbefohlenen?

Roboter, die mit Kindern spielen, im Alltag helfen und auf Gefühle reagieren: das ist doch Science-Fiction! Warum sollten wir uns da schon jetzt mit dem Datenschutz befassen? Die französische Firma Aldebaran[1], eine Tochterfirma von SoftBank Robotics, bietet bereits einen solchen Roboter mit Namen Pepper für Privatpersonen in Japan an und will das Angebot schrittweise auf andere Länder ausdehnen. Somit ist jetzt der gebotene Zeitpunkt, die Fähigkeiten der Roboter auszuloten und bei Bedarf das Datenschutzrecht anzupassen. Wartet man erst, bis sich die Entwicklung auch in Europa durchgesetzt hat, wird zwischenzeitlich oder auf lange Sicht der Schutz der Privatsphäre riskiert.

1. Roboter

Nur 1,20 m bzw. 1,40 m groß, mit Kunststoffgehäuse und comichaftem Gesicht sind die beiden *Aldebaran*-Modelle *Pepper* und *Romeo* deutlich als humanoide Roboter zu erkennen. *Pepper* (siehe Abbildung 1) soll, mit der Erkennung von Gefühlen in einem Gespräch, der Unterhaltung dienen und im Marketing und in familiärer Umgebung eingesetzt werden.[2,3] Ziel des *ROMEO*-Forschungsprojektes ist es, einen Roboter zu entwickeln, der Personen mit eingeschränkter Selbstständigkeit im Alltag unterstützt.[4]

Für die Bewältigung ihrer Aufgaben verfügen beide über eine Vielzahl an Sensoren, darunter Mikrophone, diverse Kameras, Ultraschall-, Beschleunigungs-, und Drucksensoren. *Pepper* ist konstant mit dem Internet verbunden, um Informationen wie passende Gesprächsantworten aus einer Datenbank, neue Programme und Updates abrufen zu können. Im Gegensatz dazu scheint *Romeo* auf einen lokalen Speicher beschränkt zu sein, denn ein wichtiger Teil der Forschung widmet sich verschiedenen Lernmethoden und Erinnerungsmechanismen, die die Bedeutung von Informationen bestimmen und diese dann komprimieren, verknüpfen, speichern oder vergessen.

Im Folgenden haben wir die von den Entwicklern angestrebten Aufgaben[2,3,4] der Roboter und die zugehörigen Daten mit besonderer Relevanz für den Datenschutz gelistet:

- Identifikation von Geräuschquellen und audiovisuelles Tracking
- Betreten oder Verlassen des Raums durch Personen
- Gesichtserkennung und Sprecheridentifizierung
- Zusammenarbeit mit Menschen und optimale Anpassung an den Nutzer
- Unterstützung bei Planungen wie Tagesablauf und Einkaufsliste
- Feststellen ungewöhnlicher Situationen und entsprechendem Handlungsbedarf (Information Notfalldienst)
- Alltagsmanagement (beinhaltet medizinische Daten)
- Führen von Alltagsgesprächen und Erkundigung nach Befinden
- Unterstützung bei Verarbeitung klinischer Informationen
- Vermeiden von Langeweile und Isolation durch Anregung zu sozialer Interaktion mit anderen Menschen
- Erhalt intellektueller Aktivität durch Spiele
- Verstehen und Befolgen von Anweisungen
- Erkennen und Analysieren individueller Verhaltensweisen
- Charakterisierung von Verhalten und Interaktionen
- Erkennung von Emotionen, generellem Aktivitätslevel
- Uhrzeit und Datum bei Verknüpfung mit anderen Informationen

Bisher werden *Romeo*-Prototypen erst in der Forschung eingesetzt, für unsere Analyse unterstellen wir Marktverfügbarkeit.

2. Zentrale Datensammlung

Die kritischste Eigenschaft *Peppers* ist die autonome Internetverbindung. Genau hier kommen wir zum eigentlichen Thema: dem Datenschutz. Der Roboter soll daheim die Familie unterhalten, dabei hat „er" Einblick in das gesamte Familienleben. Solange er angeschaltet und aufgeladen ist, hört und sieht er alles, was passiert. Diese Daten werden gespeichert und zur Auswertung an die *cocoro SB Corp.* gesendet. *Cocoro SB Corp.* ist eine Tochtergesellschaft der *SoftBank Corp.*, einer japanischen Mobilfunk-Firma, die 2013 *Aldebaran* zu großen Teilen aufgekauft hat.[5]

Auf der Website von cocoro SB findet man den Slogan: „Aiming to create a society where robots and people coexist"[6], zu deutsch etwa: „Mit dem Ziel, eine Gesellschaft zu erschaffen, in der Roboter und Menschen zusammenleben". In der Beschreibung des Unternehmens steht *Cloud AI service* neben *robot part time job dispatch service*.[7] Das Interessante ist hierbei der Cloud AI service. Bekannt ist die Cloud als Form mehrerer zentraler Rechner, die mehr Speicherplatz und Rechenkapazität bieten als lokale. Im Falle von Pepper ist dies die künstliche Intelligenz (KI) des Roboters. Aus den übermittelten Daten wird eine Antwort berechnet. Noch ist dem Roboter das Warten auf die Serverantwort durch die vergehende Zeit bis zu seiner Antwort anzumerken.

Es ist nicht vorherzusehen, welche Daten dem Roboter und somit der *SoftBank Corp.* anvertraut werden. Man muss genügend Vertrauen in die Firma haben, dass sie die Daten nicht an Dritte weitergibt und niemand von außen Zugriff auf sie hat. Ähnlich gelagert scheint hier die Debatte über die *Hello Barbie* von *Mattel,* die auf Knopfdruck Gespräche mitschneidet, extern auswertet und speichert. Die Daten sind über eine App für Eltern abrufbar. Im Gegensatz zur *Barbie* nimmt *Pepper* die Daten immer auf und verfügt über eine permanente Internetverbindung.[8]

Der Trend zum externen Server für Spracherkennung, um lokalen Speicherplatz und Rechenzeit zu sparen, birgt hohe Risiken. Der Nutzer unterhält sich gar nicht mit einem Roboter, sondern mit den Servern einer Mobilfunk-Firma. Die unschuldige Miene des Roboters erweckt Vertrauen, so dass man bereitwilliger sensible Daten preisgibt, die somit ihren Weg auf den Server finden. Die Daten aller User sind zentral gespeichert, so dass eine einzige Sicherheitslücke des Servers reicht, um an die Daten aller *Pepper*-Benutzer zu gelangen. Der Datenklau wird vom Verbraucher erst bemerkt, wenn die Firma die Sicherheitslücke bekannt gibt.

Nur wenige Menschen haben das Bedürfnis, wie bei *Big Brother* alles über sich öffentlich preis zu geben, aber gerade *Pepper* vertraut man wahrscheinlich mehr an, als den Verkäufern im *SoftBank*-Laden. Mit dem ungleichen Vertrauensverhältnis werden Personen immer mehr Informationen entlockt, die keinen Nutzen in der Interaktion mit dem Roboter haben. Die Firma könnte in neue Geschäftszweige expandieren, da sie die Wünsche der Bevölkerung kennt, bevor sich diese dessen überhaupt bewusst ist. *Pepper* kann auch Schaden anrichten, indem er Daten von Ereignissen speichert, an die man sich nicht erinnern möchte. Um die Daten zu löschen, muss man diese auf dem zentralen Server entfernen.

Die Kritik an der zentralen Datensammlung findet sich sogar in der *Resolution 68/167 der UN-Generalversammlung über das Recht auf Privatheit im digitalen Zeitalter*[9] wieder. Hier wird festgestellt, dass die Privatsphäre durch die technologischen Entwicklungen in unvorhersehbarem Maß gefährdet ist. Die Fähigkeiten, die Kommunikation des Roboters mit dem Server abzufangen oder zu manipulieren, können nicht vorausgesagt werden, daher besteht ein Sicherheitsrisiko, das in keinem Verhältnis zum Nutzen von *Pepper* steht.

Die o. g. Resolution bezieht sich dabei auch explizit auf Artikel 12 der *Allgemeinen Erklärung der Menschenrechte*, der lautet:

> *Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.*

Roboter wie *Pepper* sind ein Teil dieser Entwicklung, an dem der Eingriff in dieses Menschenrecht sehr deutlich wird. Werden unkontrolliert Daten im Internet veröffentlicht, die im Familienkreis aufgenommen wurden, so könnten private Äußerungen anderen Internetnutzern missfallen und durch soziale Netzwerke so oft geteilt werden, bis es auch in den Nachrichten zu sehen ist. Es könnte zum Jobverlust und gesellschaftlicher Ausgrenzung führen. Als Reaktion würde die Meinungsfreiheit durch eigenständige Anpassung beschränkt. Oft entziehen sich Unternehmen der Verantwortung, indem die Allgemeinen Geschäftsbedingungen den Verzicht bestimmter Rechte des Nutzers beinhalten.

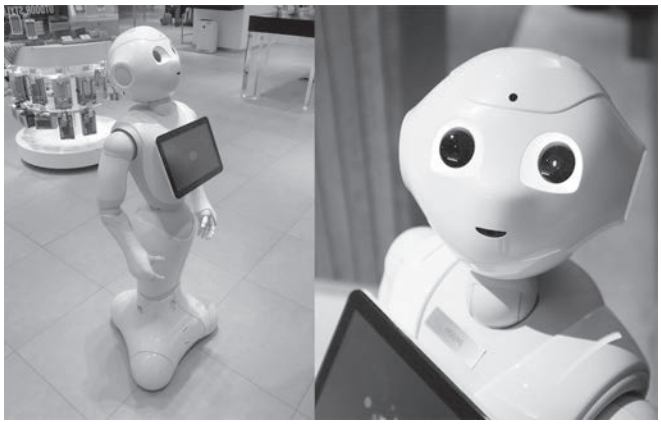


Abbildung 1: Pepper, ein humanoider Roboter für den Privatgebrauch

Mit dem § 3a BDSG zur Datenvermeidung und Datensparsamkeit wird bewusst, dass eine Datenerhebung einem Zweck folgt. Bei *Pepper* ist laut Werbung Unterhaltung der Zweck. *Pepper* kann keine Dinge transportieren oder anders helfen. Der eigentliche Zweck scheint das Sammeln von wertvollen Daten, die die Firma kommerziell nutzen kann – dem Prinzip folgend: Wissen ist Macht und Geld ist Macht.

Unterstrichen wird dies durch die Worte des CEO von *Aldebaran* Bruno Maisonnier[10]: *Mit niedlichen Robotern, so niedlich, dass Leute sie daheim haben wollen, mit denen sie leicht interagieren können und die ans Internet angeschlossen sind, öffnen wir*

ein großes Potenzial (aus dem Englischen sinngemäß übersetzt). Hier stellt sich die Frage, für wen dieses große Potenzial geöffnet wird. Denn gerade niedliche Roboter entlocken uns mehr sensible Daten, als uns bewusst ist.

Oft werden Dinge mit Internetanschluss als zeitgemäß und innovativ beworben. Die Preise für diese Geräte sind sehr niedrig, denn obwohl der Nutzen für den Einzelnen gering ist, so ist der Nutzen für die verkaufenden Firmen enorm. Eine Beschränkung auf wenige, für die KI nötige, Daten ist bei Robotern wie *Pepper* oder *Romeo* kaum zu erwarten, da ein immer besseres Ergebnis erzielt wird, je mehr Daten einer KI zur Verfügung stehen. Durch dieses Argument lassen sich viele Daten sammeln, die eventuell nicht oder nur wenig von der KI genutzt werden, aber für das Unternehmen einen großen Wert darstellen. Und selbst wenn bestimmte Daten nicht übermittelt und gespeichert werden dürften, kann man nie sicherstellen, dass die KI diese Daten nicht doch aus den restlichen vorhandenen Daten ablesen kann.

Bei *Post-Privacy*[11] geht man davon aus, dass Privatsphäre im gewohnten Rahmen nicht mehr möglich sein wird. Die Verteilung von Daten, die einmal im Internet sind, kann man nicht mehr aufhalten und Daten, auf die nicht zugegriffen werden kann, sind nicht nützlich. Bei *Pepper* stellt sich die Frage, für wen die Daten nützlicher sind: Für den Kunden, der einen kleinen Preis für einen 1,20 m großen niedlichen Roboter zahlt, oder für die Mobilfunk-Firma *SoftBank Group*?

Insbesondere die Verwendung des Roboters in Geschäften zeigt den Nutzen des humanoiden Unterhalters für Unternehmen. Kunden, die normalerweise vorbeigehen würden, bleiben stehen und *Pepper* entlockt ihnen ihre Präferenzen, die anschließend gewinnbringend in Werbekampagnen eingesetzt werden können. Die Firma kann, dank der KI von *Pepper*, ihre Kunden besser einschätzen. Gefühlserkennung und passende Reaktion sind bei den Videos im Netz noch nicht bemerkbar. Aber er sieht niedlich aus und gestikuliert viel. Oft ergreift auch der Roboter selbst die Initiative und stellt Fragen, um an bestimmte Daten zu kommen.[12]

Diese Firmen kaufen andere Dienstleistungsunternehmen auf, sie wissen, worin sie investieren müssen, denn sie wissen, was ihre Kunden wollen. Sie wissen sogar alles über die Familie und können so schon die Kleinsten zu ihren Kunden erziehen. Diese Unternehmen haben dann schnell eine Monopolstellung auf dem Markt, denn je mehr Daten sie aggregieren, um so mächtiger werden sie und um so mehr übernehmen sie gewinnbringende Marktanteile.

SoftBank ist lange nicht mehr nur ein japanischer Mobilfunk-Anbieter, sondern investierte auch in einen amerikanischen Mobilfunk-Betreiber, in eine Video-Streaming Website, einen indischen Onlineversandhandel und eine Firma, die Online-Spiele entwickelt. Wo sich die nächste Investition lohnt, könnte die *SoftBank Group* durch die *Pepper*-Nutzer erfahren. *Pepper* ist dafür noch nicht nützlich genug, aber der nächste preiswerte Heimroboter wird auf einem ähnlichen Geschäftsmodell basieren. Und vorher sollten wir dieser Entwicklung entgegenwirken.

3. Datenschutz von Personen mit gesetzlichem Vertreter

Personenbezogene Daten sind laut § 3 Abs. 1 BDSG Daten, anhand derer eine Person identifiziert werden kann. Betrachtet man die von den Robotern gesammelten Daten einzeln, gilt dies nur für einen Teil der Daten. Wir halten es jedoch auf Grund der Verknüpfung der Einzeldaten für sinnvoll, die Daten in ihrer Gesamtheit als personenbezogene Daten einzustufen.

Zur Erhebung, Verarbeitung und Nutzung von Daten ist im Normalfall entsprechend § 4a BDSG eine Einwilligung des Betroffenen nötig. Nun stellt sich die Frage, wann und in welcher Form man diese hinsichtlich der Datenerfassung durch diese Roboter abgibt. Für den Käufer eines Roboters ist es möglich, die Einwilligung im Rahmen des Kaufvertrages zu geben. Von der Datensammlung eines Roboters sind aber auch weitere Personen betroffen.

Wird der Roboter in einer Familie eingesetzt, sind auch Kinder und der Partner des Käufers betroffen. Der Partner kann den Kaufvertrag mit unterzeichnen, Eltern können die Einwilligung als gesetzliche Vertreter ihrer Kinder geben. Die nächsten Betroffenen sind Besucher in einem Haushalt mit Roboter. Eine Möglichkeit wäre, die Verantwortung vertraglich mit entsprechender Aufklärung an den Käufer zu übertragen. Dann ist es seine Aufgabe, den Roboter deaktiviert zu lassen, bis die jeweilige Person zugestimmt hat. Diese Deaktivierung könnte dann durch eine Protokollierung der Aktivitäten des Roboters nachgewiesen werden.

Eine ausführliche und juristisch sichere Aufklärung des Käufers wird in einem sehr langen und komplexen Vertrag resultieren. Dies birgt das Risiko, dass viele Menschen dem Vertrag einfach so zustimmen, da es eine Voraussetzung für die Nutzung ist, ähnlich der Nutzungsbedingungen sozialer Netzwerke. Der Entwickler könnte den Eigentümer unterstützen, indem die Aufzeichnung des Roboters bei Erkennen einer Person, deren Einwilligung fehlt oder nicht zweifelsfrei erkennbar ist, gestoppt wird.

In einer sozialen Einrichtung oder einem Unternehmen wäre der Betreiber verpflichtet, die Einwilligung aller Mitarbeiter, Kun-

Sarah Schott und Claudia Sichting

Sarah Schott studiert zur Zeit im Studiengang B. Sc. Bioinformatik an der Friedrich-Schiller-Universität Jena (FSU). Sie ist Vorstandsmitglied der *Jugend- und Entwicklungspartei Deutschlands* (JED).

Claudia Sichting ist Studentin der Bioinformatik an der Friedrich-Schiller-Universität Jena (FSU).

den und betreuten Personen einzuholen. Auf Grund der großen Anzahl betroffener Menschen in einer solchen Situation wäre ein automatisierter individueller Aufzeichnungstopp wohl nicht praktikabel. Eine automatische Abschaltung käme ohnehin nicht unbesehen in Frage, da erhebliche Verletzungsgefahr bestünde, wenn ein Roboter z. B. gerade jemandem beim Aufstehen hilft und die Person dann infolge der Abschaltung stürzen würde. Insgesamt hätte der Besitzer eines Roboters ein erhebliches Restrisiko hinsichtlich der Wahrung der Rechte aller Betroffenen zu tragen.

Ein weiterer Punkt ist das Auslesen und die Übertragung von Roboterdaten. Zum Ersten wäre sicherzustellen, dass die Übertragung zwischen Roboter und Datenbank oder Notfalldienst nicht von Unbefugten auslesbar oder manipulierbar ist, was aber zum Beispiel durch Verschlüsselung gelöst werden könnte.

Bei *Romeo* könnte zudem der Zugriff auf bestimmte Daten beschränkt werden. Jemand, der die Steuerung in einem Notfall übernimmt, braucht nur Informationen zur konkreten Situation, zu Ursachen und aktuelle Sensordaten. Ein Techniker benötigt nur systemrelevante Daten, die restlichen persönlichen Daten können separat verschlüsselt gespeichert werden und der Besitzer erhält den Schlüssel beim Kauf. Ist der Käufer eine Einrichtung, muss dieser Zugriff in der Einverständniserklärung mit berücksichtigt werden oder der Hersteller vernichtet den zugehörigen Schlüssel, dies ermöglicht bestmöglichen Schutz.

Im Bezug auf *Romeos* Datenübertragung an den Notfalldienst ist zu beachten, dass dies ein automatisiertes Abrufverfahren entsprechend § 10 BDSG ist und nach Abs. 4 die Verantwortung für die Zulässigkeit beim Empfänger liegt. Ist der Notfalldienst eine nahegelegene medizinische Einrichtung, so halten wir es für sinnvoller, dass der Einrichter der Verbindung die Verantwortung trägt. Zudem stellen wir uns die Frage, ob *Romeo* private Daten bei der Interaktion mit mehreren Nutzern weitergibt, wenn er zu gemeinsamer Interaktion anregt.

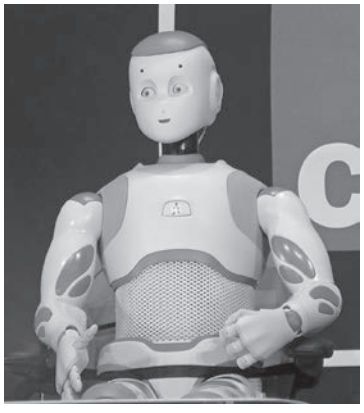
Wer trägt nun welche Verantwortung für den Datenschutz bei Personen mit gesetzlichem Vertreter? Der Betroffene hat sich entsprechend seiner Möglichkeiten zu informieren und seinen Willen zu äußern. Der gesetzliche Vertreter trägt die größte Verantwortung. Er muss den Betroffenen bei der Auseinandersetzung mit dem Thema unterstützen, sich selbst informieren und eine Entscheidung im Sinne und zum Wohl des Betroffenen treffen. Dabei kann es zur Abwägung kommen, ob ein erleichterter Alltag oder der Schutz der Daten mehr zum Wohl des Betroffenen beitragen. Die rechtliche und moralische Verpflichtung von Hersteller, Verkäufer und Betreiber eines solchen Roboters ist die genaue Befolgung der rechtlichen Vorschriften, wobei Schwierigkeiten bei der Überprüfung der Umsetzung rechtlicher Vorschriften und die Not der Betroffenen nicht ausgenutzt werden sollten.

Auf Grund der Komplexität des Themas sehen wir es als Aufgabe des Staates, gesetzliche Vertreter durch die Garantie einer fachlichen Beratung zu unterstützen. Zudem muss er seine Bürger durch Gesetze und deren konsequente Umsetzung bestmöglich entsprechend ihrer Bedürfnisse schützen. Im Gegensatz dazu ist es die Aufgabe der Gesellschaft, den Staat zu kontrollieren und sich selbstkritisch mit dem Thema Datenschutz und Verantwortung für andere auseinanderzusetzen. Die Selbstverständlichkeit, mit der angenommen wird, dass ein Roboter wie *Romeo* über das Internet mit Nutzerkonten von Streaming-Diensten verbunden ist, um bei Langeweile optimale Empfehlungen für eine Beschäftigung geben zu können, führt zu dem Schluss, dass hier der dringendste Handlungsbedarf besteht. Die Verantwortung von Personen mit Fachkenntnis ist es, den Rest der Gesellschaft zu einer intensiven, öffentlichen und politischen Auseinandersetzung mit der Thematik zu drängen.

Wenn Sie jetzt denken: „Richtig!", dann helfen Sie und beginnen Sie in Ihrem Umfeld etwas zu verändern.

Referenzen

1 *https://www.ald.softbankrobotics.com/en*
2 *SoftBank Robotics Europe (2017) Who is Pepper? https://www.ald.softbankrobotics.com/en/cool-robots/pepper*
3 *Wikipedia (2017) Pepper (Roboter). https://de.wikipedia.org/wiki/Pepper_%28Roboter%29#Design_und_technische_Details*
4 *Aldebaran Robotics (2017) Projet Romeo: Welcome. http://projetromeo.com/en/welcome*
5 *Guizzo, E (2012) Aldebaran Robotics sells majority stake for $100 million [updated]. IEEE Spectrum, 12.3.2012, http://spectrum.ieee.org/automaton/robotics/humanoids/aldebaran-robotics-sells-majority-stake*
6 *SoftBank Group Corp. (2015) cocoro SB Corp. http://www.softbank.jp/en/corp/group/ccr/*
7 *SoftBank Group Corp. (2016) About Us. http://www.softbank.jp/en/corp/group/ccr/about/*
8 *Mattel (2017) Hello Barbie Messaging / Q&A. Hello Barbie FAQ, http://hellobarbiefaq.mattel.com/wp-content/uploads/2015/12/hellobarbie-faq-v3.pdf*
9 *Vereinte Nationen, Generalversammlung (2013) Das Recht auf Privatheit im digitalen Zeitalter. A/RES/68/167, 18.12.2013, http://www.un.org/depts/german/gv-68/band1/ar68167.pdf*
10 *Hornyak T (2014) Meet Pepper, the 'love-powered' humanoid robot that knows how you're feeling. PCWorld, 5.6.2014 http://www.pcworld.com/article/2360360/softbanks-humanoid-robot-pepper-knows-how-youre-feeling.html*
11 *Politik Digital (2012) Thema: Post Privacy vs. Privatsphäre. Netzstandpunkte, 9.1.2012, http://politik-digital.de/netzstandpunkte/pro-contra-post-privacy-vs-privatsphaere-5908/*
12 *CrispyYiger (2014) Talking with a Pepper, Softbank's new robot. YouTube, 17.6.2014, https://www.youtube.com/watch?v=XCrdrcZFDU4*



Der Roboter Romeo, wie am 14.2.2015 auf dem Forum «L'année vue par… les sciences» vorgestellt. Pamputt, CC BY-SA 4.0

Felix Baral-Weber

Eine Spieler-orientierte Kritik an (mobilen) Free-to-Play-Spielen

Heute dominieren F2P (Free-to-Play)-Spiele den mobilen Spielemarkt.[1] F2P-Spiele, das sind Spiele, die kostenlos spielbar sind; oft wird der Nutzer dann im Nachhinein durch Microtransactions zur Kasse gebeten. Diese Monetarisierungs-Methode verändert Spiele grundlegend. Sie kann nicht einfach auf ein Spiel aufgesetzt werden, sie muss integraler Teil des Spieldesigns sein. F2P-Spiele sind sich in einigen Punkten sehr ähnlich. Solche Muster nennt man Patterns*.*

Der Begriff *Pattern* kommt aus der Architektur. Hier werden wiederkehrende Probleme durch eine einheitliche Entwurfsschablone gelöst. Im Spieldesign ist z. B. das Darstellen von Lebensenergie als Lebensbalken ein bekanntes Pattern.

Die folgende Auflistung führt jedoch sogenannte *Dark Game Design Patterns* auf. Der Begriff entstammt der Arbeit *Dark Patterns in the Design of Games* von Jose P. Zagal et al.[2] und ist durch die Website *darkpatterns.org* inspiriert. Ein *Dark Game Design Pattern* wird dort wie folgt definiert:

> *"A dark game design pattern is a pattern used intentionally by a game creator to cause negative experiences for players which are against their best interests and likely to happen without their consent."*[2]

Negativ meint dabei nicht nur direkt negative Effekte, sondern auch indirekte Effekte, wie z. B. eine Sucht, die sich mit der Zeit entwickelt.

Diese Definition wird mir als Leitfaden dienen. Allerdings ist ein Dark Pattern schwer einzugrenzen. Es ist meist nicht einfach als schlecht einzustufen. Ausschlaggebend sind der Kontext, in dem, und die Intention, mit der es eingesetzt wird.

Spielen auf Verabredung

Ein Spiel mit diesem Pattern nötigt den Spieler, zu bestimmten Zeiten zu spielen. Dies kann von mehrfach am Tag zu einmal die Woche reichen. Es gibt dabei ein paar wiederkehrende Muster:

- **Verfall virtueller Güter:** Z. B. müssen im Spiel *Clash of Clans* von *Supercell* regelmäßig die Ressourcenspeicher geleert werden, ansonsten verliert der Spieler die überschüssig produzierten Ressourcen.

- **Echtzeit-Abläufe** beziehen sich auf Spielelemente (z. B. das Verbessern eines Hauses), die ein Warten in Echtzeit benötigen. Die benötige Zeit kann dabei von wenigen Sekunden bis hin zu einer Woche reichen. Der Spieler kann (z. B. aus Ressourcenknappheit bzw. wegen **Energiemechaniken**) jedoch nicht beliebig viele dieser Abläufe gleichzeitig ausführen. Um effizient zu sein, muss er, wenn ein Ablauf fertig ist, das Spiel öffnen, um einen neuen zu starten.

- **Tägliche Belohnung:** Der Spieler bekommt jeden Tag eine Belohnung für das Öffnen des Spiels (Abbildung 1) oder das Erledigen einer kleinen Aufgabe. Oftmals gibt es hier Mechaniken, die **konsekutives Ausführen** dieser Tätigkeit belohnen (Abbildung 2).

Auch bei den **Lootboxen** (virtuelle Kisten, die einen zufälligen Gewinn enthalten) in *Clash Royale* von *Supercell* muss der Spieler mehrere Stunden warten, um die Box öffnen zu können (Abbildung 3, rechts).

Die negativen Effekte dieses Patterns werden meist als Auslöser genutzt, um z. B. eine Microtransaction anzubieten. So kann der Spieler gegen Geld Abläufe beschleunigen oder verfallene Güter wiederherstellen.[2]

Glücksspielelemente

Viele Spiele setzen auf klare Glücksspielelemente, wie eine tägliche Lotterie, Lootboxen oder Glücksspielautomaten (Abbildung 3, links), die als Belohnung genutzt werden können, bei denen aber auch die erarbeitete oder gekaufte Zwischenwährung wieder verloren gehen kann.

Zwischenwährung

Praktisch jedes Spiel bietet eine Zwischenwährung. Diese wird auch Premium-Währung genannt, da sie der Spieler hauptsächlich durch Echtgeld erwerben kann. Durch diesen Umtausch kann der Spieler den realen Wert der Premium-Währung nicht mehr abwägen und trifft so eine impulsivere Entscheidung.[3] Menschen unter 25 Jahren sind besonders anfällig, den Wert der Zwischenwährung falsch abzuwägen.[4]

Der Premiumwährungsladen (Abbildung 4) hat sich in praktisch allen Spielen fast identisch durchgesetzt. Darin kann die jeweilige Währung in gestaffelten Mengen gegen Echtgeld eingekauft werden. Bei praktisch allen Stores gibt es Premium-Währung für 1 € bis zu 200 €.

Diese Währung ist nicht mit den anderen Ressourcen eines Spiels zu verwechseln. Die meisten F2P-Spiele haben mehrere Währungen, die Premium-Währung ist jedoch nicht, oder nur kaum, durch Spielen erwirtschaftbar.

Energiemechaniken

Eine **Energiemechanik** dient dazu, die Spielsitzungen bzw. den Handlungsfreiraum des Spielers zu limitieren oder zu lenken. Energie lädt sich mit der Zeit bis zu einem bestimmten Level auf und wird durch Handlungen im Spiel verbraucht. Je mehr Energie der Spieler aufladen darf, desto länger oder effektiver kann er danach spielen. Ist die Energie verbraucht, wird dies oft als **Auslöser** genutzt, um den Spieler zu einer Microtransaction oder einer anderen für das Spiel vorteilhaften Aktion zu verleiten.

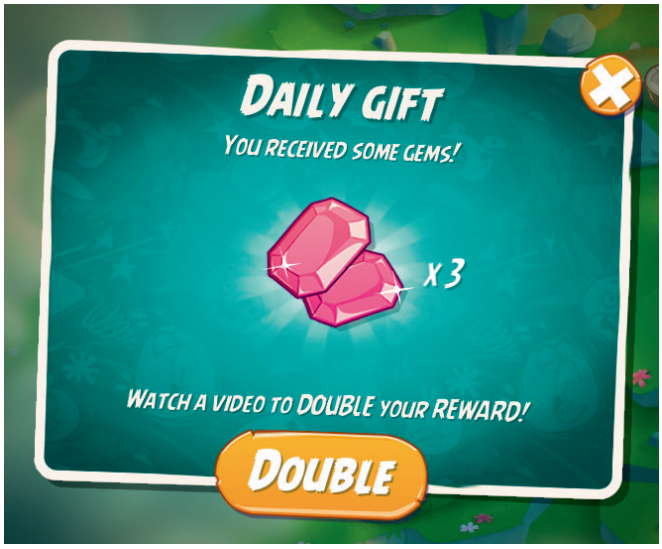


Abbildung 1: In Angry Birds 2 *von* Rovio *wird der Spieler* **jeden Tag einmal** *mit drei Edelsteinen belohnt. Wenn der Spieler ein Werbevideo ansieht, wird sein Gewinn verdoppelt* **(Auslöser).**

Eine beliebte Art der Energie sind Leben, aber an sich ist jede Art von Ressource dafür nutzbar. Wer z. B. in *Candy Crush* von *King* in einem Puzzle verliert, verliert ein Leben. Ein Leben benötigt 20 Minuten, um sich zu regenerieren. Man kann bis zu 5 Leben auf Vorrat halten. Wenn alle Leben aufgebraucht sind, muss man warten oder kann Leben mit der entsprechenden **Zwischenwährung** nachkaufen (Abbildung 5).

Auslöser

Das Spiel präsentiert zur richtigen Zeit die richtige Lösung am richtigen Ort. Wenn der Spieler das Problem eines einsetzenden Verlusts seiner erarbeiteten Güter hat, ermöglicht ihm das Spiel gegen eine Gegenleistung das Weiterspielen. Diese Situation soll den Spieler in einen Impulskauf locken.[3,5]

Die hier angewandte Theorie nennt man *Verlustaversion*[6]. Verluste werden, im Verhältnis zu Gewinnen, für den Spieler überproportional schmerzhaft wahrgenommen. Spiele nutzen dies aus. Dabei wird oft eine Zwischenwährung oder das Ansehen einer Werbung als „Lösegeld" genutzt.[5]

Abbildung 2: In Star Girl *von* Animoca *wird der Spieler für* **konsekutives Einloggen** *belohnt*

Abbildung 3: (Links) Ein Spielautomat aus Crossy Road *von* Hipster Whale, *bei dem* **Zwischenwährung** *gewettet werden kann, um Charaktere freischalten zu können. (Rechts)* **Lootboxen** *in* Clash Royale *von* Supercell, *aus denen zufällige Spielkarten gewonnen werden. Diese benötigen* **Echtzeit,** *um geöffnet zu werden, was als* **Auslöser** *für das Ausgeben der* **Zwischenwährung** *(hier 17 grüne Edelsteine) genutzt wird.*

Eine naheliegende Vermutung ist, dass das Spiel versucht, gerade diese Situationen zu provozieren. Es könnte dem Spieler das Level gerade so schwer gestalten, dass er kurz vor dem Ende verliert (Abbildung 6). Dies ist jedoch recht schwer nachzuweisen.

Drittanbietertools

Drittanbietertools sind Dienste von Dritten, die der Entwickler aus verschiedenen Gründen in das Spiel einbindet. Darunter sind hauptsächlich:

- Analyse und Nutzertracking
- Verbindung zu sozialen Netzwerken
- Preisanpassungen
- Werbung

Dabei können die Tools wie die App selbst auf die Systemfunktionen des Smartphones zugreifen und so Nutzermetriken abgreifen. Diese Funktionen sind selbst für den Entwickler nicht vollständig durchschaubar, der Nutzer weiß jedoch meist gar nicht, was die App einbindet. Wie auch bei Werbung entsteht dadurch eine Privatsphären- und Sicherheitsgefährdung[7].

Für den Browser gibt es schon länger Plugins, wie *Lightbeam*[8] oder *Disconnect*, die visualisieren, welche Drittdienste von einer bestimmten Website eingebunden werden. Ich wollte herausfinden, mit wie vielen Dritten eine App kommuniziert, und habe so ein kleines Tool geschrieben, welches eine ähnliche Visualisierung wie *Lightbeam* erzeugen kann (Abbildung 7). Bei den an-

Abbildung 4: Der **Währungsladen** *in* Smurf 's Village *von* Beeline Interactive

Abbildung 5: Bei Candy Crush Soda *von* King *sind die Leben ausgegangen und regenerieren sich mit 20 Minuten pro Leben.*

gesprochenen Websites handelt es sich um einige CDNs (Content Delivery Networks) sowie Analysenetzwerke. Oft werden jedoch Amazon AWS Server angesprochen, deren Besitzer nicht ohne weiteres erkannt werden können.

Wale

Ein *Wal* (*engl. whale*) ist ein Nutzer, der Geld, oder überdurchschnittlich viel Geld, in einem F2P-Spiel ausgibt. Der Begriff stammt aus der Glücksspielindustrie.[9] Eine aktuelle Studie von *Swrve* zeigt erneut, dass nur ein sehr kleiner Prozentsatz (hier 1,9 %) der Spieler von F2P-Spielen überhaupt etwas zahlt und dass noch weniger Spieler viel zahlen[10]. Das bedeutet, dass ein kleiner Personenkreis das Spielen für die meisten anderen Spieler finanziert. Kritisiert wird dabei oft, dass diese Personen die gleichen Personen sind wie die, die auch zu Glücksspiel neigen, und dass die Spiele darauf ausgelegt sind, die Wale zu fangen[10]. Viele F2P-Mechaniken, wie z. B. **Lootboxen**, erlauben unbeschränkte Ausgaben und stellen ein Suchtpotential dar.

Abbildung 6: Beim Spiel Scubby Dubby Saga *von* King *sind gerade, als nur noch zwei Schaumfelder übrig waren, die Züge ausgegangen. Für 9 Goldbarren (***Zwischenwährung,** *Gegenwert von etwa 0,01 € bis 1 €) können 5 weitere Züge gekauft werden.*

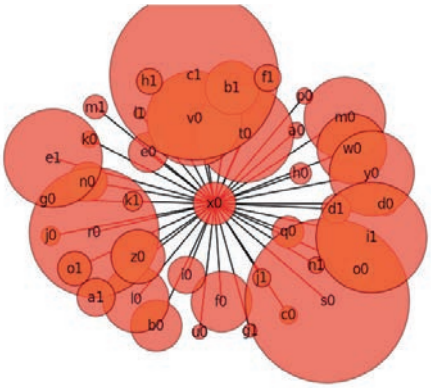


Abbildung 7: Bei Piano Tiles 2 *von* Clean Master Games *werden etwa 40 verschiedene Server angesprochen. Das Spiel finanziert sich über Werbung und bindet viele soziale Netzwerke ein, was die Anzahl der Verbindungen erhöht. Je größer die Blase, desto mehr Daten wurden übertragen.*

Soziale Verstrickung

Soziale Verstrickung (*engl. social entrapment*) bezeichnet das Festhängen des Spielers in dem sozialen Geflecht des Spieles. Er und seine Mitspieler haben ein gegenseitiges Interesse daran, dass der jeweils andere das Spiel weiterführt (Abbildung 8). Dies erhöht die Hürde, das Spiel zu beenden, und sorgt dafür, dass der Spieler das Spiel eventuell länger spielt als er eigentlich will. Zagal et al. bezeichnet dies sogar als soziales Pyramidensystem, bei dem man nur durch das Anwerben immer neuer Mitglieder, die wiederum Mitglieder anwerben, erfolgreich sein kann, ohne die Zwischenwährung einzuwerfen[2]. So kann der Spieler z. B. die virtuelle Farm des Freundes für Extrapunkte pflegen. Dadurch profitiert sowohl der Freund als auch der Spieler.

Abbildung 8: In Blossom Blast *von* King *kann man, wenn die Leben* **(Energiemechanik)** *aufgebraucht sind, von Freunden neue Leben geschickt bekommen.*

Felix Baral-Weber

Felix Baral-Weber, geborener Schwabe, interessierte sich bereits zu seiner Schulzeit für Informatik und Computerspiele. Nachdem er nun seinen Informatik-Bachelor in Jena abgeschlossen hat, will er seine Zeit nutzen, um pretenziöse Computerspiele zu entwickeln.

Fazit

F2P-Spiele bieten Vor- und Nachteile. Gerade bei Multiplayer-Spielen bewährt sich das Modell, da jeder ohne große Investition mitspielen kann. Wer sich jedoch auf ein solches Spiel einlässt, lässt sich auf einen ständigen Kampf gegen das Spiel ein. Das daraus entstehende Metaspiel, der Spieler gegen das manipulative Spiel, kann für den Spieler nachteilhaft sein. Unter diesem Kampf leidet die Beziehung zwischen Spiel und Spieler. Das Spiel wird zum Antagonisten. Es manipuliert, lügt und heuchelt. Durch diese Respektlosigkeit dem Spieler gegenüber hat der Spieler alle Lust daran verloren, für ein F2P-Spiel Geld auszugeben. Fragen Sie mal einen F2P-Spieler, ob er schon einmal Geld für ein F2P-Spiel ausgegeben hat und wie er sich dabei fühlte.

Werbung

Um der Kritik Ausdruck zu verleihen, habe ich, als Bachelorarbeit, ein kleines Mobile-Spiel entwickelt. Dabei versuche ich, die genannten Patterns aufzugreifen und dann ins Lächerliche zu überhöhen. Das Spiel versucht, eine Persiflage mobiler F2P-Spiele zu sein. Es ist noch nicht ganz fertig, soll jedoch bald, und selbstverständlich im F2P-Format, für Android und iOs erhältlich sein. Auf *www.runningwhale.de* findet sich alles Weitere dazu.

Referenzen

1 *App Annie (2015) 2015 gaming report: mobile widens its lead over other platforms. https://www.appannie.com/en/insights/app-annie-idc-gaming-report-2015-review/*

2 *Zagal JP, Björk S, Lewis C (2013) Dark patterns in the design of games. Foundations of Digtal Games, 16.5.2013, Chania, Kreta, http://soda.swedishict.se/5588/1/DarkPatterns.1.1.6_cameraready.pdf*

3 *Madigan J (2015) Getting gamers: the psychology of video games and their impact on the people who play them. Rowman & Littlefield*

4 *Shokrizade R (2013) Monetizing children. Gamasutra, 20.6.2013, http://www.gamasutra.com/blogs/RaminShokrizade/20130620/194429/Monetizing_Children.php*

5 *Adar D (2015) 7 psychological tactics used in games to hook users. 12.10.2015, http://www.doriadar.com/7-psychological-tactics-used-in-games-to-hook-users/*

6 *https://de.wikipedia.org/wiki/Verlustaversion*

7 *Grace MC et al. (2012) Unsafe exposure analysis of mobile in-app advertisements. Proc. 5th ACM Conf. on Security and Privacy in Wireless and Mobile Networks (WISEC '12), Tucson, AZ, S. 101–112*

8 *http://mozilla.org/de/lightbeam/*

9 *Wikipedia (2015) High Roller (Glücksspieler). 22.12.2015, https://de.wikipedia.org/wiki/High_Roller_(Glücksspieler)*

10 *Cifuentes J (2016) Half of all mobile games revenue reportedly comes from only 0.19 % of players. Venturebeat, 23.3.2016, http://venturebeat.com/2016/03/23/half-of-all-mobile-games-revenue-comes-from-only-0-19-of-players-report*

Maximilian Katzmann

Darf Google mein Profilbild verkaufen?

Nach Apple war Google im März 2017 das zweitwertvollste Unternehmen der Welt.[1] Ein großer Anteil der Einnahmen, die das Unternehmen erwirtschaftet, stammt aus Werbung, die Google seinen Nutzern präsentiert. Für die Verwendung vieler Google-Dienste, wie YouTube, Google Drive und Gmail ist das Anlegen eines Google-Kontos erforderlich. Die damit verbundenen Daten benötigt Google unter anderem, um jedem Nutzer relevante Werbung anzeigen zu können. Im Februar 2016 verkündete das Unternehmen, dass monatlich mehr als eine Milliarde Nutzer den kostenlosen E-Mail-Dienst Gmail aktiv verwendeten.[2] Außerdem kündigte Googles CEO Sundar Pichai im September 2015 an, dass monatlich 1,4 Milliarden Nutzer das mobile Betriebssystem Android, welches nicht ohne Google-Konto eingerichtet werden kann, benutzten. Mittlerweile enthalten die meisten Smartphones eine gebündelte Sammlung der persönlichsten Informationen ihrer Nutzer. Zu denen gehören private Konversationen, Fotos von Freunden und Familie, ortsbezogene Daten, welche über den Tag verteilt gespeichert werden, sowie mittlerweile auch Informationen, die unseren Gesundheitszustand beschreiben. All diese Daten werden mit dem Google-Konto verknüpft. Damit ergibt sich eine große Menge an Informationen, die Google zur Verfügung gestellt wird. Um zu verstehen, wie das Unternehmen mit diesen Daten umgeht, sollte man sich dessen Datenschutzbestimmungen anschauen.

1. Googles Datenschutzbestimmungen

Verständlichkeit

Mit elf Seiten sind die Datenschutzbestimmungen des Unternehmens eher überschaubar gehalten.[3] Es handelt sich dabei um eine Datenschutzbestimmung die „für alle Dienste, die von Google Inc. und den verbundenen Unternehmen angeboten werden, einschließlich YouTube, der Dienste, die Google auf Android-Geräten bereitstellt, und der Dienste, die auf anderen Webseiten angeboten werden"[3] gilt. Sie ist eher umgangssprachlich und einfach geschrieben, sodass sie auch für weniger technikversierte Nutzer verständlich ist. Schon zu Beginn der Erklärung beschreibt Google: „Wir haben uns um eine möglichst einfache Darstellung bemüht, wenn Sie jedoch mit Begriffen wie Cookies, IP-Adressen, Pixel-Tags und Browsern nicht vertraut sind, sollten Sie sich zunächst über diese Schlüsselbegriffe informieren", wobei direkt auf eine Seite verwiesen wird, die unter anderen diese Begriffe definiert.[3] Damit wird es dem Nutzer erleichtert, den Formulierungen der Datenschutzbestimmungen zu folgen.

Erhebung von Daten

Im Verlauf des Dokuments wird beschrieben, welche Daten Google sammelt und wie diese erhoben werden. Dazu gehö-

ren Informationen, die man als Nutzer angeben muss, um ein Google-Konto anzulegen, wie beispielsweise der Name, eine E-Mail-Adresse sowie gegebenenfalls Telefon- und Kreditkartennummer. Ein weitaus größerer Anteil der gesammelten Daten wird während der Interaktion des Nutzers mit Googles Diensten erhoben. Darunter fallen zum Beispiel Protokolldaten, wie die IP-Adresse des Nutzers und welches Gerät zur Verwendung des Dienstes benutzt wurde. Zudem wird mit Cookies festgestellt, wie der Nutzer eine Google-Anwendung verwendet, um herauszufinden, wie wahrscheinlich Werbung wahrgenommen wird. Zum besseren Verständnis, welche Cookies das Unternehmen einsetzt, wird eine ausführliche Beschreibung angeboten.[4]

Nutzung erhobener Daten

In Googles Datenschutzbestimmungen wird darauf hingewiesen, dass die gesammelten Informationen dazu verwendet werden, um Google-Dienste zu verbessern und sicherer zu machen sowie Nutzern personalisierte Werbung anzuzeigen. So analysieren automatisierte Systeme die Inhalte der Nutzer, wie zum Beispiel durch das Parsen von E-Mails, um Spam- und Malware-Erkennung bereitzustellen, wovon die Qualität von Googles E-Mail-Dienst profitiert. Außerdem werden die dadurch gewonnenen Informationen verwendet, um Such-Ergebnisse bei der Verwendung von Googles diversen Suchdiensten und angezeigte Werbung an den Nutzer anzupassen. Dies ist ein Beispiel dafür, dass Google „personenbezogene Daten aus einem Dienst mit Informationen und personenbezogenen Daten aus anderen Google-Diensten [verknüpft]“[3].

Weitergabe von Daten

Mit der Einwilligung des Nutzers werden diese personenbezogenen Daten an Unternehmen und Personen außerhalb von Google, zum Beispiel zu Analysezwecken, weitergegeben. Davon ausgenommen sind sensible personenbezogene Daten, wie medizinische Informationen und politische, religiöse sowie sexuelle Neigungen, für deren Weitergabe eine *ausdrückliche* Einwilligung erforderlich ist. Diese wird auch als „informierte Einwilligung“ bezeichnet und unterscheidet sich in wesentlichen Punkten von einer *konkludenten* Einwilligung. Sie zeichnet sich nach § 4a Abs. 1 des Bundesdatenschutzgesetzes dadurch aus, dass der Nutzer die Einwilligung schriftlich erteilt, nachdem er darüber aufgeklärt wurde, zu welchem Zweck die Daten erhoben oder verarbeitet werden und welche Konsequenzen es nach sich zieht, diese Einwilligung nicht zu erteilen. Auch beim Anlegen eines Google-Kontos muss der Nutzer den Nutzungs- und Datenschutzbestimmungen ausdrücklich zustimmen. Hierbei ist es wichtig, anzumerken, dass auch die Zustimmung per Mausklick als ausdrückliche Einwilligung zu verstehen ist. Für die Nutzung einiger Google-Dienste, wie zum Beispiel der Google-Suche, ist es jedoch nicht erforderlich, ein Google-Konto anzulegen. Dennoch werden, wie zuvor beschrieben, Daten erhoben. In diesem Fall handelt es sich jedoch im Gegensatz zur informierten Einwilligung um eine konkludente Einwilligung, also um eine mutmaßliche Zustimmung des Nutzers. Diese wird aus seinem Handeln abgeleitet, ohne ihn zuvor ausdrücklich über die Datenschutzbestimmungen aufzuklären.[5] So wird im ersten Abschnitt von Googles Nutzungsbedingungen, welche die Datenschutzbestimmungen umfassen, erklärt, dass die Nutzung der Google-Dienste voraussetzt, dass der Nutzer diesen Bedingungen zustimmt[6]. Er wird beim Besuchen von Googles Website jedoch nicht darauf hingewiesen, die Nutzungsbestimmungen zu lesen.

Das Unternehmen wird Daten jedoch auch ohne Einwilligung an Unternehmen oder Personen außerhalb von Google weitergeben, wenn es um ein rechtliches Anliegen geht. Dies geschieht, wenn Google nach *Treu und Glauben* davon ausgeht, dass die Weitergabe notwendig ist, um zum Beispiel einer vollstreckbaren behördlichen Anordnung nachzukommen oder die Rechte und Sicherheit von Google, dessen Nutzern oder gar der Öffentlichkeit vor Schaden zu bewahren.[3]

2. Transparenz

Da Google auf verschiedenste Weisen eine große Menge personenbezogener Informationen erhebt, welche auch an andere Unternehmen weitergeleitet werden können, ist es sehr wichtig, dass dem Nutzer dennoch das Recht auf informationelle Selbstbestimmung erhalten bleibt. Dieses wurde aus dem allgemeinen Freiheitsgrundrecht und dem Grundrecht auf Menschenwürde hergeleitet und ist damit Bestandteil des allgemeinen Persönlichkeitsrechts, welches durch Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 des Grundgesetzes geschützt wird.[7] Es gewährleistet das Recht des Einzelnen, über Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. In diesem Sinne stellt Google verschiedene Möglichkeiten bereit, um die vom Unternehmen erhobenen Daten zu bearbeiten, zu löschen und weiteres Erheben zu unterbinden, sofern der Nutzer ein Google-Konto erstellt hat. So kann zum Beispiel der Standortverlauf bearbeitet und dessen Aktualisierung unterbunden werden. Darin können ortsbezogene Daten in Längen- und Breitengraden auf die Sekunde genau verfolgt werden (Abbildung 1).

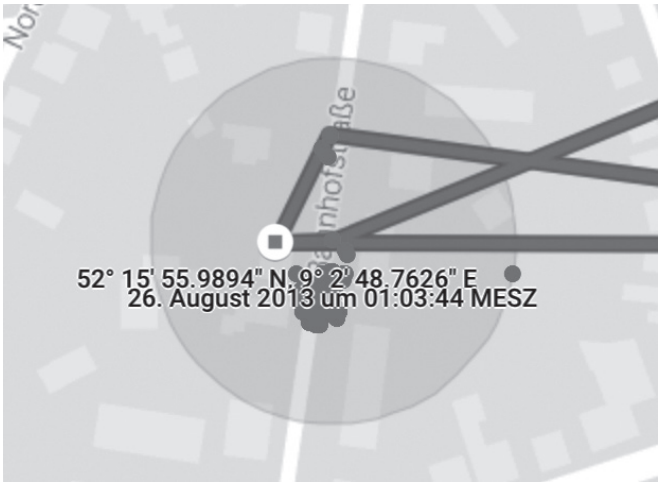


Abbildung 1: Bildschirmaufnahme des von Google gespeicherten Standortverlaufes

Es ist deswegen im vollsten Interesse des Nutzers, diesen Dienst abschalten und bearbeiten zu können. Auch ist ein besonderes Augenmerk auf Sprach- und Audioaktivitäten in Verbindung mit Google-Diensten zu legen. Googles Sprachsuche ist ein Dienst, der auf den meisten Smartphones mit dem Android-Betriebssystem vorinstalliert und aktiviert ist. Dieser ermöglicht dem Nutzer bereits durch einfaches Aussprechen der Phrase „Okay, Google“ mit dem Telefon zu interagieren. Alle sprachlichen Interaktionen

werden dabei aufgezeichnet und auf Googles Servern gespeichert. Diese können vom Nutzer jedoch eingesehen und selektiv oder gar vollständig gelöscht werden. Auch eine Auswahl der Angaben zur Person kann geändert und entfernt werden. Davon ausgeschlossen sind zum Beispiel der Name und das Geburtsdatum. Diese Informationen können zwar bearbeitet, aber nicht entfernt werden. Letztlich bietet Google die Möglichkeit, alle Daten, die mit dem Konto verknüpft sind, herunterzuladen oder über den Cloudspeicherdienst Google Drive online zu speichern. Die zuvor beschriebenen Daten im Rahmen der Sprach- und Audioaktivitäten werden dabei nicht mit ausgeliefert. Jedoch umfasst diese Sammlung unter anderem alle Nachrichtenverläufe aus Googles E-Mail-Dienst Gmail und Nachrichtendienst Hangouts. Letztere werden beispielsweise im JSON-Format bereitgestellt und enthalten die Nachrichteninhalte unverschlüsselt in einfachem Text. Googles Direktor für Strafverfolgung und Informationssicherheit Richard Salgado erklärte im Mai 2015, dass Hangouts-Nachrichten während der Übertragung verschlüsselt werden.[8] Jedoch hat Google nach der Übertragung auf deren Server vollen Zugriff (ebd.). Dadurch war das Unternehmen in der Lage, Wiretapping-Anordnungen nachzukommen. Das bedeutet, dass Google Nachrichten, welche über die Server des Unternehmens versendet wurden, an Justizbehörden übergeben hat. Auch das wird in Googles Transparenzbericht angegeben.[9] Diese Schwachstelle der Verschlüsselung erlaubt es Google, dem Nutzer Nachrichtenverläufe in reinem Text zur Archivierung zu übermitteln. Andere Unternehmen verwenden die sogenannte *End-to-End Encryption* (Ende-zu-Ende-Verschlüsselung), bei der die Nachrichten beim Sender verschlüsselt und erst beim Empfänger entschlüsselt werden. Da es auf dem Server nicht zu einer Entschlüsselung kommt, würde diese Art der Übertragung die Daten des Nutzers besser schützen. In diesem Fall können ihm Nachrichtenverläufe nicht zur Sammlung seiner Daten beigefügt werden. Ebenso wenig kann es dann aber dazu kommen, dass Nachrichten eventuell an Dritte übermittelt werden, was im Interesse des Datenschutzes ist.

3. Googles Rechte an den Daten der Nutzer

Urheberrecht des Nutzers

Möchte ein Nutzer Daten über Googles Dienste im Internet verfügbar machen oder online abspeichern, so geht dies oft nicht ohne das Anlegen eines Google-Kontos. Dies erfordert die ausdrückliche Einwilligung des Nutzers zu Googles Datenschutzerklärung und Nutzungsbedingungen. Damit willigt der Nutzer ein, dass Google die Daten, welche dem Unternehmen mitgeteilten wurden, verwenden darf. Insbesondere wird im Abschnitt „Wie wir die von uns erhobenen Informationen nutzen" beschrieben, dass der Profilname des Nutzers sowie das Profilbild eventuell in Anzeigen und anderen kommerziellen Kontexten verwendet werden. Da das Profilbild vom Nutzer gewählt und hochgeladen wurde, ist dabei nicht ausgeschlossen, dass er selbst Urheber dieses Bildes ist. Nach § 7 des Urheberrechtsgesetzes (UrhG) ist Urheber, wer Schöpfer eines Werkes ist. Laut § 2 Abs. 1 UrhG ist ein solches Werk unter anderem ein durch das Urheberrecht geschütztes Werk, wenn es sich um ein Lichtbildwerk beziehungsweise ein Werk handelt, das ähnlich wie ein Lichtbildwerk geschaffen wurde. Davon sind auch digitale Fotografien eingeschlossen, solange ein gewisses Maß an Individualität erkennbar ist, womit durchgesetzt werden soll, dass Zufallsfotografien vom urheberrechtlichen Schutz ausgenommen werden.[10] Diese Individualität ist gegeben, wenn das Bild eine Aussage enthält, die auf einer Gestaltung beruht, wozu beispielsweise die Wahl des Bildausschnitts oder die Platzierung des Motivs gehören (ebd.). Demzufolge ist es für einen Nutzer einfach, Urheber eines Fotos zu sein, welches vom Urheberrechtsgesetz geschützt ist und dieses als Profilbild seines Google-Kontos zu verwenden.

Einräumung von Nutzungsrechten

Zunächst sollte betrachtet werden, welche Aussagen Google in den Nutzungsbedingungen zu den Rechten an den Daten der Nutzer trifft. Zu beachten ist, dass es zwei deutsche Nutzungsbedingungen gibt, wobei eine von beiden explizit an Deutschland gerichtet ist[6] und sich von den allgemeinen Nutzungsbedingungen[11] an einigen Stellen unterscheidet. Im Folgenden wird die explizit für Deutschland ausgelegte Nutzungsbedingung betrachtet. Googles Standpunkt zum Urheberrecht der Daten des Nutzers wird darin unter dem Punkt „Ihre Inhalte in unseren Diensten" deutlich beschrieben: „Sie behalten Ihre Rechte als Urheber und alle bestehenden gewerblichen Schutzrechte an den Inhalten, die Sie in unsere Dienste einstellen. Kurz gesagt: Was Ihnen gehört, bleibt auch Ihres."[6] Direkt im Anschluss wird jedoch erklärt, dass Google und dessen Partnern unentgeltlich die notwendigen, *nicht ausschließlichen*, weltweiten und zeitlich unbegrenzten Rechte eingeräumt werden, die vom Nutzer eingestellten Daten zu nutzen. Allerdings geschieht dies nur im nötigen Umfang, um den vom Nutzer verwendeten Dienst auszuführen (ebd.). Nach § 31 UrhG kann der Urheber, in diesem Fall der Nutzer, einem anderen das Recht einräumen, ein Werk zu nutzen. Dies bezeichnet man als die „Einräumung von Nutzungsrechten". Dabei wird zwischen dem *nicht ausschließlichen* (einfachen) und dem ausschließlichen Nutzungsrecht unterschieden. Der Unterschied besteht darin, dass beim einfachen Nutzungsrecht die Nutzung der Daten durch andere nicht ausgeschlossen wird. Demzufolge ist es für einen Nutzer, der seine Werke zu kommerziellen Zwecken verwenden möchte, wichtig, dass Google nicht das ausschließliche Nutzungsrecht übertragen wird. Unmissverständlich wird in den Nutzungsbedingungen überdies klargestellt, dass der Nutzer die Nutzungsrechte unentgeltlich einräumt. Darum kann Google die Daten verwenden, ohne die Nutzer dafür bezahlen zu müssen. Es stellt sich nun die Frage, wozu das Unternehmen die Nutzungsrechte tatsächlich verwendet.

Um Inhalte von Nutzern online speichern oder anzeigen zu können, muss Google diese auf Servern hosten. Darum wird in den Nutzungsbedingungen erklärt, dass das an Google eingeräumte Nutzungsrecht das Recht umfasst, Inhalte technisch zu vervielfältigen (§ 16 UrhG). Dies kann einige informationstechnische Hintergründe haben, wie zum Beispiel die Vermeidung von Datenverlust durch Backups. Des Weiteren erhält Google das in § 19a UrhG definierte Recht der öffentlichen Zugänglichmachung der Inhalte des Nutzers, jedoch ausschließlich für den Fall, dass der Nutzer dies aufgrund der Natur des Dienstes beabsichtigt. So liegt es beispielsweise in der Natur des Dienstes YouTube, Videos der Öffentlichkeit zur Verfügung zu stellen. Die dort vom Nutzer hochgeladenen Videos sind zunächst auch ur-

heberrechtlich geschützt und Google benötigt das Recht der öffentlichen Zugänglichmachung, um das Video auf der Plattform öffentlich darstellen zu können. In diesem Fall ist im Interesse des Nutzers, dass Google das urheberrechtlich geschützte Material online präsentiert. Für den Nutzer ist dabei relevant, dass das Recht der öffentlichen Zugänglichmachung endet, sobald er die Daten aus dem jeweiligen Dienst entfernt, sodass er stets die Möglichkeit hat, die Einräumung dieses Rechts zu widerrufen.

Öffentliche Zugänglichmachung in der Natur eines Dienstes

Das vom Nutzer eingestellte Profilbild wird nach Googles Angaben möglicherweise in Anzeigen oder anderen kommerziellen Kontexten verwendet. Dieses (mit dem Google-Konto verknüpfte) Bild wird jedoch nicht nur in einem bestimmten Dienst dargestellt, sondern in allen Diensten, die auf das Google-Konto zugreifen. Es stellt sich also die Frage, ob die öffentliche Zugänglichmachung des Profilbildes in der Natur des Google-Kontos liegt, welches keinem einzelnen Dienst per se zugeordnet werden kann. Einerseits spricht dafür, dass viele von Googles Diensten dazu gedacht sind, Inhalte für andere Nutzer verfügbar zu machen. Darunter zählt zum Beispiel Googles Journal-Dienst *Blogger,* bei dem Nutzer Inhalte oft in einer Kombination aus Text und Bild veröffentlichen. Auch können beispielsweise auf YouTube Videos hochgeladen werden, wodurch Nutzer sich sogar Karrieren aufbauen.[12] Solchen Nutzern ist es natürlich sehr wichtig, im Internet Wiedererkennungswert zu erlangen, sodass Profilname und Profilbild des Google-Kontos durchaus zur öffentlichen Zugänglichmachung eingestellt werden, um diesen Effekt zu verstärken. Ebenso benutzen berühmte Personen und Unternehmen YouTube und andere Google-Dienste, wie zum Beispiel das soziale Netzwerk Google+, um im Internet präsent zu sein. Auch dabei werden Profilname und Profilbild bewusst zur öffentlichen Präsentation hochgeladen. Andererseits gibt es auch einige Dienste, die das Anlegen eines Google-Kontos erfordern, in deren Natur es jedoch nicht ausschließlich liegt, Inhalte öffentlich zugänglich zu machen. Dazu zählt zum Beispiel Googles Cloudspeicherdienst Google Drive. Dort können Daten jeglicher Art online gespeichert werden. Nutzer profitieren davon dadurch, dass sie von jedem Computer mit Internetzugang auf ihre Daten zugreifen können und damit auch ein Backup hinterlegen, für den Fall, dass lokale Daten verloren gehen. Zusätzlich bietet der Dienst die Möglichkeit, die hochgeladenen Inhalte mit anderen Nutzern zu teilen. Demzufolge entscheidet die Art und Weise, wie der Nutzer den Dienst verwendet, darüber, ob es in dessen Natur liegt, Daten öffentlich zugänglich zu machen. Auch die Verwendung von Googles E-Mail-Dienst Gmail ist ohne Anlegen eines Google-Kontos nicht möglich. Natürlich liegt es in der Natur eines E-Mail-Dienstes, Inhalte eines Nutzers mit anderen Nutzern zu teilen, jedoch ist dies stark abzugrenzen von öffentlicher Zugänglichmachung. So werden häufig E-Mails als Übertragungsmedium zwischen einer Auswahl von Personen verwendet, welche auch private Informationen enthalten und somit nicht für die Öffentlichkeit bestimmt sind. Auch ist es dabei häufig nicht im Interesse eines Nutzers, sein Profilbild im E-Mail-Verkehr zu verwenden. Da Google-Dienste also auch ohne die Absicht genutzt werden können, irgendwelche Daten, einschließlich des Profilbildes, öffentlich zugänglich zu machen, ist es für Nutzer keine Pflicht, ein Profilbild einzustellen. Wenn sich ein Nutzer jedoch dazu entscheidet, seinem Profil ein solches Bild zuzuordnen, dann ist dessen Zweck eindeutig die öffentliche Assoziation des Bildes mit dem Google-Konto und die öffentliche Zugänglichmachung damit beabsichtigt. Damit erhält Google dieses Nutzungsrecht, ohne das es das Profilbild eines Nutzers nirgends im Internet anzeigen dürfte. Dadurch ist es dem Unternehmen jedoch auch gestattet, das Bild unter anderem in Anzeigen oder kommerziellen Kontexten zu verwenden.

Kommerzielle Nutzung personenbezogener Inhalte

Nach Anlegen eines Google-Kontos werden sämtliche Aktivitäten, die der Nutzer in den verschiedenen Diensten ausübt, mit dem Konto verknüpft. Dazu gehören beispielsweise Handlungen wie das Hochladen oder Kommentieren eines YouTube-Videos oder das Veröffentlichen von Fotos auf Google Maps. Eine weitere Handlung, die mit dem Konto verknüpft wird, ist das Verfassen einer Bewertung. Dazu zählen beispielsweise *Daumen hoch*, als positive Wertung eines YouTube-Videos, oder *+1* zum Bewerten eines Beitrags auf Google+. Ein Nutzer kann jedoch auch Bewertungen für Produkte und Dienstleistungen jeglicher Art abgeben, die über Googles Dienste angeboten werden. Dazu gehören beispielsweise Restaurants und andere Etablissements, die auf Googles Kartendienst *Google Maps* angezeigt werden. Auch gilt dies für Produkte, die das Unternehmen in der Google Suche als Empfehlungen präsentiert. So werden zum Beispiel bei der Suche nach dem Begriff „Kino“ zunächst aktuelle Kinofilme sowie Kinos in der Nähe des Nutzers angezeigt. Diese Anzeigen enthalten Bewertungen anderer Nutzer, welche „Soziale Empfehlungen“ genannt werden und auch vom Nutzer selbst erstellt werden können. Sofern vorhanden, werden dabei folglich das urheberrechtlich geschützte Profilbild eines Nutzers sowie möglicherweise dessen Name in einem kommerziellen Kontext verwendet (Abbildung 2).

Abbildung 2: Bildschirmaufnahme der von Google angezeigten Kommentare in kommerziellen Kontexten

Durch die ausdrückliche Einwilligung der Nutzer zu Googles Datenschutzbestimmungen und Nutzungsbedingungen wurden Google die dafür notwendigen und vor allem nicht ausschließlichen Nutzungsrechte unentgeltlich eingeräumt. Demzufolge verliert der Nutzer die Rechte an seinen Daten nicht, und Google muss ihn für die Verwendung dieser auch nicht entschädigen. Dies ist jedoch nur möglich, solange der Nutzer diese Inhalte nicht wieder entfernt, denn damit endet das Recht der öffentlichen Zugänglichmachung. Des Weiteren hat der Nutzer die Option, „Soziale Empfehlungen" abzuschalten, sodass sein Profilname, Profilbild und seine Aktivitäten nicht in Werbeanzeigen erscheinen.

Googles Rechte an anderen Nutzerdaten

Zunächst sollte betont werden, dass Google nur Angaben darüber macht, Profilname, Profilbild und Aktivitäten, wie Bewertungen und Kommentierungen in Anzeigen oder anderen kommerziellen Kontexten zu verwenden. Zu anderen Inhalten, die ein Nutzer in einem Google-Dienst verfügbar machen kann, werden diesbezüglich keine Aussagen getroffen. Klar ist jedoch, dass der Nutzer beim Anlegen eines Google-Kontos die ausdrückliche Einwilligung zu den Datenschutzbestimmungen und Nutzungsbedingungen erteilt. Damit räumt er dem Unternehmen „unentgeltlich die notwendigen, nicht ausschließlichen, weltweiten und zeitlich unbegrenzten Rechte ein, diese Inhalte ausschließlich zum Zweck der Erbringung des jeweiligen Dienstes und lediglich in dem dafür nötigen Umfang zu nutzen"[6]. Anschließend wird beschrieben, dass diese Nutzungsrechte insbesondere die Rechte zur Vervielfältigung (§ 16 UrhG) und der öffentlichen Zugänglichmachung (§ 19a UrhG) umfassen. Später wird jedoch hinzugefügt, dass „bestimmte Dienste [...] zusätzlichen Bedingungen unterliegen [können], welche die Einräumung weiterer Rechte vorsehen"[6]. Demzufolge handelt es sich hierbei nach § 31a UrhG um einen Vertrag über unbekannte Nutzungsarten, da man einwilligt, eventuell weitere Rechte einzuräumen, die im Moment noch unbekannt sind. In § 31a UrhG wird beschrieben, dass der Urheber in diesem Fall ein Widerrufsrecht hat. Dieses ist drei Monate, nachdem ihm die Beabsichtigung über die Aufnahme neuer Nutzungsarten mitgeteilt wurde, gültig. Dies impliziert folglich, dass Google den Nutzer informieren muss, sobald weitere Rechte eingeräumt werden müssen und dieser die Möglichkeit hat, die abgegebenen Nutzungsrechte zu widerrufen. Nach § 32c UrhG hat der Urheber dann Anspruch auf eine angemessene Vergütung, falls eine neue Art der Nutzung nach § 31a UrhG aufgenommen wird. Wenn Google sich demnach entschließt, die Inhalte eines Nutzers zu kommerziellen Zwecken zu verwenden, muss der Nutzer darüber informiert werden. Dieser hat dann einen Anspruch auf Vergütung. Zum aktuellen Zeitpunkt macht Google dazu jedoch eine eindeutige Aussage: „Wir verkaufen keine persönlichen Daten."[13] An dieser Stelle wird anschließend erklärt, wie Google die Informationen über Nutzer einsetzt, um diesen möglichst genau zugeschnittene Werbung zu präsentieren, ohne Werbetreibenden die Identität der Nutzer preiszugeben. Auch wenn Inhalte der Nutzer verwendet werden, um diesen möglichst personalisierte Werbung anbieten zu können, so werden diese Nutzerdaten von Google nicht in Anzeigen und kommerziellen Inhalten benutzt.

4. Empfehlungen

Google sammelt viele Informationen über die Nutzer seiner Dienste. Selbst wenn man kein Google-Konto hat, sollte man die Cookie-Einstellungen seines Browsers überprüfen, um besser zu steuern, welche Daten erhoben werden können. Ist man im Besitz eines solchen Kontos, ist es umso wichtiger, seine Privatsphäre-Einstellungen zu überprüfen und gegebenenfalls anzupassen. Schließlich ist es im Interesse des Nutzers, seine Daten zu schützen.[14]

Referenzen

(letzter Abruf am 13.03.2017)

1 *https://www.forbes.com/powerful-brands/list/#tab:rank*
2 *https://techcrunch.com/2016/02/01/gmail-now-has-more-than-1b-monthly-active-users/*
3 *https://www.google.de/intl/de/policies/privacy/*
4 *https://www.google.de/intl/de/policies/technologies/types/*
5 *https://www.procado.de/datenschutz-lexikon/928/Einwilligung,%20konkludente.html*
6 *http://www.google.de/policies/terms/regional.html*
7 *https://www.grundrechteschutz.de/gg/recht-auf-informationelle-selbstbestimmung-272*
8 *https://www.reddit.com/r/IAmA/comments/35b6bt/we_are_senior_members_of_googles_public_policy/*
9 *https://www.google.com/transparencyreport/userdatarequests/*
10 *https://www.rechtambild.de/2010/02/bin-ich-urheber-meines-bildes/*
11 *https://www.google.com/policies/terms/*
12 *http://variety.com/2015/digital/news/pewdiepie-youtube-top-earner-12-million-1201619802/*
13 *https://privacy.google.com/how-ads-work.html*
14 *https://myaccount.google.com/privacy*

Maximilian Katzmann

Maximilian Katzmann ist Doktorand am Hasso-Plattner-Institut für Digital Engineering in Potsdam. Seine Forschung im Bereich der theoretischen Informatik befasst sich vor allem mit dem Zusammenhang zwischen skalenfreien Netzwerken und der hyperbolischen Geometrie.

Maike Küper

Der Wert unserer Daten

Jeden Tag stellen wir Unternehmen und anderen Institutionen unsere Daten zur Verfügung – unbewusst oder bewusst, freiwillig oder unfreiwillig. Wir nutzen Google, Facebook oder alle möglichen Smartphone-Apps, die oft für ihre Dienste keinen monetären Preis verlangen, gleichzeitig aber zu den wertvollsten Unternehmen der Welt gehören. Die CEO von IBM, Ginni Rometty, ist nur eine derjenigen, die prophezeit: „Big Data is the world's natural resource for the next century."[1] Dass Daten eine wertvolle Ressource sind, scheint also unstrittig. Diese Feststellung hat jedoch bedeutende Konsequenzen. Wenn Daten ein so wertvolles Gut sind, stellt sich die Frage nach dem Warum.

Warum ist es für alle möglichen Stakeholder so interessant und lukrativ, unsere persönlichen Daten zu kennen? Insbesondere bei Unternehmen liegt ökonomisches Kalkül nahe, sodass sich im Weiteren die Frage stellt, wie diese mit persönlichen Daten Geld verdienen können. Die Frage lautet also: Was sind unsere Daten wert? Lässt sich monetär beziffern, was Google daran verdient, dass es unsere Suchaufträge nachverfolgt, oder Facebook daran, dass es unsere Lieblingsserie und die Namen unserer Haustiere kennt?

Diese Frage in Ansätzen zu beantworten und dabei auch die Konsequenzen dieses Datenmarkts zu beleuchten, ist Ziel dieses Artikels. Dabei soll vernachlässigt werden, welche unterschiedlichen Geschäftsmodelle dazu genutzt werden, Umsätze zu generieren; das Ergebnis und die Implikationen des Datenwerts für Anbieter und Nachfrager soll im Vordergrund stehen. Ein Motivationsgrund für diesen Artikel war, dass verschiedenste Unternehmen und Dienste daran beteiligt sind, unsere Daten zu sammeln, zu verarbeiten und auszuwerten. Wie genau dies vonstattengeht, ist jedoch den wenigsten Nutzern bekannt. Daher möchte dieser Artikel auch einen Beitrag dazu leisten, die Anreize und Funktionsweisen der Datensammler darzustellen, damit die Nutzer den Wert ihrer Daten realisieren und bewusst mit dieser Ressource umgehen können.

Versuch einer Begriffsbestimmung

Drei Definitionen sollen zunächst dazu dienen, in den Kontext der Untersuchung einzuführen und Begriffsungenauigkeiten zu klären. Der Trend-Begriff im Zusammenhang mit der zunehmenden Sammlung und Auswertung von Daten ist *Big Data*. Eine Definition der National Science Foundation beschreibt diesen Begriff wie folgt: „The phrase 'big data' […] refers to large, diverse, complex, longitudinal, and/or distributed data sets generated from instruments, sensors, Internet transactions, email, video, click streams, and/or all other digital sources available today and in the future."[2] Sonka und Cheng nähern sich dem Begriff weniger über die technische Seite und sehen Big Data vor allem vor dem Hintergrund der Datenanalyse eher als eine Fähigkeit an: „Big Data is a capability. It is the capability to extract information and craft insights where previously it was not possible to do so."[3]

Daten an sich werden definiert als „a reinterpretable representation of information in a formalized manner, suitable for communication, interpretation, or processing"[4]. Sie sind also keine Informationen, nur deren formale Darstellung. Informationen hingegen entstehen erst durch eine Bedeutung, beispielsweise dass die Zeichen „38°" eine (hohe) Temperatur beschreiben (vgl. z. B. Herrmann[5] hinsichtlich der „Wissenspyramide" aus Zeichen, Daten, Informationen und Wissen).

In diesem Artikel soll es vor allem um persönliche Daten gehen. *Personenbezogene Daten* werden in Art. 4 der seit 25. Mai 2016 geltenden Europäischen Datenschutz-Grundverordnung (EU-DSGVO) definiert als

> *alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person […] beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.*[6]

Der Wert der Daten: Zwei Analogien

Um dem Wert der Daten für Individuen und Unternehmen näher zu kommen, werden zunächst zwei Analogien vorgestellt, die häufig zur Veranschaulichung des Werts – auch im Sinne der Funktionen, Potenziale und Wichtigkeit – von (persönlichen) Daten genutzt werden, gleichzeitig aber auch die Schwierigkeiten bei der Wertbestimmung offenbaren.

Daten als Zahlungsmittel

Die erste Analogie ist die der *Daten als Währung des digitalen Zeitalters*[7]. Zwar ist dies vielen Nutzern nicht bewusst, doch sind Daten im Internet oftmals das Zahlungsmittel für alle möglichen Dienste. Eine vielzitierte Aussage lautet: „If you're not paying for something, you're not the customer; you're the product being sold."[8] Es gibt also keine kostenlose App, kein kostenlos soziales Netzwerk – wir bezahlen nur nicht mit Geld, sondern mit Informationen über uns. Daten sind weiterhin wie Geld „liquide", als digitales Gut können sie jederzeit überallhin transferiert werden und haben für zahllose Interessierte einen Wert[7]: Man denke beispielsweise an Informationen über den Gesundheitszustand, die sowohl für den einzelnen Menschen als auch für Krankenkassen, Arbeitgeber oder Fitnessgerätehersteller von Wert sein können.

Es gibt jedoch einige entscheidende Unterschiede zwischen Geld und Daten als Tauschmittel. Daten haben keinen festen ökonomischen Wert – wir wissen also nicht, wie viel wir wirklich

für eine App bezahlen, der wir Zugriff auf unsere Smartphone-Daten geben. Auch fehlen Wechselkurse oder eine feste Umlaufmenge von Daten, wie sie bei Geld vorliegen[9]. Teilweise ist die Eigentumsfrage auch nicht eindeutig zu beantworten; bei den Daten, die in Autos aufgezeichnet werden, ist zum Beispiel rechtlich noch nicht geklärt, wem sie gehören[10].

Darüber hinaus werden Daten in Kombination mit neuen Daten immer wertvoller, sodass deren Wert einerseits sehr volatil ist und andererseits für Unternehmen kein Anreiz zum Sparen besteht[9]. Im Gegenteil: Viele Daten werden auch gespeichert, ohne dass ein momentaner direkter Nutzen aus ihnen entsteht[11]. Diese „je mehr, desto besser"-Philosophie ist aus ökonomischer Sicht sinnvoll, aber ethisch und für das Individuum bedenklich[12]. Es ist also gut möglich, dass unsere Daten in Zukunft viel wertvoller werden als sie es momentan sind[13]. Mayer-Schönberger und Cukier kommen zu dem Schluss: „Letzten Endes besteht der Wert von Daten aus der Summe dessen, was aus allen vorstellbaren Nutzungen gewonnen werden kann."[11]

Was Daten aber vor allem von Geld unterscheidet, ist ihre Aussagekraft – die gegenwärtige, aber auch die potenzielle zukünftige Aussagekraft. Oder, wie Boie es formuliert:

> *Daten können keine Währung sein. […] Wer sie auf ihren monetären Wert reduziert, übersieht, was mit ihnen alles angestellt werden kann – und mit Geld nicht. Fünf Euro bleiben, egal in wessen Hand, fünf Euro. Die Tatsache, welches Kosmetik-Unternehmen ein Facebook-Nutzer mag, wann und wie er surft und mit wem er befreundet ist, lässt dagegen einen Teil seiner Persönlichkeit offenbar werden.*[14]

Zusammengefasst sind Daten folglich kein neutrales Zahlungsmittel, sondern, um die Analogie zu bedienen, ein Geldschein mit einem Teilfoto unserer Person – und bedenkt man die Leichtigkeit, mit der persönliche Daten oft an- bzw. abgegeben werden und die Intransparenz, was mit diesen Daten geschieht, resultiert daraus, dass wir nicht wissen, welche Unternehmen oder Institutionen wie viele Teilfotos unserer Person besitzen, was sie daraus für Erkenntnisse ziehen und wieviel Geld sie damit verdienen.

Rohstoff Daten: Das neue Öl?

Die zweite Metapher, die immer wieder verwendet wird, ist die der Daten als entscheidende Ressource dieses Jahrhunderts; dies postulierte Clive Humby zuerst 2006 in seiner Aussage „Data is the new oil"[15]. Laut Toonders sind Daten mit Öl zunächst deswegen vergleichbar, weil jene, die den Wert von Daten verstehen und sie weiterverarbeiten können, große Profite erwarten können[16]. Die nächste Parallele ist, dass Daten ebenso wie Öl als Rohstoff angesehen werden können; auch Bundeskanzlerin Angela Merkel verkündete dies[17]. Eine Art und Weise, Daten zu monetarisieren, ist in der Tat der direkte Verkauf dieses „Rohmaterials" an interessierte Parteien[18]. Das ist jedoch nicht das einzige Geschäftsmodell; für weitere Verwendungen gilt, was Palmer schreibt: „Data is just like crude. It's valuable, but if unrefined it cannot really be used. It has to be changed into gas, plastic, chemicals, etc [sic!] to create a valuable entity […]; so must data be broken down, analysed for it to have value."[15] Vor der Verarbeitung haben Daten also keinen wirklichen Wert; erst durch die Analyse und Weiterverarbeitung können sie diesen generieren. Durch die Weiterverarbeitung ergibt sich eine weitere Parallele zum Öl: Dieses brachte neue Materialien und Erfindungen hervor, ebenso wie nun durch Big Data eine Vielzahl neuer Möglichkeiten entsteht, von der Verbesserung medizinischer Diagnosen bis zur Stauvermeidung[19].

Die Analogie ist weiterhin passend, da Daten die entscheidende Ressource der heutigen Informationsgesellschaft sowie -wirtschaft sind, ebenso wie das Öl das industrielle Zeitalter ermöglichte[19]. Das lässt sich auch an der Entwicklung der Unternehmen ablesen, die mit Öl bzw. mit Daten Geld verdienen. Noch im Jahr 2009 führte Exxon Mobil mit 337 Mrd. Dollar die Liste der wertvollsten Unternehmen (nach Börsenwert) an[20]. 2015 stand Apple mit 725 Mrd. Dollar an der Spitze, Google folgt an zweiter Stelle[20]. In der Tat sind Apple und Google die Gewinner der letzten Jahre, mit einer Steigerung des Börsenwerts von 674 % bzw. 242 %[20]. Im Fall von Google ist dies angesichts der Tatsache, dass das Unternehmen erst 1998 gegründet wurde, besonders bemerkenswert. Diesem Aufstieg steht der Abstieg der Ölfirmen gegenüber: Petrochina Co. und Gazprom gehören bei der Betrachtung des Börsenwerts zu den größten Verlierern.[21]

Es gibt jedoch einige entscheidende Unterschiede zwischen Daten und Waren oder Rohstoffen wie Öl. Materialien wie Metalle und Öl können nur einmal verkauft werden – Daten dagegen können mit sehr geringem Aufwand vervielfältigt und ohne Wertverlust immer wieder benutzt werden[22]. Für unterschiedliche Nutzer oder Käufer der Daten kann deren Wert je nach Analyse und Weiterverwendung ferner unterschiedlich hoch ausfallen. Der Wert einer einzelnen Information steigt darüber hinaus, wie bereits angesprochen, durch die Kombination mit weiteren[22]: Für Versicherungen beispielsweise ist die körperliche Aktivität eines Versicherten in Kombination mit seinen Essgewohnheiten wertvoller als nur eine der beiden Informationen.

Goldhammer postuliert außerdem, dass Daten nicht alle ökonomischen Bedingungen erfüllen, um als Gut klassifiziert werden zu können, und verweist auf die problematische Nutzenbewertung[23]: Wie bereits erwähnt, ist es unmöglich, den genauen Wert bestimmter Informationen zu bestimmen. In diesem Kontext wird auch auf das Informationsparadoxon von Arrow verwiesen: „Ein Konsument kann den Wert einer Information nicht beurteilen, bevor er sie kennt. Kennt er sie aber, um sie zu beurteilen, muss er sie nicht mehr kaufen."[23]. Der tatsächliche Wert der persönlichen Informationen bzw. Daten, die wir beispielsweise an Facebook abgeben, kann im Vorhinein also nur näherungsweise bestimmt werden, z. B. über den erzielten Preis bei Werbetreibenden.

Die schwierige Einschätzung des Werts von Informationen und Daten hindert mit Daten handelnde Unternehmen wie Google und Facebook allerdings nicht daran, hohe Gewinne einzustreichen. Einige der Internetfirmen, die heute hohe Börsenwerte haben, sind außerdem erst seit kurzer Zeit am Markt. Twitter beispielsweise hat seit seiner Gründung noch keine schwarzen Zahlen geschrieben[24] – der Börsenwert liegt jedoch aktuell bei 13,6 Mrd. Dollar[25] (Stand: 14.5.2017). Herrlich erklärt diese hohen Bewertungen trotz fehlender Gewinne als die zukünftigen Erwartungen des Werts der gesammelten Daten und meint:

„Dass so hohe Wetten auf die steigende Monetarisierbarkeit von Daten aus sozialen Netzwerken abgeschlossen werden, ist nachvollziehbar."[26]

Es geht also nicht nur um die Gewinne, die die Unternehmen aktuell mit den Daten erzielen können – die Anleger scheinen damit zu rechnen, dass die Daten als Ressource noch wertvoller werden. Diese Vermutung haben auch Mayer-Schönberger und Cukier: „Nahezu jede Datensammlung, jedes Datenstück hat intrinsische, verborgene noch unentdeckte Nutzen und damit auch ökonomischen Wert, und das Rennen, all diese Datenschätze zu heben, ist in vollem Gange."[11] Im Zusammenhang mit dem steigenden Wert von Informationen in Kombination mit weiteren Informationen erscheint dies nachvollziehbar, da auch weiterhin viele Aktivitäten und Institutionen digitalisiert werden und so mit einem weiteren Anstieg der Datenmenge zu rechnen ist[27]. Zwar ergibt sich erneut – auch rein sprachlich gesehen – eine Ähnlichkeit zum Kampf um Rohstoffe, doch geht es hier nicht um endende, fossile Brennstoffe, sondern um ein Rohmaterial, das nicht zu versiegen droht oder teuer hergestellt werden muss.

Die monetäre Bewertung der Daten

Wenn nun Daten das Öl als wertvollsten Rohstoff abgelöst haben und die Unternehmen derartige Gewinne damit erzielen, stellt sich die Frage nach dem tatsächlichen monetären Wert, den wir mit unseren Daten an diese Unternehmen abgeben. Es folgen nun konkrete Beispiele, wie dieser Wert näherungsweise berechnet werden könnte.

Wert aus Unternehmens- und Nachfragesicht

Morey, Forbath und Schoop teilen die Funktionen von Daten für Unternehmen in drei Kategorien auf: Sie nutzen Daten, um (1) ein Produkt oder eine Dienstleistung zu verbessern, (2) gezielte Werbung zu platzieren oder (3) neue Umsätze durch den Verkauf von Daten zu erzielen.[18] Aus wirtschaftlicher Sicht entstehen so zwei Möglichkeiten, durch die Nutzung und Analyse von Daten den Gewinn zu steigern: zum einen durch Einsparungen, zum Beispiel weil Prozesse effizienter werden oder Produkte zielgerichteter angeboten werden können, zum anderen durch Zugewinne in neuen Geschäftssparten[22].

Ein Beispiel soll die Einsparmöglichkeiten durch die Nutzung personenbezogener Daten veranschaulichen. Versicherungen haben beispielsweise ein großes Interesse daran, möglichst viel über den Lebensstil ihrer Kunden zu erfahren, um die Wahrscheinlichkeiten von Erkrankungen oder Unfällen zu berechnen[28]. Ein Analyst von Deloitte postuliert: „I think I could better predict someone's risk of a heart attack based upon their Visa bill than their genome."[28] Wenn die Versicherungen, zum Beispiel mit gezielten Informationen, die sie aus deren Einkaufsverhalten ablesen, die Kunden über bestimmte Risiken aufklären und diese abschwächen, können sie Kosten einsparen[28].

In diesem Artikel sollen jedoch die Umsätze im Vordergrund stehen, die Unternehmen mithilfe der persönlichen Daten ihrer Kunden neu generieren. Dies soll am Beispiel von Facebook exemplarisch veranschaulicht werden. Kurz gesagt besteht das Hauptgeschäft von Facebook darin, anhand der persönlichen Daten des jeweiligen Nutzers auf ihn abgestimmte Werbung zu schalten, für die die Werbetreibenden bezahlen. Dabei gibt es zwei Möglichkeiten, um den Preis zu bestimmen: Ein Unternehmen zahlt entweder die Kosten pro Klick oder pro 1.000 Mal angezeigter Werbung[29]. In den USA zahlt ein Werbetreibender durchschnittlich 24 Dollar für 100 Klicks durch Nutzer oder um seine Anzeige 36.364 Mal anzeigen zu lassen[29]. Diese Preise unterscheiden sich jedoch stark, je nach Branche und Relevanz des beworbenen Produkts, Ortes, Unternehmens etc.[29]. Um ein „Like" zu erhalten, so die Rechnung, müssen Werbetreibendende im Schnitt 50 bis 80 (US-)Cent zahlen[29].

Diese Zahlen beziffern, was Unternehmen die Dienstleistung wert ist, die Facebook ihnen bietet, also gewissermaßen den indirekten Wert, den die persönlichen Daten generieren. Was aber ist der genaue Wert, den Facebook mit den Daten eines Nutzers verdient? Unter der oben zitierten Prämisse „If you're not paying for something, you're not the customer; you're the product being sold" – was ist der Rohstoff unserer persönlichen Daten wert?

Es gibt einige rechnerische Möglichkeiten, den Wert eines Nutzers zu beziffern. Die erste Möglichkeit ist, den Umsatz pro Nutzer zu berechnen. Im letzten Quartal des Jahres 2015 hatte Facebook 1,59 Mrd. aktive Nutzer, der Umsatz betrug 5,84 Mrd. Dollar[30]. Dies ergibt einen Umsatz von ca. 3,67 Dollar, den Facebook mit jedem Nutzer verdiente, davon 96,5 % durch Werbung[30]. Zum Vergleich: Google hatte 2,5 Mrd. registrierte Nutzer, der Umsatz betrug 74,54 Mrd. und es ergibt sich ein Umsatz pro Nutzer von 29,82 Dollar, davon 90,4 % durch Werbung[31]. Ferner lässt sich der Wert eines Nutzers berechnen, indem man den Börsenwert durch die Nutzerzahl teilt[32]. Dieser betrug im November 2015 bei Facebook 303,6 Mrd. Dollar[33]; geteilt wiederum durch die Nutzerzahl von 1,59 Mrd. ergibt sich ein Börsenwert pro Nutzer von 190,94 Dollar.

Unabhängig von Social-Media-Plattformen gibt es weitere Berechnungen dazu, welchen unmittelbaren Wert Daten für Unternehmen haben. Werbetreibende und sogenannte Datenbroker

Maike Küper

Maike Küper arbeitet als Unternehmensberaterin für die Detecon International GmbH. Dort ist sie zuständig für HR Innovation, Change Management und Design Thinking und begleitet internationale und nationale Kunden auf dem Weg in die Zukunft der Arbeit.

sind laut einer Studie bereit, umgerechnet ungefähr 0,05 (US-) Cent für das Wissen um Geschlecht, Alter und den Wohnort eines Menschen zu zahlen – das sind 50 Cent für 1000 Menschen[34]. Die Financial Times hat aus allen möglichen Daten, die über Menschen im Internet gesammelt werden, einen interaktiven Rechner erstellt (Abbildung 1), der nach der Eingabe z. B. des Alters oder von Berufs- oder Alltagsinformationen kalkuliert, was diese Informationen wert sind[34]; selten ergibt sich ein Wert von über einem Dollar.

Abbildung 1: Datenrechner[34], © Financial Times

Je spezifischer und persönlicher eine Information ist, desto wertvoller wird sie: Die Information, dass eine Frau im zweiten Trimester schwanger ist, ist beispielsweise 11 (US-)Cent wert, gesundheitliche Probleme oder die Notwendigkeit spezieller Medikamente 26 Cent.[35] Zugangsdaten erzielen etwas höhere Preise: Ein Netflix-Login bringt im „Dark Web" 55 Cent, Nutzername und Login für ein Bankkonto mit 2200 Dollar ganze 190 Dollar.[35]

Wert aus Nutzersicht

Nach einer Näherung an den Datenwert von Unternehmens- und Händlerseite, also gleichsam der Nachfrager, stellt sich nun die Frage, wie die Nutzer selbst bzw. die Anbieter den Wert ihrer persönlichen Daten einschätzen. Danach befragt, nennen sie als Schätzwert umgerechnet insgesamt 2.972 Euro[35]. Dabei schätzen Frauen den Wert ihrer Daten höher ein als Männer, und jüngere Menschen sind eher dazu bereit, ihre Daten abzugeben.[35] Die Menschen vermuten also, dass der Wert ihrer persönlichen Daten für Unternehmen recht hoch ist – zumindest wesentlich höher als der Wert, der bei den verschiedenen Berechnungsmöglichkeiten von Unternehmensseite pro Nutzer ermittelt wird. In einer Studie der TU Darmstadt werden geringere Werte genannt; nur 13,9 % der Befragten geben hier an, dass sie den Wert ihrer Daten auf über 1.000 Euro schätzen[36]. Über ein Viertel der Befragten können den Wert ihrer Daten nicht einschätzen[36]. Der Großteil glaubt zwar, sie seien mehr als 10 Euro wert – doch bedeutet dies umgekehrt nicht, dass sie bereit sind, einen hohen Betrag für den Schutz ihrer Daten zu bezahlen: Über 90 % der Befragten würden maximal 10 Euro für den Schutz ihrer persönlichen Daten ausgeben (Abbildung 2).[36]

Zu etwas höheren Werten kommt eine Studie des DIVSI, in der sich eine Zahlungsbereitschaft für den Schutz der persönlichen Daten von durchschnittlich 41 Euro ergibt[37]. Dies ist nicht nur ein Problem der fehlenden Sensibilisierung oder Einsicht: 59 % der Befragten sind auch deswegen nicht bereit, Geld zu zahlen, weil sie den Onlinediensten nicht trauen; sie bezweifeln, dass die Zahlungen tatsächlich zu sicheren Daten führen[37].

Morey, Forbath und Schoop fragten Personen in einem internationalen Vergleich ebenfalls nach dem Wert bestimmter Daten in Form der Zahlungsbereitschaft für deren Schutz, beispielsweise Kreditkarteninformationen, Standorte oder Online-Suchhistorien.[18] Es kam heraus, dass es starke nationale Unterschiede bezüglich der Wertschätzung von Daten gibt: US-Amerikaner beispielsweise sehen ihre Personalien als am wichtigsten an und würden 112 Dollar für deren Schutz bezahlen, Briten und Deutsche würden mit knapp 60 bzw. 184 Dollar vor allem ihre Krankengeschichte schützen.[18]

Die eher niedrigen Schätzwerte der Nutzer weisen darauf hin, dass vielen nicht bewusst ist, welche Gewinne Unternehmen mit ihren Daten erzielen können oder dass die Daten in Zukunft noch an Wert gewinnen können. Daten werden zuweilen in drei Arten aufgeteilt: „Volunteered data", das heißt Informationen, die bewusst eingegeben werden, wie Name und Wohnort in einem Online-Profil, „observed data", die beispielsweise durch das Verfolgen von Standorten oder IP-Adressen entstehen, und „inferred data", also das, was Unternehmen aus der Kombination der ersten beiden schließen können[38]. Da nur erstere bewusst vom Nutzer veröffentlicht werden und viele nicht wissen, dass auch ihre Suchhistorie, Standorte etc. übermittelt werden, schätzen diese demnach den Wert ihrer Daten als geringer ein.

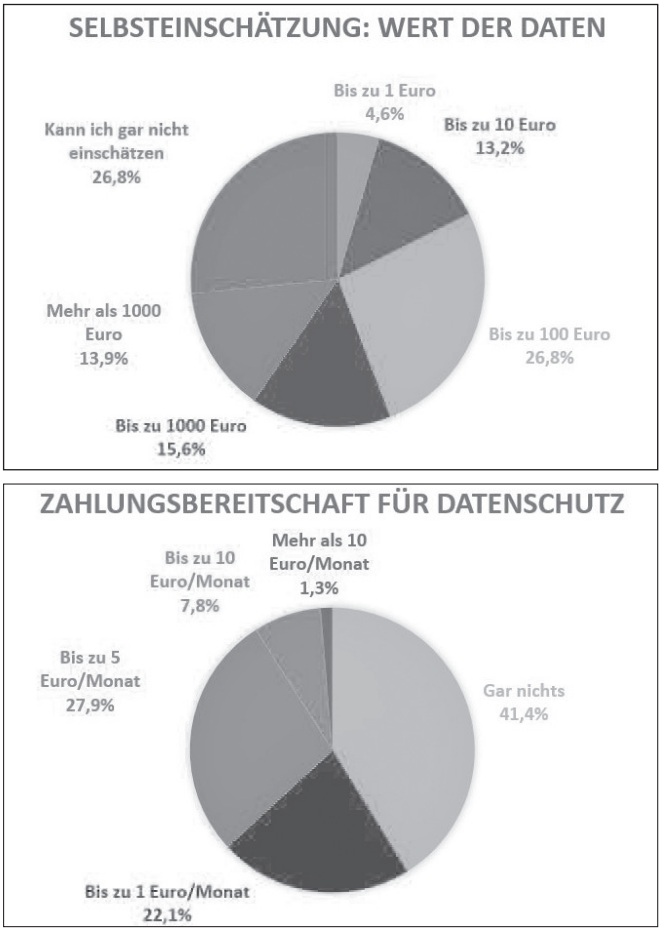


Abbildung 2: Einschätzung des Werts der eigenen persönlichen Daten (oben) und Zahlungsbereitschaft für deren Schutz (unten), nach Buxmann, Gerlach & Wenninger[36]

Insbesondere die letzte Art von Daten ist für die Nutzer sehr intransparent: Es ist nicht nachzuvollziehen, welche Daten gesammelt und aggregiert werden, und daher ebenso wenig transparent, welche Schlüsse daraus gezogen werden können. So geben auch 96 % der Befragten an, dass Unternehmen in dieser Hinsicht mehr Informationen offenlegen sollten[37]. Das zentrale Problem bei der Wertschätzung der persönlichen Daten ist also die Unwissenheit darüber, was mit den Daten geschieht und welchen Wert Unternehmen mit ihnen generieren können.

Fazit: Konsequenzen der problematischen Wertschätzung von Daten

Der Wert der Daten ist also weder aus Anbieter- noch aus Nachfragesicht eindeutig zu beziffern. Zwar schätzen Individuen den Wert wesentlich höher ein, doch sind sie sich nicht sicher, welche Aussagekraft ihre aggregierten Daten haben. Gleichzeitig werden Unternehmen, die große Mengen von Daten speichern und verarbeiten, sehr hoch bewertet – auch weil anzunehmen ist, dass ihre gesammelten „Rohstoffe" in der Zukunft noch wertvoller sein werden. Zwar gibt es durchaus Überlegungen, wie ein „Datenmarkt" mit Bewertungen funktionieren könnte, beispielsweise mit Lizenzmodellen.[11] Aufgrund der ungeklärten Potenziale und der großen Intransparenz im Datengeschäft ziehen Cooper, LaSalle und Wei aber den Schluss: „Anders als die Geldwirtschaft ist der Markt für persönliche Daten noch lange nicht ausgereift."[7] Dies hat auch damit zu tun, dass es augenscheinlich noch kein allgemeines Wissen ist, dass Daten in vielen Fällen als geldwertes Gut gehandelt werden. Čas und Peissl bezeichnen es als das zentrale Problem,

> *dass für die einen personenbezogene Daten einen monetär bewertbaren Produktionsfaktor darstellen, während sie für andere Marktteilnehmer einen immateriellen Wert – ein Recht symbolisieren […] Es lässt sich kaum ein Preis festlegen, wenn einer der Marktpartner gar nicht in ökonomischen Größen denkt.*[22]

Hinzu kommt, dass der Markt für Daten von großer Intransparenz und Asymmetrie bestimmt wird[22]. Die unterschiedlichen Schätzungen des Wertes der eigenen Daten zeigen, dass Unsicherheit herrscht, was dieses Zahlungsmittel angeht. Die Menge an Daten und die Verarbeitungs- und Anwendungsmöglichkeiten steigen stetig an, sodass es für den individuellen Nutzer immer schwieriger wird, den Weg seiner Daten nachzuvollziehen[22].

Näherungsweise Berechnungen des Werts der persönlichen Daten können dabei helfen, zunächst das Bewusstsein dafür zu schärfen, dass diese Daten einen monetären Wert haben und welche Konsequenzen diese „Zahlungsweise" hat. Denn die Intransparenz und Unsicherheit gelten ebenso für die Risiken, die mit der Abgabe der Daten einhergehen. Hirsch führt in diesem Kontext die Analogie der Daten als Öl weiter und verweist so auf die Risiken: „If data is the new oil, then these data releases are the new oil spills. […] Just like oil spills, data spills cause a variety of different types of damages."[19] Der EU-Politiker Jan Philipp Albrecht schlussfolgert daraus weiter: „Wenn Daten das neue Öl sind, ist Datenschutz der neue Umweltschutz."[39] Der Datenschutz wiederum beginnt beim Nutzer: Ohne das Wissen, dass Unternehmen mit seinen persönlichen Daten auf mannigfaltige Art und Weise Geld verdienen und ohne das Wissen, was mit seinen Daten geschieht, kann er sich weder empören noch zur Wehr setzen. Aufklärung und ein gewisses technisches Verständnis sind daher laut Kurz und Rieger der erste Schritt zu einer „digitalen Mündigkeit", die sie als unbedingt notwendig erachten[13]. Schlussendlich bleibt auch zu bedenken, dass Big Data großartige Vorteile in allen möglichen Lebensbereichen bietet – doch darf das Recht auf Privatsphäre dabei nicht ungehindert auf der Strecke bleiben.

Referenzen

1 Akhtar O (2014) "Big Data is the world's natural resource for the next century" – IBM CEO Ginni Rometty. DMN, *14.5.2014,* http://www.dmnews.com/marketing-strategy/big-data-is-the-worlds-natural-resource-for-the-next-century--ibm-ceo-ginni-rometty/article/346991/

2 *National Science Foundation (2012) Core techniques and technologies for advancing Big Data science & engineering. Program solicitation NSF 12-499,* http://www.nsf.gov/pubs/2012/nsf12499/nsf12499.htm

3 *Sonka S, Cheng Y-T (2015) Big Data: more than a lot of numbers! farmdoc daily 5(201), Univ. of Illinois at Urbana-Champaign, Dept. of Agricultural and Consumer Economics, 29.10.2015,* http://farmdocdaily.illinois.edu/2015/10/big-data-more-than-a-lot-of-numbers.html

4 *The Consultative Committee for Space Data Systems (2012) Reference model for an open archival information system (OAIS). Recommended practice CCSDS 650.0-M-2, Washington, DC, Juni 2012,* http://public.ccsds.org/publications/archive/650x0m2.pdf

5 *Herrmann R (2012) Wissenspyramide. Der WINF, 12.9.2012,* https://derwirtschaftsinformatiker.de/2012/09/12/it-management/wissenspyramide-wiki/

6 *Europäische Union (2016) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). ABl. L 119, 4.5.2016,* http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=OJ:L:2016:119:TOC

7 *Cooper T, LaSalle R, Wei K (2015) Daten sind wie Geld. Harvard Business Manager, 2015(6):10f.* http://www.harvardbusinessmanager.de/heft/d-134876707.html

8 *Woher das Zitat stammt, ist nicht eindeutig zu klären – meist wird es Andrew Lewis zugeschrieben, der es 2010 im Blog MetaFilter veröffentlichte,* http://www.metafilter.com/95152/Userdriven-discontent#3256046

9 *Kempf D (2015) Sind Daten die Währung von morgen? Bitkom, 4.3.2015,* https://www.bitkom.org/Presse/Blog/Sind-Daten-die-Waehrung-von-morgen.html

10 *Maak N (2014) Angriff aufs Auto. Frankfurter Allgemeine Zeitung, 1.2.2014,* http://www.faz.net/aktuell/feuilleton/der-glaeserne-fahrer-angriff-aufs-auto-12779186.html

11 *Mayer-Schönberger V, Cukier K (2013) Big Data: die Revolution, die unser Leben verändern wird. Redline-Verlag, München*

12 *Rooney Martin E (2014): The ethics of Big Data. Forbes, 27.3.2014,* http://www.forbes.com/sites/emc/2014/03/27/the-ethics-of-big-data/#5f3c519d30c7

13 *Kurz C, Rieger F (2011) Der Informationstreibstoff von Google & Co. Zeit Online, 12.4.2011,* http://www.zeit.de/digital/datenschutz/2011-04/datenfresser-kurz-rieger/komplettansicht

14 *Boie J (2013) Ein Knopf zur Selbstauskunft bei Facebook, Twitter und Co. Süddeutsche Zeitung, 12.3.2013, http://www.sueddeutsche.de/digital/persoenliche-daten-im-internet-ein-knopf-zur-selbstauskunft-bei-facebook-twitter-und-co-1.1622692*

15 *Palmer M (2006) Data is the new oil. Association of National Advertisers, 3.11.2006, http://ana.blogs.com/maestros/2006/11/data_is_the_new.html*

16 *Toonders J (2014) Data is the new oil of the digital economy. Wired, 23.7.2014, http://www.wired.com/insights/2014/07/data-new-oil-digital-economy/*

17 *Kannenberg A (2015) Merkel: Daten sind Rohstoffe des 21. Jahrhunderts. Heise Online, 2.11.2015, http://www.heise.de/newsticker/meldung/Merkel-Daten-sind-Rohstoffe-des-21-Jahrhunderts-2867735.html*

18 *Morey T, Forbath T, Schoop A (2015) Customer data: Designing for transparency and trust. Harvard Business Review 2015(5), https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust*

19 *Hirsch DD (2014) The glass house effect: Big Data, the new oil and the power of analogy. Maine Law Review 66(2):373–395, http://www.mainelawreview.org/wp-content/uploads/2014/06/02-Hirsch.pdf*

20 *PriceWaterhouseCoopers (2015): Global top 100 companies by market capitalisation – 31 March 2015 update. http://www.pwc.com/gx/en/audit-services/capital-market/publications/assets/document/pwc-global-top-100-march-update.pdf*

21 *PriceWaterhouseCoopers (2015): Global top 100 companies – 2015 update. http://www.pwc.com/gx/en/services/audit-assurance/publications/top100-market-capitalisation.html*

22 *Čas J, Peissl W (2010) Datenhandel – ein Geschäft wie jedes andere? Bundeszentrale für politische Bildung, 12.3.2010, http://www.bpb.de/gesellschaft/medien/wissen-und-eigentum/73338/datenhandel*

23 *Goldhammer K (2006) Wissensgesellschaft und Informationsgüter aus ökonomischer Sicht. Bundeszentrale für politische Bildung, 18.10.2006, http://www.bpb.de/gesellschaft/medien/wissen-und-eigentum/73312/die-oekonomische-sicht*

24 *wallstreet:online (2017) http://www.wallstreet-online.de/aktien/twitter-aktie/bilanz (14.5.2017)*

25 *Bloomberg Business (2017) TWTR:US. http://www.bloomberg.com/quote/TWTR:US (14.5.2017)*

26 *Herrlich C (2012) Private Daten – Die Währung des digitalen Zeitalters. IntraWorlds, http://www.intraworlds.de/talent-blog/2012/02/private-daten-die-waehrung-des-digitalen-zeitalters/*

27 *Schmidt E (2015) Ressource Big Data: Gewinnbringend aber gefährlich. Interview mit Sandro Gaycken. 3sat, 28.5.2015, http://www.3sat.de/page/?source=/boerse/magazin/181951/index.html*

28 *Robbins R (2015) Insurers want to nudge you to better health. So they're data mining your shopping lists. STAT, 15.12.2015, http://www.statnews.com/2015/12/15/insurance-big-data/*

29 *Prosser M (2013) How much does Facebook advertising cost? FitSmallBusiness, 1.9.2016, http://fitsmallbusiness.com/how-much-does-facebook-advertising-cost/*

30 *dpa (2016) Werbung bringt Facebook Milliarden-Gewinn. Frankfurter Allgemeine Zeitung, 28.1.2016, http://www.faz.net/agenturmeldungen/dpa/werbung-bringt-facebook-milliarden-gewinn-14038727.html*

31 *Statista (2016) Fakten zum Thema: Google. http://de.statista.com/themen/651/google/ (16.2.2016)*

32 *Shah N (2015) You are worth $182 to Google, $158 to Facebook and $733 to Amazon! Arkenea, 2.9.2015 , http://arkenea.com/blog/big-tech-companies-user-worth/*

33 *Schaefer S (2015) Facebook and Amazon join the $300 billion club with stocks at new highs. Forbes, 4.11.2015, https://www.forbes.com/sites/steveschaefer/2015/11/04/new-highs-put-facebook-amazon-in-the-300-billion-market-cap-club/#9b3240e29502*

34 *Steel E, Locke C, Cadman E, Freese B (2013) How much is your personal data worth? The Financial Times, 12.6.2013, http://www.ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html*

35 *Curtis S (2015) How much is your personal data worth? The Telegraph, 23.11.2015, http://www.telegraph.co.uk/technology/news/12012191/How-much-is-your-personal-data-worth.html*

36 *Buxmann P, Gerlach J, Wenninger H (2012) Der Preis des Kostenlosen. Ergebnisbericht zur Umfrage in Kooperation mit hr-iNFO. TU Darmstadt, Sept. 2012, http://blogs.hr-online.de/der-preis-des-kostenlosen/files/2013/05/Ergebnisbericht_Der_Preis_des_Kostenlosen.pdf*

37 *Deutsches Institut für Vertrauen und Sicherheit im Internet (2014): Daten – Ware und Währung. Hamburg, 17.11.2014. Archiviert unter https://web.archive.org/web/20161223120701/https://www.divsi.de/publikationen/studien/divsi-studie-daten-ware-und-waehrung/*

38 *Ehrenberg B (2014) How much is your personal data worth? The Guardian, 22.4.2014, http://www.theguardian.com/news/datablog/2014/apr/22/how-much-is-personal-data-worth*

39 *Barth T (2015) Democracy – Im Rausch der Daten? Oder der Bürokraten? Telepolis, 21.11.2015, http://www.heise.de/tp/artikel/46/46594/1.html*

Anja Grunert

Schöne neue Bücherwelt

Was E-Book-Reader über unser Leseverhalten herausfinden und wie Verlage oder Buchhändler dies nutzen können

„Die wichtigsten «Manhattan-Projekte» der Zukunft werden umfangreiche, von der Regierung geförderte Untersuchungen darüber sein, was die Politiker und die daran teilnehmenden Wissenschaftler «das Problem des Glücklichseins» nennen werden, mit anderen Worten, wie man die Menschen dahin bringt, ihr Sklaventum zu lieben."[1] Der britische Autor Aldous Huxley war ein überaus tiefgründiger Kritiker seiner Zeit. Er vollendete 1932 seinen Roman Brave New World*, welcher eine düstere Zukunft prophezeit. In dieser Wohlstandsgesellschaft, wo Sicherheit und Gesundheit gegeben sind, gibt der Mensch das Wichtigste in seinem Leben auf: seine Freiheit.[1]*

Das Buch entwickelte sich seit der Erfindung des Buchdrucks von Johannes Gutenberg weiter und wurde mittlerweile digitalisiert. Es ist eine der bedeutendsten Erfindungen überhaupt und dient der Kommunikation sowie der Bildung. Seit 2007 wurde in den Vereinigten Staaten das Buch digitalisiert und folglich entstand das erste E-Book. Das E-Book ist ein Buch, welches in ein digitales Format umgewandelt wurde. Der E-Book-Reader enthält alle E-Books, die Kunden gekauft, geliehen oder anderweitig kostenlos erhalten haben.[2] Er ist definiert als „flache[s], handliche[s] Lesegerät […] für die Darstellung von E-Books"[3]. Der Reader ist kompakt und leicht[2] und garantiert durch das E-Ink-Display ein angenehmes Lesen. Darüber hinaus bieten die meisten Reader On-Screen-Keyboards als Tastaturen auf dem Touchscreen an. Das ermöglicht die schnelle und einfache Eingabe von Notizen. Durch eine drahtlose Verbindung zum Internet wird der Zugang zum World Wide Web ermöglicht, was zur Folge hat, dass Bü-

cher immer und überall heruntergeladen werden können. Die Reader ermöglichen die Speicherung von über 1000 E-Books. Falls mehr vorhanden sein sollten, können diese von einer Cloud abgerufen werden.[4]

In Abbildung 1 wird dargestellt, mit welchen Geräten E-Books in Deutschland gelesen werden. Laut einer Studie von *Bitkom Research* mit 2.171 Testpersonen aus Deutschland lasen im Jahre 2016 die Mehrheit (46 %) E-Books auf E-Book Readern. Anschließend folgten Smartphones mit 41 % und der Laptop mit 36 %. 2015 lagen der Laptop mit 41 % und das Smartphone mit 38 % an der Spitze, erst danach folgte der E-Book Reader mit 34 %. Daran ist erkennbar, dass die Akzeptanz des Readers 2016 um 12 % gestiegen ist.[5]

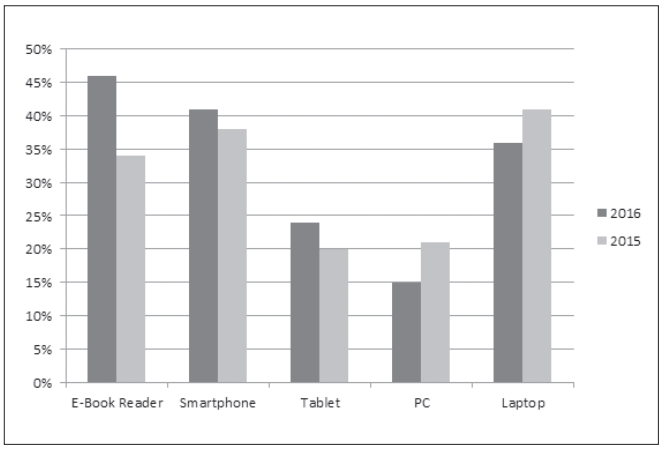


Abbildung 1: Prozentuale Verteilung der Nutzung von Geräten, um E-Books zu lesen (eigene Darstellung nach Shahd & Lutter[5])

Vor der Einführung des E-Books konnte kein Verlag feststellen, ob ein Buch wirklich von den Lesern gelesen wird oder was dem Leser besonders gut gefallen hat.[6] Das Prinzip war, dass „[d]er Autor schreibt [...] [und] der Leser liest“[7]. Durch die Einführung von E-Books ist es für Verkäufer, Autoren und Verlage erkennbar, welche Textstellen wichtig sind.[6] Durch den E-Book-Reader ist eine Art „Leserbeobachtung“ möglich geworden, da der Reader alle Funktionen, die der Nutzer ausführt, speichert und dem Gerätehersteller mitteilt. Folglich entwickelte sich im Laufe der letzten Jahre eine „direkte Rückkoppelung von Schreibenden und Lesepublikum“[7]. Hervorzuheben ist, dass E-Books über interaktive Inhalte verfügen können. Dazu zählen u. a. Spiele, Bilder, Hörbücher und Videos.[8] Dieser Bonus ermöglicht dem Leser bspw. bei Wechsel des Transportmittels Flexibilität. Nach dem Aussteigen aus Bus oder Bahn schaltet er einfach auf den Hörbuchmodus, sodass er das Buch weiter anhören kann. Außerdem gibt es die Alternative zum Einfügen einer Videobotschaft des Autors oder das kostenlose Blog-Abo als Zusatz.[9] Es gibt unter anderem Autoren, die das Buch zusammen mit ihrer Leserschaft schreiben.[7] Das Ziel dabei ist, dass die Bücher und deren Verkauf optimiert werden sollen.[6]

Unternehmen wie *Amazon* nutzen diese Tatsachen zu ihren Vorteil und sammeln aus elektronischen Büchern Daten, um die Gewohnheiten der Nutzer kennen zu lernen. Anstatt wie in vergangenen Zeiten nur die Verkaufszahlen zu kennen, verfügen die Verlage seit der Einführung von E-Books über ein „detailliertes Profil“ des Lesers und können neben dem Leseverhalten auch persönliche Interessen festhalten.[10] Die gewonnenen Datenwerte werden ohne ausdrückliche Zustimmung des Kunden zu Werbezwecken an Partnerunternehmen und Dritte weitergegeben.[11] Aus dem großen Erfolg von Firmen wie z. B. Amazon resultierte ein Hype um E-Books, sodass Buchhandlungen zunehmend an Bedeutung verlieren. Ersetzt werden sie durch E-Book-Stores, da die elektronischen Bücher keine Kosten durch „Transport und […] Lagerung“ verursachen[12].

In der Vergangenheit konnten Verlage, Autoren und Buchhändler kaum nachvollziehen, was mit einem Buch passierte, nachdem es gekauft wurde. Sie wussten weder, ob der Leser das Buch nach drei Seiten weglegt, noch ob er die Einleitung überspringt. Bücher lesen war eine Privatsache, die als sehr intim angesehen wurde. Durch die Einführung von E-Books haben die Verkäufer nun die Möglichkeit, einen Teil der Persönlichkeit des Lesers kennen zu lernen und Daten über ihn zu erhalten.[8] Das bedeutet aber auch, dass der E-Book-Reader den Leser überwacht. Der Reader erfasst z. B., wie oft die Bücher heruntergeladen, geöffnet und gelesen werden.[8] Abbildung 2 zeigt, welche Daten zusätzlich übermittelt werden und welche Aussagen Unternehmen nach dem Data-Mining-Verfahren z. B. treffen könnten.

Sobald der Reader über WLAN oder eine mobile Datenverbindung mit dem Internet verbunden ist, werden die in Abbildung 2 veranschaulichten Daten (Titel, Gerät, Lesezeit usw.) an einen Server gesendet. Einige Software-Anbieter wie *Adobe* scannen darüber hinaus den Computer, den E-Book-Reader oder das Smartphone. Aus bisheriger Erfahrung ist zu sagen, dass dieser Sachverhalt kritisch zu betrachten ist. Es gibt einige Anbieter, die ebenso E-Mail-Adressbücher oder Kennwörter mit diesem Vorgang auf ihren Server laden und somit Zugriff auf Kontakte und private Daten erhalten.[13] Diese Daten machen das Lesen sowohl publik als auch quantifizierbar.[14] Durch die Verarbeitung der Big Data werden einige Erkenntnisse über den Nutzer wie z. B. sein Geschlecht oder die Bildung erlangt.[10] Um das Ausmaß der Überwachung des Lesers an einen Beispiel zu verdeutlichen, wird in Abbildung 3 eine Grafik des gläsernen Lesers präsentiert:

Anja Grunert

Anja Grunert studiert Wirtschaftsinformatik an der Friedrich-Schiller-Universität Jena und ist bei der Softwareentwicklungsfirma zollsoft GmbH in Jena tätig. Schwerpunkte im Studium und bei der Arbeit sind unter anderen Datenschutz, Datenbanken und E-Commerce.

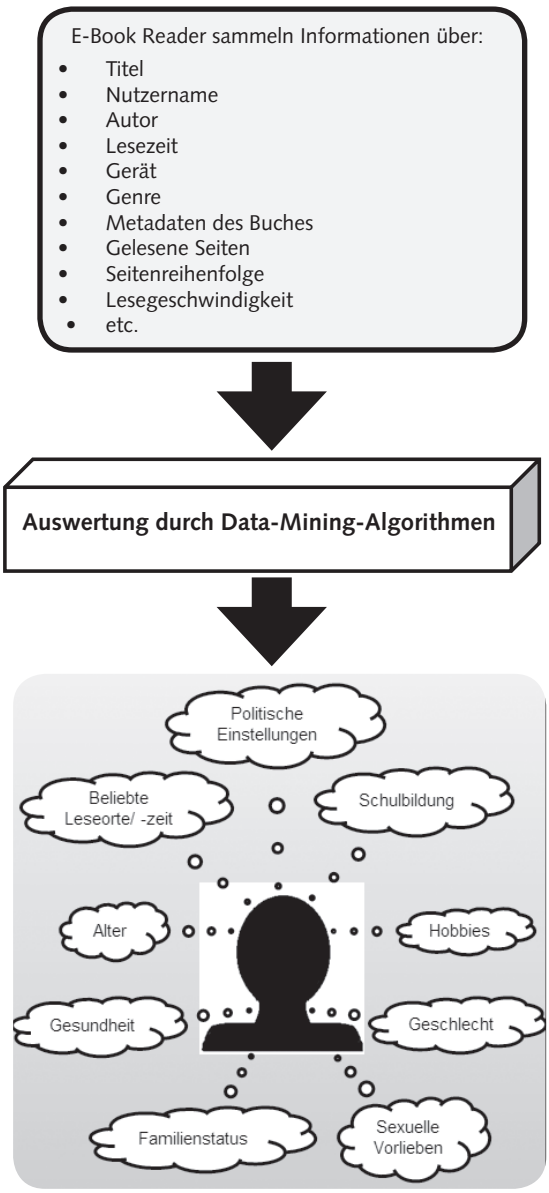


Abbildung 2: Input und Output von Data Mining (eigene Darstellung nach Hoffelder[13], Alter[8], Schroeder[14], Pursche[10])

Abbildung 3 sagt aus, dass der durchschnittliche Mann, der romantische Bücher liest, eine europäische Sprache spricht, 30 Jahre alt ist, schwarze Haare und grüne Augen hat. Dieser Mann ist auf der Abbildung dargestellt mit einer Rose in der Hand. Darüber hinaus liegen ebenso genaue Daten über das Buch *Hunger Games* (*Die Tribute von Panem – Gefährliche Spiele*) von Suzanne Collins vor. Der durchschnittliche Leser benötigt 7 Stunden, um das Buch durchzulesen. Er liest etwa 57 Seiten pro Stunde. Außerdem haben 18.000 *Kindle*-Leser (Stand: 19.07.2012) in der englischen Fassung des E-Books die folgende Stelle markiert:

> *„Because sometimes things happen to people and they're not equipped to deal with them."*

Ein weiteres Beispiel bietet George R. R. Martins Buch mit dem Titel *A Game of Thrones*. Durchschnittlich werden 20 Stunden zum Lesen von 1.040 Seiten benötigt. Analysten haben weiterhin herausgefunden, dass die meisten Leser des ersten Buches anschließend das nächste Buch herunterladen. Ebenso verhält es

Abbildung 3: Der gläserne Leser[8], © John Cuneo

sich mit anderen Novellen, Romanzen, Krimis und Science-Fiction-Romanen. Bei Fachliteratur wird das Lesen hingegen öfters unterbrochen, um zu einem späteren Zeitpunkt fortzufahren. Darüber hinaus werden mehrere Fachbücher gleichzeitig geöffnet, um zwischen ihnen hin und her zu springen.[8]

Die Rohdaten der E-Book Reader werden von dem Anbieter mit bereits vorhandenen Daten verknüpft. Daher ist es möglich, den Daten einen monetären Wert zuzuordnen und zielgruppengenaue Einblendung von Online-Werbung zu betreiben.[15] Die Statistik in Abbildung 4 zeigt, dass dieses Vorgehen Erfolg hat.

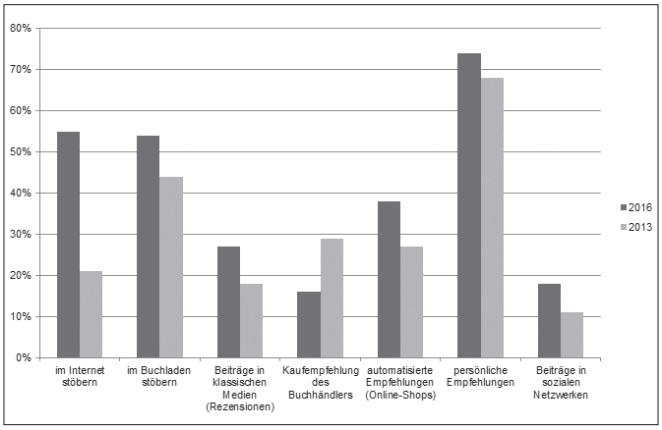


Abbildung 4: Woher das Interesse für neue Bücher kommt (eigene Darstellung nach Shahd & Lutter[5])

Die automatisierten Empfehlungen von Online-Shops und das Stöbern im Internet sind im Vergleich zu 2013 immer wichtiger geworden, wohingegen das Interesse an der Kaufempfehlung des Buchhändlers um 13 % gesunken ist. Die Mehrheit der Leser wird durch persönliche Empfehlungen (74 %) sowie das Stöbern im Internet (55 %) und im Buchladen (54 %) auf Bücher aufmerksam. Das Internet ist somit eine „zentrale Informationsquelle für Literatur und Sachliteratur" geworden, sodass gezielte und angepasste Werbemaßnahmen im Internet überaus bedeutend sind.[5]

Die Auswertung der Daten wird unter anderem an die Verleger weitergeleitet. Zweck ist die Generierung von Büchern, die im Interesse des Lesers sind und somit der Umsatzsteigerung des Verlags und der Buchverkäufer dienen.[8] Ferner werden sie ohne „Zustim-

mung de[s] Kunden an andere Unternehmen […] in aggregierter Form" zu Werbe- und Marketingzwecken weitergegeben. Das Widersprechen ist mittels nachträglicher Verweigerung des Kunden möglich. Eine Ausnahme hierbei bietet *Google Books*. Diese Firma gibt die Daten nur mit vorheriger Zustimmung weiter.[15]

Eine Gefahr, die bei der Auswertung von Millionen von Leserdaten entsteht, könnte in der Einschränkung des Reichtums an Büchern liegen. Die Statistik in Abbildung 5 zeigt, welche Kategorien von Büchern von Männern und Frauen bevorzugt werden.

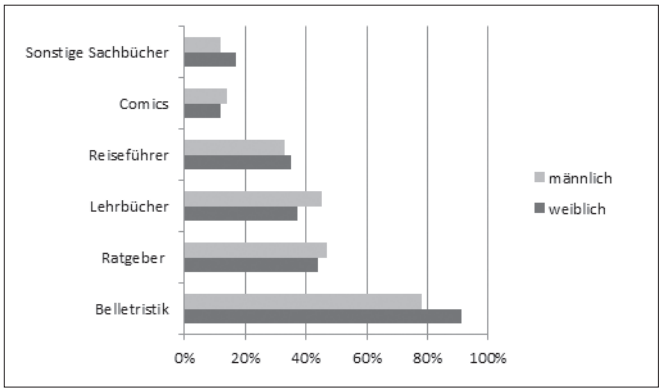


Abbildung 5: Welche Genres von Männern und Frauen gelesen werden (eigene Darstellung nach Shahd & Lutter[5])

Daraus resultiert, dass Bücher, die nur von Minderheiten gekauft werden, wie bspw. Lehrbücher, durch das mangelnde Interesse der Leserschaft seltener durch Verlage veröffentlicht werden. Verlage und Verkäufer könnten der Ansicht sein, dass Belletristik das Genre ist, das die Leser begeistert. Infolgedessen könnte es zum Innovationsstopp und zur verminderten Erstellung von Fachliteratur kommen.[8] Zukünftig führt dieses Vorgehen zu einem „literarische[n] Einheitsbrei"[14].

Ein weiterer Nachteil ist, dass der Leser das gewünschte Buch bei Amazon nicht kauft, sondern es ihm nur „zur Verfügung gestellt" wird[16]. Die Lizenzvereinbarung von Amazon sagt dazu folgendes: „Digitale Inhalte werden durch den Anbieter von Inhalten lizensiert, nicht aber verkauft."[17] Beim Kauf muss der Leser einen Account bei Amazon haben und eine „Lizenz sowie ein digitales Rechtemanagement akzeptieren". Dieser Vorgang schließt bestimmte Nutzungsmöglichkeiten wie bspw. das Kopieren des E-Books aus.[18] Das heißt, dass Amazon bei Nichteinhalten der Nutzungsbedingungen alle E-Books vom Gerät „ohne Rückerstattung des Kaufpreises" löschen darf[16]. Ein gutes Beispiel ist an dieser Stelle die Rücknahme bzw. Löschung von Orwells *Animal Farm* und *1984* von den E-Book-Readern Kindle, da Amazon diese Bücher von einem Unternehmen kaufte, welches die Rechte nicht besaß. Kunden, die die genannten E-Books gekauft hatten, reagierten empört. Ein 17-jähriger Junge aus Detroit war besonders betroffen. Er las das Buch *1984* für einen Sommerkurs und machte Bemerkungen in seinem E-Book. Bei Löschung des Buches gingen alle Daten verloren.[19]

Durch die Speicherung und Auswertung der riesigen Datenmengen (*Big Data*) durch Amazon können Werbeanzeigen „zielgerichtet geschaltet und vermarktet werden" (*Targeting*)[20]. Es ermöglicht dem Unternehmen die Einteilung der Kunden nach Eigenschaften wie Geschlecht, Alter, Wohnort, Schulbildung, Interessen sowie Umsatz. Weiterhin ist die Vorhersage von Verhaltensmustern durch Amazons Algorithmen möglich und bedeutend, um das Einkaufsverhalten der Kunden zu bestimmen und auszulösen.[20] Ein Beispiel hierfür ist die Bestellung eines Krimis. Innerhalb kürzester Zeit schaltet Amazon Werbung auf dem Kindle des Lesers über Bücher aus denselben oder ähnlichen Kategorien. Darüber hinaus erhält das Unternehmen z. B. durch die Bestellung eines Schwangerschaftsbuches die Information, dass die Leserin schwanger ist und blendet Babyartikel wie ein Vornamenbuch ein. Weiterhin wird durch die Bestellung eines Autobuches für Kinder erkannt, dass das Baby höchstwahrscheinlich ein Junge ist und somit werden Kleidung, Spielzeug und Ratgeber für Jungs als Werbeanzeige geschaltet.[21] Die Amazon.de-Datenschutzerklärung erklärt nicht, welche Daten vom Kunden erhoben werden. Es wird lediglich darauf hingewiesen, dass es Informationen sind, die sie von Kunden erhalten. Weiterhin werden auch „automatische Informationen", die z. B. von Cookies übertragen werden, gesammelt. Amazon rechtfertigt den Vorgang mit der Aussage, dass viele andere Webseiten das auch machen.[11] Die Daten werden benötigt, um das Einkaufserlebnis, die Abwicklung des Kaufvorgangs sowie sonstige Marketingangebote zu verbessen. Auf die Frage, an wen die Daten weitergegeben werden könnten, nennt Amazon.de folgende Parteien: verbundene Unternehmen, Partnerunternehmen, Dienstleister, Promotionen und Dritte.

Außerdem „verhindert Amazon […] verlegerische Innovationen" wie z. B. den gemeinsamen Verkauf von E-Books und Taschenbüchern[20]. „Der Umgang mit Nutzerdaten" kostete das Unternehmen den Testsieg bei Stiftung Warentest.[22] Allerdings bieten Features wie z. B. „Was kaufen Kunden, nachdem sie diesen Artikel angesehen haben?" für Amazon einen Nutzen, da der Kunde auf neue Kaufideen gebracht wird und sich somit mehr Umsatz generieren lässt.[23]

Zusammenfassend ist zu sagen, dass Amazon einerseits eine überaus große Büchervielfalt bietet, andererseits hortet es die Daten der Kunden, um daraus Profit zu erzielen. Weiterhin wird das Unternehmen aufgrund seiner erfolgreichen Datennutzung vom E-Commerce-Unternehmen zum Big-Data-Unternehmen, welches neben Büchern, Kleidung und Spielzeug die Daten seiner Kunden an Werbeunternehmen verkauft.[24] Kritiker sehen in E-Books „eine unzulässige Einschränkung der Freiheit der Leser" und einen „Rückschritt gegenüber gedruckten Büchern". Sie rufen zum Boykott auf, damit Amazon und andere E-Book-Anbieter mehr Freiheiten für ihre Kunden einräumen.[18]

Durch die Sammlung von Daten ergeben sich neue Herausforderungen für die Gesetzgebung in Sachen Datenschutz und Selbstbestimmung.[25] Daten, die Personen zugeordnet werden können, sollten nicht ohne ausdrückliche Erlaubnis an Dritte weitergegeben werden dürfen. Dazu gehört, dass der Leser Auskunft darüber erhält, „wem er in welchem Umfang, zu welchem Zweck und in welchem Zeitraum" seine Daten preisgibt[26]. Weder der Amazon Shop noch andere E-Book-Stores erläutern das Ziel der Datensammlung in ihren AGBs (Allgemeine Geschäftsbedingungen).[10] Bedauerlicherweise ist der Umgang mit den Daten sowie die Form der AGBs bei nahezu allen Readern mangelhaft. Kein Anbieter schließt die Nutzung der Daten für andere Zwecke aus.[22] Darüber hinaus werden Autoren von ihren Verlegern aktuell dazu gebracht, das zu schreiben, was die Leser am meisten interessiert und in welchem Genre die höchsten Absatzpotentiale zu finden sind. Durch diese gravierenden Veränderungen wurde das Lesen ein überwachter Akt.[14] Laut einer Aussage der Zeitschrift *Die Zeit*

werden die Unternehmen, die die meisten Leserdaten besitzen, „die Zukunft des Buchmarktes“ bestimmen. Das heißt, dass Firmen wie Amazon bald die Richtung in Sachen Lesestoff angeben.[7] Schützen gegen die Datensammlung kann der Leser sich nur durch Lesen eines normalen Buches.[23] Maßnahmen, die der Sicherung der Daten dienen könnten, wären u. a. neue Verschlüsselungstechnologien sowie die „Sicherheit von Speichersystemen und qualifizierte […] Zugriffs- und Berechtigungslogiken“[26].

Die Welt des digitalen Buches ist ein „goldener Käfig“ geworden. Neben Komfort und Nutzen wirken E-Book-Reader durch dauerhaftes *Tracken* ihrer Leser freiheitsberaubend.[22]

> *„Auch die Kunst hat ihre Moral und viele Gesetze dieser Moral sind dieselben wie die Gesetze gewöhnlicher Ethik oder ihnen zumindest analog.“*[1]

Referenzen

1 *Huxley A (2012) Schöne neue Welt. Fischer Taschenbuch Verlag, Frankfurt a. M., 68. Auflage, S. 9, 15*
2 *Plöger S, Schmidt F (2015) eBook-Reader: Die besten Modelle im Test. Computer Bild*
3 *ITwissen.info (2015) E-Book-Reader. http://www.itwissen.info/E-Book-Reader-ebook-reader-eReader.html*
4 *Colon A, Lendino J (2015) The best ebook readers of 2015. PCMag*
5 *Shahd M, Lutter T (2016) Nutzung von E-Books bleibt stabil. Bitkom, 11.10.2016, https://www.bitkom.org/Presse/Presseinformation/Nutzung-von-E-Books-bleibt-stabil.html*
6 *Lang T (2013) E-Books lesen persönliche Daten aus. PC Magazin, 18.3.2013, http://www.pc-magazin.de/ratgeber/e-books-persoenliche-daten-datenschutz-1473671.html*
7 *Probst M, Trotier K (2013) Leser, mach's dir selbst! Die Zeit Nr. 06/2013, http://www.zeit.de/2013/06/Internet-Buecher-schreiben*
8 *Alter A (2012) Your E-Book is reading you. The Wall Street Journal, 19.7.2012, https://www.wsj.com/articles/SB10001424052702304870304577490950051438304*
9 *Oppmann V (2009) Die neuen Vertriebskanäle des Lesens. The European, 4.11.2009, http://www.theeuropean.de/volker-oppmann/1893-wie*
10 *Pursche O (2013) eBooks: Anbieter lesen fleißig mit. Computer Bild, 7.10.2013, http://www.computerbild.de/artikel/cb-News-PC-Hardware-eBook-Reader-Hersteller-lesen-mit-7625845.html*
11 *Amazon.de (2015) Amazon.de-Datenschutzerklärung. https://www.amazon.de/gp/help/customer/display.html/ref=hp_left_v4_sib?ie=UTF8&nodeId=201909010 (1.5.2017)*
12 *Müller C, Spiegel S, Ullrich F (2010) E-Books in Deutschland: Der Beginn einer neuen Gutenberg-Ära? PricewaterhouseCoopers, Sept. 2010, http://www.pwc.de/de/technologie-medien-und-telekommunikation/assets/e-books_in_deutschland_-_beginn_einer_neuen_gutenberg-aera.pdf*
13 *Hoffelder N (2014) Adobe is spying on users, collecting data on their ebook libraries. The Digital Reader, 6.10.2014, http://the-digital-reader.com/2014/10/06/adobe-spying-users-collecting-data-ebook-libraries/*
14 *Schroeder T (2013) Der Kindle liest mit: Datenschutz adé! E-Reader FAQ, 10.9.2013, http://www.ereaderfaq.de/der-kindle-liest-mit-privatsphaere-ade/*
15 *unwatched.org (2012) Datenschutz: Welche eBook-Reader ihre Leser tracken. Archiviert unter https://web-beta.archive.org/web/20130901133230/http://www.unwatched.org/20121216_Datenschutz_Welche_E-Book-Reader_ihre_Leser_tracken*
16 *Bitomsky F (2014) Das Kindle-Format: Vor- und Nachteile des Amazon-Readers. Liber Laetitia, 25.7.2014, http://liber-laetitia.de/blog/kindle-format-vor-und-nachteile-des-amazon-readers/*
17 *Spiegel Online (2012) Amazon sperrt Kindle-Account. 23.10.2012, http://www.spiegel.de/netzwelt/web/amazon-sperrt-account-einer-kindle-nutzerin-samt-bibliothek-a-862926.html*
18 *Pluta W (2011) Richard Stallman will E-Books boykottieren. Golem.de, 9.6.2011, https://www.golem.de/1106/84107.html*
19 *Stone B (2009) Amazon erases Orwell books from Kindle. The New York Times, 18.7.2009, http://www.nytimes.com/2009/07/18/technology/companies/18amazon.html*
20 *Knop C (2013) Amazon kennt dich schon: Vom Einkaufsparadies zum Datenverwerter. Frankfurter Allgemeine Buch, Frankfurt a. M.*
21 *Hentschel A (2009) Amazon kennt Sie besser als Sie sich selbst. Focus Online, 6.2.2009, http://www.focus.de/digital/computer/chip-exklusiv/tid-13299/datenschutz-amazon-kennt-sie-besser-als-sie-sich-selbst_aid_367742.html*
22 *Pachali D (2013) Stiftung Warentest: Viele Mängel bei AGB und Datenschutz von E-Book-Portalen. iRights.info, 26.9.2013, http://irights.info/artikel/stiftung-warentest-viele-mangel-bei-agb-und-datenschutz-von-e-book-portalen/18062*
23 *Haupt J (2009) EFF: Datenschutz bei eBooks mangelhaft. lesen.net, 22.12.2009, http://www.lesen.net/diskurse/eff-datenschutz-bei-ebooks-mangelhaft-1918/*
24 *Rijmenam M (2015) How Amazon is leveraging big data. Datafloq, https://datafloq.com/read/amazon-leveraging-big-data/517*
25 *OECD (2012) E-books: Developments and Policy Considerations. OECD Digital Economy Papers, Nr. 208, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/5k912zxg5svh-en*
26 *Beer N (2015) Ein zentraler Ort für alle meine Daten. Zeit Online, 17.4.2015, http://www.zeit.de/politik/deutschland/2015-04/fdp-digitalisierung-datenschutz-nicola-beer*

Peter Wohlgenannt

Auf der Spur digital terrestrischer Fußabdrücke

Ein Großteil der Bevölkerung aus Industrieländern ist durch mobile Geräte wie Smartphones und Tablet-Computer befähigt, ständig auf das Internet zuzugreifen. Die Bundesanstalt Statistik Österreich *hat für das Jahr 2015 erhoben, dass österreichweit 72,3% aller Personen im Alter zwischen 16 und 74 Jahren innerhalb von drei Monaten mittels einem mobilem Gerät (nachfolgend als* Station *bezeichnet) das Internet benutzt haben. In der Gruppe der 16- bis 24-Jährigen nutzten sogar 97,7 % mobiles Internet.[1] Viele dieser Personen dürften u. a. per WLAN über eigene und fremde* Access Points *(APs) den Internetzugang hergestellt haben. Betrachtet man den technischen Vorgang bzw. das für den Verbindungsaufbau benutzte Kommunikationsprotokoll, gelangt man zur Erkenntnis, dass ein mobiles Gerät auf der Suche nach verwendbaren APs stetig Klartextinformation zu dessen* MAC-Adresse *(dem eindeutigen Identifikator des verbauten WLAN-Adapters) sowie teilweise die Namen bevorzugter Netzwerke aussendet. Gelingt die Zuordnung einer MAC-Adresse zu einer bestimmten Person, können in weiterer Folge sensible Information (wie Standortdaten) zu dieser Person gesammelt bzw. bereits erhobene Daten mit ihr verknüpft werden.*

Das Protokoll IEEE 802.11

Das Protokoll 802.11 für Kommunikation in Funknetzwerken[2], hauptsächlich unter den Begriffen WLAN und Wi-Fi bekannt, wurde durch das Institute of Electrical and Electronics Engineers (IEEE) entwickelt. Die Datenübertragung erfolgt, aufgeteilt auf 14 Kanäle (wobei Kanal 14 nur in Japan verwendet wird), hauptsächlich im 2,4-GHz- und eher selten auch im 5-GHz-Band.

Eine *MAC-Adresse* (Media-Access-Control-Adresse) setzt sich aus sechs normalerweise durch Doppelpunkt voneinander getrennten Bytes in hexadezimaler Schreibweise zusammen. Über die ersten drei Bytes lässt sich der Hersteller jeder individuellen WLAN-Karte eruieren[3] (z. B. 00:07:E9:XX:XX:XX ist dem Hersteller Intel zuzuordnen). Über die Broadcast-Adresse FF:FF:FF:FF:FF:FF werden alle Geräte in einem lokalen Netzwerk adressiert. Häufig ist die MAC-Adresse auf einem am Netzwerkgerät angebrachten Sticker aufgedruckt oder kann über das Betriebssystem abgefragt werden (z. B. per Linux-Befehl *ifconfig*, Windows-Befehl *ipconfig*).

Die *SSID* (Service Set ID) ist der durch den AP-Betreiber frei wählbare Name für den AP. Es ist möglich, mehrere Namen für ein und dasselbe Gerät zu vergeben und unterschiedliche Restriktionen dafür vorzugeben (Stichwort *Virtual Local Area Networks*). Anhand der SSID wählt der Nutzer den AP, mit dem er sich verbinden möchte.

Bei der *BSSID* (Basic Service Set ID) handelt es sich um die eindeutige MAC-Adresse des AP, welche der Nutzer normalerweise nicht zu sehen bekommt – gleichnamige APs aber unterscheidbar macht. Werden mehrere APs unter derselben SSID (also demselben Namen) betrieben, um damit beispielsweise eine größere Fläche abdecken zu können, wird diese als *ESSID* (Extended SSID) bezeichnet. Der Nutzer kann nicht zwischen SSID und ESSID unterscheiden.

Die zwischen Netzwerkgeräten übertragenen Pakete werden in drei unterschiedliche Typen unterteilt:

1. *Management Frames* werden für Authentifizierung, Verbindung sowie Synchronisation benötigt und sind immer im Klartext verfügbar (z. B. Beacon Frames, Probe Request Frames, Authentication und Deauthentication Frames). Zur Informationsgewinnung und Durchführung der hier vorgestellten Angriffe werden ausschließlich die in den Management Frames enthaltenen Daten genutzt.

2. *Control Frames* müssen ebenfalls in unverschlüsselter Form vorliegen, regeln den Datenfluss und werden vor allem zur Vermeidung von Kollisionen benötigt.

3. *Data Frames* sind die eigentlichen Nutzdaten (auch als *Payload* bezeichnet), welche zumeist verschlüsselt sind und den nutzerspezifischen Inhalt befördern.

Jedes 802.11-Paket enthält unter anderem die Absender- und Ziel-MAC-Adresse in unverschlüsselter Form.

Aktive und passive Access Points

Einerseits bieten APs ihre Dienste mobilen Geräten passiv per Beacon Frame über einen Broadcast an (Abbildung 1, rechts), welcher u. a. Information über den Netzwerk-Namen und zur erforderlichen Authentifikation (offen/frei zugänglich, im Allgemeinen WEP-, WPA- bzw. WPA2-verschlüsselt) liefert. Hierbei ist anzumerken, dass der Broadcast des Netzwerk-Namens aus Sicherheitsgründen unterdrückt sein könnte. Dies bedeutet, dass der AP sich nicht anbietet, sondern an einer Verbindung interessierte Stations aktiv nach ihm suchen müssen.[4] Aktives Suchen bedeutet, dass die Station auf sämtlichen Kanälen per Probe Request nach bereits bekannten (E)SSIDs sucht und bei dieser Gelegenheit auch die MAC-Adresse mitschickt (siehe Abbildung 1, links). Die meisten Geräte speichern standardmäßig eine Liste mit APs, mit welchen sie sich schon einmal erfolgreich verbunden haben – die *Configured Network List* (*CNL)*. Diese Information liegt in den übertragenen Paketen immer unverschlüsselt vor, auch wenn die Nutzdaten durch Verschlüsselung gegen unbefugte Einsicht geschützt sind.

Abbildung 1: Aktive Suche nach APs (links) vs. sich passiv anbietender AP (rechts)
© New H3C Technologies Co., Limited

WLAN-Sniffen – verbreitete Hard- und Software

Das Vorhandensein dieser Klartextinformation ermöglicht es, passiv von APs gesendete Beacon Frames als auch Probe Requests und dazugehörige Probe Responses mitzulesen, was auch als WLAN-Sniffen oder Snooping (engl. für schnüffeln) bezeichnet wird. Für das passive und aktive Sniffen bedarf es spezieller Hard- und Software. Der Autor dieses Artikels verwendet hauptsächlich das Betriebssystem *Kali Linux 2016.1* mit dem vorinstallierten Softwarepaket *Aircrack-Suite*[5] sowie den bereits gepatchten Treibern für kompatible WLAN-Karten in Verbindung mit einer USB-WLAN-Karte der Marke/Type *Alfa Awus036h* (Chipset RTL8187L, Treiber r8187).

Vorbereitend muss die Netzwerkkarte dann nur noch in den *Monitor Mode* geschaltet, anschließend können die eintreffenden Datenpakete aufgezeichnet werden. Der Monitor Mode fängt sämtliche an der WLAN-Karte vorbeifliegenden Pakete ein, auch wenn sie nicht an diese adressiert sind.

Standardmäßig aktiviertes WLAN

Bei der Firmware *Android* ab der Version 4.3 alias *Jelly Bean*[6] ist das WLAN als ständig aktiv vorkonfiguriert, auch wenn der Nutzer es vermeintlich ausgeschaltet hat. Dies dient den dazu berechtigten Programmen, den Standort ohne aktiviertes GPS-Modul feststellen zu können. Der Vorteil liegt im geringeren Stromverbrauch. Möchte der Nutzer dies unterbinden, muss er in der Rubrik *Erweiterte WLAN-Einstellungen* unter dem Punkt *WLAN im Ruhemodus aktiviert lassen* die Option „Nie“ auswählen.

```
CH  9 ][ Elapsed: 1 min ][ 2007-04-26 17:41 ][ WPA handshake: 00:14:6C:7E:40:80

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:09:5B:1C:AA:1D   11  16       10        0    0  11  54.  OPN              NETGEAR
00:14:6C:7A:41:81   34 100       57       14    1   9  11e  WEP  WEP         bigbear
00:14:6C:7E:40:80   32 100      752       73    2   9  54   WPA  TKIP   PSK  teddy

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

00:14:6C:7A:41:81  00:0F:B5:32:31:31   51   36-24    2       14
(not associated)   00:14:A4:3F:8D:13   19    0-0     0        4    mossy
00:14:6C:7A:41:81  00:0C:41:52:D1:D1   -1   36-36    0        5
00:14:6C:7E:40:80  00:0F:B5:FD:FB:C2   35   54-54    0       99    teddy
```

Abbildung 2: airodump-ng Konsolenausgabe Quelle: Ausgeschnitten aus http://www.aircrack-ng.org/doku.php?id=airodump-ng Aircrack-ng, CC BY-NC-SA 4.0

Die in Geräten großer Hersteller wie Apple und Microsoft eingesetzte Firmware dürfte sich bezüglich der WLAN-Ortung ähnlich verhalten und durch den Nutzer mehr oder weniger transparent einstellbar sein. Es folgt daraus, dass ein mobiles Gerät, beispielsweise ein Smartphone, auch dann WLAN-Signale aussenden könnte, wenn der Nutzer seiner Meinung nach die WLAN-Karte deaktiviert hat.

Reichweite von WLAN-Geräten

Die typische Reichweite eines AP beträgt ca. 35 Meter in Räumen und ca. 100 Meter im freien Gelände.[7] Auch die in den Smartphones verbauten WLAN-Karten dürften stark in ihrer Reichweite variieren und ebenfalls max. 100 Meter an Reichweite erreichen können[7], zumal diese im Gegensatz zu vielen APs über keine leistungsstarken, externen Antennen verfügen.

Zuordnung einer bekannten Zielperson zu einem noch nicht identifizierten mobilen Gerät

Wie bereits erwähnt, muss die WLAN-Karte des Angreifers zuerst in einen Modus gebracht werden, welcher sämtlichen Datenverkehr mithört. Am konkreten Beispiel der Konsolenapplikationen *Aircrack-Suite* gelingt dies mit dem Kommando `sudo airmon-ng <start|stop> <interface>` (wobei es sich bei *<interface>* um die Aircrack-Suite-kompatible WLAN-Karte handelt). Anschließend befindet sich die Karte im sogenannten *Monitor Mode*, wobei die neu hinzugekommene Schnittstelle als *mon<Nr>* bezeichnet wird. Mit dem Kommando `airodump-ng --write </path/filename> mon<Nr>` können nun die in Reichweite der WLAN-Karte befindlichen APs und Stations über die im Klartext vorliegenden Control- und Management-Frames bei ihren Aktivitäten beobachtet und in Dateien gespeichert werden. Abbildung 2, der Aircrack-Webseite entnommen, enthält Information zu den aktuell beobachteten APs und Stations (PWR = Signalstärke, CH = Kanalnummer, ENC = verwendete Verschlüsselung).

Versuchsaufbau – mobile Überwachungseinheit

Um die nachstehend beschriebenen Angriffe auch tatsächlich durchführen zu können, wären folgende Eigenschaften betreffend unsere mobile Überwachungseinheit wünschenswert:

1. Auf dem Überwachungsgerät sollte das OS Kali Linux lauffähig sein.
2. Das Überwachungsgerät sollte möglichst klein und bestenfalls unauffällig sein.

Einerseits bieten sich dafür Kleinstcomputer wie beispielsweise der *Raspberry Pi*[8] an. Andererseits würde sich speziell für die nachfolgend beschriebenen Angriffe ein modifiziertes Smartphone sehr gut eignen, da ein solches über einen Touchscreen verfügt. Dadurch kann individuell auf den Programmablauf Einfluss genommen werden (vor allem auf den Beginn und den Abbruch eines Angriffs).

Zur Implementierung wurde ein ausgedientes Smartphone der Marke/Type *LG-E960* aka *Google Nexus 4* mit dem Betriebssystem *Nethunter*[9] bespielt, welches auf (der *Debian*-Distribution) Kali Linux basiert. Außerdem wird zusätzlich ein Micro-USB-OTG-Hub, ein USB-Akkupack und eine USB-WLAN-Karte der Marke/Type *TP-Link TL-WN722N* eingesetzt.

Angriff Nr. 1 – die WLAN-AP-Replay-Attacke

Auf Abbildung 2 ist zu erkennen, dass verschiedene Stations per Probe Request nach konkreten APs Ausschau halten (z. B. mossy) und versuchen, sich damit zu verbinden. Die WLAN-AP-Replay-Attacke nutzt genau diesen Umstand aus; sie gliedert sich in zwei Phasen:

Zuerst werden an einem der Zielperson vertrauten Ort, z. B. der Privatadresse, die verfügbaren APs erhoben. Wenn diese Liste bevorzugter Netzwerke mehrere individuelle Namen für SSIDs führt, kann von einem gerätespezifischen Wi-Fi-Fingerprint gesprochen werden. Mathieu Cunche[10] hat dafür ein Shell-Skript geschrieben (welches wiederum ein Perl-Skript startet), das die APs in vereinfachter Weise lediglich mit den Attributen SSID und `0` für offen bzw. `1` für gesichert in eine Textdatei (im folgenden Beispiel nach `APFinger.txt`) schreibt .

```
root@kali: #
./WiFi\_AP\_fingerprinter.sh
APFinger.txt mon0
---------------------------------
FAU\_WiFi;1
myWifi;1
Kitzmann Guest;0
FBI\_Surveillance - Van\_02;0
```

Alternativ könnten diese Daten auch online über die Webseite *Wigle*[11] beschafft werden. Wigle steht für *Wireless Geographic*

Logging Engine und bietet über seine Webseite die Möglichkeit, im Zuge von *Wardriving*[12] gesammelte Access-Point-Daten hochzuladen und auch abzufragen. Zum Zeitpunkt der Erstellung dieses Artikels sind ca. 340 Millionen Datensätze weltweit erfasst worden.[11]

Zu einem späteren Zeitpunkt begibt man sich in die Nähe der Zielperson, um die ihr bekannten APs als verfügbar vorzutäuschen und währenddessen mitzuprotokollieren, welche Geräte versuchen, sich zu verbinden. Für die Replay-Attacke bietet sich insbesondere der Arbeitsplatz dieser Person an. Wie von Golle und Partridge[13] gezeigt, ist die Wahrscheinlichkeit, dass zwei Personen am gleichen Ort wohnen und auch arbeiten, sehr gering.

Praktisch läuft das durch Cunche in zwei Skripten automatisierte Verfahren folgendermaßen ab: Die in der Wi-Fi-Fingerprint-Textdatei gespeicherten APs werden ausgelesen und durch das zur Aircrack-Suite gehörige Tool *airbase-ng* vorgetäuscht.[10] Das hoffentlich in Reichweite befindliche Smartphone erkennt die SSIDs und versucht, sich im besten Fall als Einziger zu verbinden. Dieser Verbindungsversuch wird schlussendlich protokolliert und unter *Displaying results* im Terminal ausgegeben.

```
root@kali: #
./WiFi\_AP\_replayer.rb APFinger.txt mon0
Creating fake AP : myWifi (privacy=1)
Creating fake AP : Kitzmann usw.
Analyzing results ...
Displaying results ...
C0:EE:FB:XX:XX:XX myWifi
```

Lediglich die Station mit der MAC-Adresse *C0:EE:FB:XX:XX:XX* hat versucht, sich mit *myWifi* zu verbinden. Es könnte sich daher um unsere Zielperson handeln. Es wäre nun möglich, das Ergebnis der Zuordnung mit dem im nachfolgenden Abschnitt vorgestellten Angriff zu verifizieren, welcher jedoch auch für sich alleine stehen kann.

Angriff Nr. 2 – die „Stalker-Attacke"

Auch dieser Angriff[10] gliedert sich in zwei Phasen, diesmal in eine Beschaffungs- und eine Analysephase. Es wird im Folgenden von einem Smartphone mit aktiviertem WLAN ausgegangen, wobei es sich natürlich um jede Art von mobilem Gerät handeln könnte.

1) Im Zuge der Beschaffungsphase wird die Zielperson im öffentlichen Raum über einen nicht genau definierten, aber möglichst langen Zeitraum unauffällig verfolgt. Es muss dabei zum einen darauf geachtet werden, nicht das Signal zum betreffenden Smartphone zu verlieren, zum anderen, der Zielperson nicht aufzufallen. Die MAC-Adressen der aktiv suchenden Smartphones und die Kontaktlänge in Sekunden werden dabei in eine Textdatei gespeichert. Die Erfassung der Kontaktlänge hängt mit dem Umstand zusammen, dass im Zuge der Verfolgung vermutlich auch andere Personen in den Fokus der mobilen Überwachungseinheit geraten. Das Kommando zur Aufzeichnung lautet:

```
root@kali: #
./WiFi\_monitor.sh capture\_file.txt mon0
```

Cunche hat einen Versuch unternommen,[10] bei welchem er sich zwei Stunden lang planlos durch eine große Stadt bewegt und zwei Aufzeichnungen erstellt hat. Bei der ersten Aufzeichnung wurden 1.644, bei der zweiten 460 Geräte erfasst. In der ersten Aufzeichnung betrug die Kontaktlänge bei 80 % der erfassten Geräte weniger als 500 Sekunden; einige Kontakte bestanden jedoch auch deutlich länger.

2) Nach Beendigung der Aufzeichnung werden die dabei aufgenommenen Daten mit dem dafür geschriebenen *Ruby*-Programm *Analyze_capture.rb* hinsichtlich Kontaktdauer absteigend sortiert. An erster Stelle sollte abhängig von der Dauer der Beschaffungsphase mit hoher Wahrscheinlichkeit die gesuchte MAC-Adresse zu finden sein.

```
root@kali: #
./Analyze\_capture.rb capture\_file.txt
MAC addr : Contact Length ( sec )
[C0:EE:FB:XX:XX:XX] : 1023.129089
[1C:4B:D6:XX:XX:XX] : 13.435345
[F8:1E:DF:XX:XX:XX] : 0.12231
...
```

ARP Poisoning bzw. *Man-In-The-Middle-Attacke* betreffend die erlangte, mutmaßliche MAC-Adresse

Falls Zugang zu dem von der Zielperson verwendeten AP besteht (wenn dieser unverschlüsselt ist) oder der Angreifer sich diesen verschafft, könnte im Anschluss zur weiteren Verifizierung und ersten Datensammlung durch *ARP-Poisoning* eine *Man-In-The-Middle-Attacke* durchgeführt werden, denn nun ist die mutmaßliche MAC-Adresse bekannt.

Im LAN sind nur MAC-Adressen relevant, während IP-Pakete an die IP-Zieladresse geliefert werden. Um eine Verknüpfung zwischen diesen beiden Adresstypen herzustellen, wird das *Address Resolution Protocol (ARP)* eingesetzt. Ein Netzwerkgerät, das ein IP-Paket abzuliefern hat, kann über ARP einfach alle Hosts im LAN fragen, welche MAC-Adresse zu dieser IP-Adresse gehört. Da die Antwort auf eine solche Anfrage nicht kryptographisch geschützt ist, kann ein im LAN sitzender Angreifer alle solchen Anfragen mit seiner eigenen MAC-Adresse beantworten. Dies bezeichnet man als *ARP Spoofing* oder *ARP-Poisoning*. Wenn er schnell genug ist, kann er so den gesamten IP-Verkehr im LAN über sich umleiten, da die zeitlich erste Antwort zählt. Der Angreifer kann so im LAN als *Man-in-the-middle* agieren, d. h. er schaltet sich einfach in die Leitung zwischen zwei Teilnehmer A und B, gibt sich A gegenüber als B, und B gegenüber als A aus, und kann so jegliche Netzwerkkommunikation mitlesen und auch verändern.[14]

Eine äußerst effektive Methode, um sehr schnell an persönliche Daten zu gelangen, stellt das im Rahmen einer Bachelorarbeit im Jahr 2011 realisierte Tool *DroidSheep*[15] von Andreas Koch dar. Es handelt sich dabei um eine Android-App, mit welcher sich Session-IDs, die u. a. von Amazon, Facebook und Google eingesetzt werden, abfangen lassen. Der Angreifer ist dadurch in der Lage, dem Server gegenüber die Identität des Opfers vor-

zutäuschen und Zugang zum Account zu erlangen, was als *Session Hijacking* bezeichnet wird. Dadurch wäre es möglich, die Personaldaten inklusive Kontaktlisten und Nachrichten in Erfahrung zu bringen.

Konkrete Nutzung dieser Verknüpfung zwischen realer Person und mobilem Gerät

Die Kenntnis über die Verknüpfung zwischen MAC-Adresse und Person könnte in weiterer Folge u. a. dafür genutzt werden, um sich beim Aufscheinen der betreffenden MAC-Adresse an einem bestimmten Ort, z. B. per E-Mail, über diesen Umstand informieren zu lassen. Damit sind unter Verwendung mehrerer dieser Detektoren (in anderen Quellen meist *Drohnen* genannt) die Voraussetzungen für Standortbestimmungen und Bewegungsprofile geschaffen.

Implementierung der MAC-Adressen-Alarmierung per E-Mail

Zur Umsetzung der E-Mail-Alarmierung wurde im Zuge dieser Arbeit nach einem Log-File-Überwachungsprogramm recherchiert, welches eine Blacklist (in unserem Fall bestehend aus MAC-Adressen) entgegen nehmen und darauf basierend eine Alarmierung durchführen kann. Das *Perl*-Programm *swatch*[16] alias *swatchdog* erfüllt diese Anforderungen. Nachdem das Hauptprogramm samt einiger anderer vorausgesetzter Programme (insbesondere *tail*) installiert wurde, muss eine Konfigurationsdatei erzeugt werden, welche folgenden textuellen Aufbau hat (*swatch* Konfigurationsdatei mit einem vollständigen Eintrag):

```
watchfor /C0:EE:FB:xx:xx:xx/
        echo=red
        mail addresses=xxx, subject=xxx
watchfor ...
```

watchfor / hier steht die gesuchte MAC-Adresse /
echo=red für die Terminalausgabe in der Farbe rot
mail addresses=xxx und subject=xxx für die Mailweiterleitung per *sendmail-Dienst*

Anmerkung: Im Betreff könnte z. B. der Name einer Drohne sowie einer Zielperson inklusive Angaben zum Standort untergebracht werden.

Wie bisher beschrieben, funktioniert die Ausgabe des Suchtreffers auf der Konsole ohne weitere Installations- und Konfigurationsarbeiten. Zur Umsetzung der E-Mail-Alarmierung muss jedoch zusätzlich ein Mail-Server auf dem Überwachungsgerät eingerichtet werden. Diesbezüglich eignet sich der Mail Transfer Agent *exim4*, welcher folgende Möglichkeiten bietet:

- Die IP-Adresse für eingehende SMTP-Verbindungen auf den *localhost 127.0.0.1* festzulegen und externe Verbindungsversuche abzulehnen – was aus sicherheitstechnischer Sicht sehr wünschenswert und für den beschriebenen Zweck perfekt geeignet ist.
- Die ausgehenden E-Mails über einen externen Mail-Server, z. B. von *Gmail*, an den Empfänger-Server weiterzuleiten.

Das Programm *exim4* ist mit der richtigen Anleitung[17] schnell installiert und konfiguriert. Problematisch ist lediglich, dass die Zugangsdaten zum Postfach des Mail-Providers im Klartext in einer Textdatei abgelegt werden müssen.

Im Zuge des ersten praktischen Versuchs ist aufgefallen, dass die E-Mails nicht unmittelbar versendet werden. Nach längerem Stöbern in der Konfiguration wurde festgestellt, dass der Standardwert für die E-Mail-Warteschlange 30 Minuten beträgt. Nach Abändern des Eintrages `QUEUEINTERVAL` auf `2s` (2 Sekunden) funktionierte dann alles wie gewünscht. In diesem Zusammenhang sind die Befehle `exim -bp` zum Anzeigen der Anzahl wartender E-Mails und `exim -qff` zum Leeren der Warteschlange sehr hilfreich. Beispiel einer Konsolenausgabe nach Ausführung von *swatchdog*:

```
root@kali: # swatchdog --config-file=/etc/swatch.conf
--tail-file=capture.csv --tail-args -f
*** swatchdog version 3.2.4 (pid:1903) started at Die
Mai 31 11:24:35 CEST 2016
C0:EE:FB:XX:XX:XX, 2016-05-28 16:31:38, 2016-05-28
17:08:34, -80, 100, (not associated) ,
```

Der tail-Befehl bekommt die vom Programm *airodump-ng*[18] erzeugte csv-Datei *capture* als Log-File übergeben (siehe dazu auch Abbildung 2).

Zuordnung eines bestimmten mobilen Geräts zu einer unbekannten Person

Bisher wurde beschrieben, wie es gelingen kann, eine bekannte Person mit ihrer digitalen/elektronischen Ausstrahlung zu verschmelzen. Nun wird der umgekehrte Fall erörtert: ob und wie anhand einer bekannten MAC-Adresse die dazugehörige, unbekannte Person eruiert werden kann. Dazu wird hauptsächlich auf die frei verfügbare Software *Snoopy-ng* im Zusammenspiel mit dem Analyse-Programm *Maltego* eingegangen und auf Wilkinson[7] Bezug genommen. Dieser bezeichnet die Ortung von Personen durch deren digitale/elektromagnetische Ausstrahlung als *Digital Terrestrial Tracking* (DTT) und deren digitale/elektronische Spur als *Digital Terrestrial Footprint* (DTF). Ihm gelingt es, in sehr anschaulicher Weise den Vergleich zwischen dem eindeutigen physikalischen und dem digitalen Profil zu ziehen – nachfolgend eine sinngemäße Übersetzung aus seiner Arbeit[7]:

> *Der Digital Terrestrische Fußabdruck (DTF) ist zwischen dem physikalischen und dem Online-Fußabdruck einzuordnen. Das physikalische Tracking von Personen bezieht sich auf deren biometrische Merkmale. Online-Tracking erfolgt über individuelle, digitale Netzwerkspuren wie u. a. IP-Adressen, Cookies, Social Media Accounts. Mit Digital Terrestrischem Tracking (DTT) ist die geografische Lokalisation einer Person, basierend auf der Ausstrahlung individueller Signaturen mitgeführter Geräte, gemeint.*

Mögliche Einsatzszenarien

Zum einen gibt es die bereits angesprochene Einsatzmöglichkeit zur Standortbestimmung von mobilen Geräten (welche sich beispielsweise auf einer hinterlegten Blacklist befinden könnten). Zum anderen wäre es auch denkbar, Orte mit Drohnen zu bestücken, an denen ein bislang noch unbekannter Täter schon mehrfach Straftaten begangen hat, von dem vermutet wird, dass er auch in Zukunft solche Straftaten ausführen wird. Scheint im Zeitraum der Tatausführungen immer wieder die gleiche MAC-Adresse (bestenfalls inklusive der präferierten SSIDs) auf, kann es über diesen Ansatzpunkt zur Ausmittlung der Täterschaft kommen. Beispielsweise ist damit die Überwachung einer bestimmten Örtlichkeit möglich, an welcher ein Sexualstraftäter wiederholt seine Übergriffe setzt.

Eine weitere Einsatzmöglichkeit besteht in der Überwachung von Konsumenten, welche sich z. B. innerhalb eines Einkaufszentrums befinden. Nebst dem aktuellen Aufenthaltsort könnte anhand der Bewegungsprofile unter Umständen sogar vorausgesagt werden, wohin sie sich bewegen.

Emissionen anderer Geräte

Aus Gründen der Übersichtlichkeit und der Gefahr des Abschweifens wurde bislang nicht auf den Umstand eingegangen, dass auch andere am Körper getragene Geräte über Technologien wie *Bluetooth* oder *NFC/RFID* Emissionen verursachen (z. B. ein Headset, ein Reisepass[19], eine Bankomatkarte oder ein Fitnessarmband). Auch diese Daten können natürlich erfasst werden, wobei deren Ausstrahlungsstärke teilweise massiv schwächer als bei der WLAN-Technologie ausfällt[7], siehe dazu Tabelle 1.

Gerät	Reichweite
Wi-Fi	bis zu 100 m
Bluetooth	ca. 50 m
RFID	10 cm bis 200 m
NFC	ca. 10 cm

Tabelle 1: Reichweite von Wi-Fi, Bluetooth, RFID und NFC

Snoopy-ng

Die Software *Snoopy-ng*[20] wurde im Jahre 2012 ursprünglich als Proof of Concept (PoC) auf der Security Conference *44CON* in London von zwei Mitarbeitern (Penetration Tester) der Cyber-Security-Firma *SensePost* (u. a. Glenn Wilkinson) vorgestellt. Snoopy-ng ist ein in der Programmiersprache *Python* geschriebenes Framework, welches dafür ausgelegt ist, möglichst viele Daten von am Körper getragenen Geräten zu sniffen bzw. zu snoopen.

Dabei kommt eine *Client-Server-Infrastruktur*[21] zum Einsatz. Die Clients werden *Drohnen* genannt, wobei es sich in der Regel um kleine elektronische Geräte mit diversen Sensoren handelt. Die Drohnen (z. B. ein adaptiertes Smartphone, ein Raspberry Pi, ein Laptop, …), mit der Client-Software bespielt, nehmen lediglich den Traffic entgegen und leiten ihn an einen analysierenden Server weiter bzw. führen Befehle (z. B. NMAP-Scan, Auslieferung von Malware, Modifikationen am Traffic) von diesem aus. Siehe dazu auch Abbildung 3.

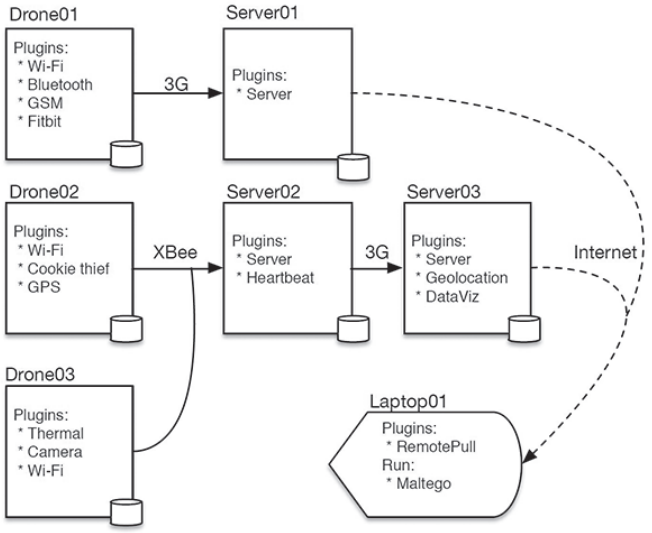


Abbildung 3: Mögliches Snoopy-Setup, bei welchem drei Drohnen ihre gesammelten Daten über unterschiedliche Technologien (3G und XBee) an zwei Server übertragen. Ein Client-Laptop ruft die Daten zum Zwecke der Auswertung bei diesen Servern ab. Pfeile mit durchgehenden Linien kennzeichnen einen **push** *(Auslieferung von Daten), während Pfeile mit gestrichelter Linie einen* **pull** *(Abholen von Daten) symbolisieren. © Glenn Wilkinson / SensePost 2014 [Ref. 7]*

Alternativ können die erfassten Daten jedoch auch in eine lokale Datenbank geschrieben werden, welche im Arbeitsverzeichnis unter der Bezeichnung *snoopy.db* abgelegt wird. Es handelt sich dabei standardmäßig um eine *SQLite*-Datenbank.

Den Opfern kann unter Vortäuschung unverschlüsselter, präferierter Netzwerke Zugriff auf das Internet gewährt werden, wobei der Server alle Daten aufzeichnet. Unter anderem sind folgende Features enthalten: *SSL Strip*, *Traffic-Inspektor* für *PDF* und *VoIP*, *Social Media Plugins* für z. B. Facebook.

In nachfolgender Textbox wird `Snoopy` mit dem WLAN-Plugin `wifi` auf Schnittstelle `mon0` unter der Bezeichnung `myDrone` und der Spezifizierung des Standortes *bregenz* gestartet:

```
root@kali: # snoopy -v -m wifi:iface=mon0 -d myDrone -l
bregenz
[+]Starting Snoopy with plugins: wifi
[+]Capturing local only.
Saving to 'sqlite:///snoopy.db' ...
```

Die dabei gespeicherten Daten können entweder über einen entsprechenden Datenbank-Viewer betrachtet oder mit Hilfe des Analysetools *Maltego* ausgewertet werden. Für das Programm *Maltego* ist im Programmpaket von *Snoopy-ng* ein Plugin (mit Symbolen) enthalten, welches die Datenbank-Aufzeichnung grafisch aufbereiten kann. Anhand der erlangten Information könnte auf die Identität der Zielperson geschlossen werden.

Abbildung 4 zeigt das Ergebnis einer von Wilkinson über das Programm *Maltego* durchgeführten Analyse hinsichtlich Stations, welche nach demselben Netzwerk mit der Bezeichnung *RBS-1-1111* suchen. Da dieser AP über die geografische Lokalisation der *Royal Bank of Scotland Branch*, Standort Liverpool Street zugeordnet werden konnte, könnte es sich bei den Besitzern der Stations um Arbeitskollegen handeln.

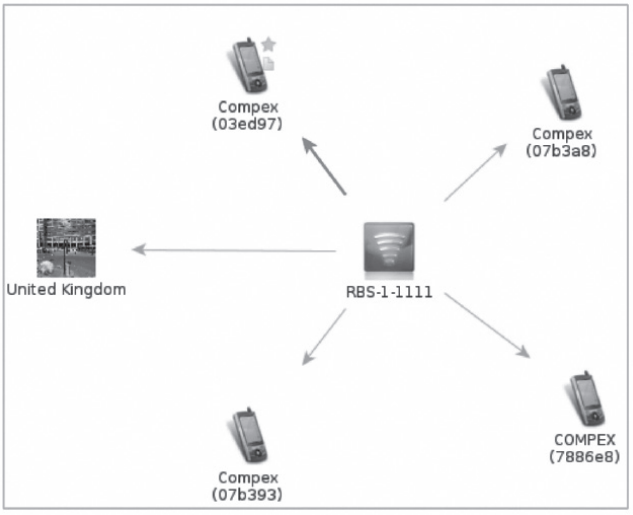


Abbildung 4: Maltego Snapshot – die als Mobiltelefon dargestellten Stations führen allesamt den AP **RBS-1-1111** *in ihrer Liste präferierter Netzwerke, welcher laut Wigle-Datenbank einem Geldinstitut in England zuzuordnen ist. © Glenn Wilkinson / SensePost 2014 [Ref. 7]*

Diskussion

Von uns allen am Körper getragene, elektronische Geräte können unsere geografische Lokation und darüber hinaus zahlreiche persönliche Informationen an einen Angreifer verraten. Sie ermöglichen es, nach erfolgreicher Zuordnung zwischen einer konkreten Person und der individuellen MAC-Adresse Bewegungsprofile zu erstellen und Standortbestimmungen durchzuführen.

Die Zuordnung zwischen Person und Gerät ist jedoch nicht unkritisch. Möglicherweise führt die Zielperson gar kein Smartphone mit sich. Oder die für den Angriff benötigten elektronischen Komponenten (z. B. der WLAN-Adapter) wurden von der Zielperson deaktiviert. Dadurch könnte es, speziell bei der vorgestellten Stalker-Attacke, zu einer falschen Zuordnung kommen. Denn hier wird lediglich die nach Verbindungszeit an erster Position gereihte MAC-Adresse als der Zielperson zurechenbar angenommen. Es wurde deshalb die Verifizierung der Zuordnung zwischen Zielperson und MAC-Adresse mittels Durchführung und Abgleich der Ergebnisse beider Angriffe und eventuell zusätzlicher Absicherung durch eine *Man-In-The-Middle*-Attacke angeregt.

Hinsichtlich der klassischen Handypeilung über den von der Zielperson verwendeten Betreiber hat das vorgestellte Verfahren hauptsächlich folgende zwei Nachteile:

1. Die Zuordnung zwischen Zielperson und Gerät ist beim vorgestellten Verfahren möglicherweise nicht mit Sicherheit zu klären. Der Telefonbetreiber knüpft die Information zur ausgelieferten SIM-Karte jedoch eindeutig an den Vertragspartner (eine mögliche Ausnahme sind Prepaid-SIM-Karten).
2. Den von uns vermutlich nur vereinzelt eingesetzten Drohnen steht ein flächendeckendes Netz an Mobilfunk-Sendemasten gegenüber, bei welchen sich der Kunde zumeist automatisch einbucht.

Dem können jedoch folgende Vorteile der vorgestellten Verfahren gegenübergestellt werden:

1. Die Veranlassung des Betreibers zur Handypeilung ist nur über staatliche Institutionen wie die Polizei möglich. Auf das Drohnen-Netzwerk (wie in Abbildung 3 gezeigt) hat dessen Administrator jederzeit und unbeschränkt Zugriff.

2. Das vorgestellte Verfahren beschränkt sich nicht nur auf die Standortdaten des Geräts und somit der Zielperson, sondern ermöglicht zusätzliche Informationsgewinnung in großem Umfang.

Dies kann zur Bekämpfung von Kriminalität und Terrorismus dienen oder aber auch für gezielte Werbung und kriminelle Zwecke missbraucht werden. Mit den vorgestellten Techniken, Gratis-Tools, günstiger Hardware und dem entsprechenden Know-how kann diese Überwachungs-Infrastruktur theoretisch durch jedermann realisiert werden. Die praktische Umsetzung des Verfahrens dürfte jedoch mit großem Aufwand für den Aufbau, die Verwaltung und Wartung verbunden sein.

Gegenmaßnahmen

Angriffe, die auf die WLAN-MAC-Adresse abzielen, können unter anderem teilweise verhindert werden durch

1. sich immer wieder ändernde MAC-Adressen,
2. das periodische Löschen von Listen präferierter Netzwerke oder
3. die Aussendung zufälliger Probe Requests zur Detektion von Replay-Angriffen.

Zu 1. und 2. hat der Programmierer Jorrit Jongma (bekannt unter dem Namen *Chainfire*) für Android das Tool *Pry-Fi*[22] entwickelt, welches nach einem pseudo-zufälligen Verfahren in kurzen zeitlichen Intervallen die MAC-Adresse ändern und abgespeicherte Listen präferierter Netzwerke löschen kann. Zu Punkt 3 beschreibt Thomas Kropeit[23] u. a. eine Methode zur Erkennung von Replay-Attacken. Er stellt fest, dass beim Senden einer zufällig generierten SSID lediglich eine Wahrscheinlichkeit von etwa 2^{-209} besteht, dass ein AP mittels Probe Response darauf antwortet. Es kann dadurch mit hoher Wahrscheinlichkeit festgestellt werden, ob gerade ein Replay-Angriff durchgeführt wird. Diese Gegenmaßnahmen werden jedoch durch folgende Umstände erschwert:

1. Ein Smartphone muss dazu im Falle von Android *gerootet*[24] sein. Änderungen, welche die MAC-Adresse betreffen, bedürfen der vollständigen Kontrolle über das Betriebssystem und dessen Ressourcen. Erfahrungsgemäß verfügt die große Masse der Nutzer jedoch nicht über die dafür erforderlichen Fertigkeiten. Außerdem könnte das *Rooten* zu Garantieverlust sowie zum *Bricken*[22] des Geräts führen; ein *Hardbrick* ist hierbei der schlimmste Fall und bedeutet, dass das Gerät komplett unbrauchbar ist und keine Möglichkeit der Reparatur mehr besteht.

2. Nicht alle Geräte erlauben ein Löschen der Netzwerklisten.

Fazit und Ausblick

Die Untersuchung der von mobilen Geräten ausgesendeten Signale zeigt, dass diese zur Gewinnung sensibler Daten verwertet werden können. Es ist dadurch möglich, Information zu einer bestimmten Person sowie über Menschenmassen zu sammeln. Die Zuordnung von eindeutigen Gerätenummern zu individuellen Personen kann mit den vorgestellten Techniken gelingen, ist jedoch keineswegs trivial.

Das ständige Mitführen gesprächiger mobiler Geräte wie Smartphones gefährdet daher die informationelle Selbstbestimmung. Dem Großteil der Bevölkerung fehlt das Wissen um die automatisiert geführte, kabellose Kommunikation und die Auswirkungen der am eigenen Gerät eingestellten (Standard-)Konfiguration. Dadurch werden die angesprochenen massiven Eingriffe in die Privatsphäre ermöglicht, welche nicht unter Kontrolle der Behörden/Gerichte oder an die Gesetze gebundener Konzerne wie Telefonbetreiber stehen. Aufbau und Einsatz einer autonomen Überwachungsinfrastruktur sind verhältnismäßig kostengünstig und unter Einsatz allgemein zugänglicher, freier Software realisierbar. Mit den vorgestellten Gegenmaßnahmen können sich Nutzer von betreffenden Endgeräten aber unter bestimmten Rahmenbedingungen dagegen schützen.

Die große Anzahl potentieller Opfer sowie die Möglichkeit, tief in den privaten Bereich gehende Information zu beschaffen, macht eine weitere Vertiefung dieses Themas, schon aus Gründen des Selbstschutzes, lohnenswert. Insbesondere möchte ich wesentlich mehr Erfahrungen im praktischen Umgang mit dem Framework Snoopy-ng und weiterer dafür verfügbarer Plugins für Sensoren wie Bluetooth und NFC sammeln. Auch die grafische Analyse mit dem Programm Maltego sowie der Aufbau eines größeren Snoopy-Setups mit mehreren, über Internet angebundenen Clients und Servern dürfte einige Herausforderungen mit sich bringen.

Referenzen

1 *Statistik Austria (2015) IKT-Einsatz in Haushalten. http://www.statistik.at*
2 *IEEE (2012) IEEE Standard for Information technology–Telecommunications and information exchange between systems–Local and metropolitan area networks–Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007), März 2012, S. 1–2793*
3 *Heise Online (2016) MAC-Adressen. Heise Netze, http://www.heise.de/netze/tools/mac/ (23.6.2016)*
4 *Cunche M, Kaafar MA, Boreli R (2013) Linking wireless devices using information contained in Wi-Fi probe requests. Pervasive and Mobile Computing 11(April 2014):56–69*
5 *http://www.aircrack-ng.org/*
6 *https://www.android.com/versions/jelly-bean-4-3/*
7 *Wilkinson G (2014) Digital terrestrial tracking: The future of surveillance. DefCon 22, Las Vegas, 7.-10.8.2014, https://www.defcon.org/images/defcon-22/dc-22-presentations/Wilkinson/DEFCON-22-Glenn-Wilkinson-GRW-WP.pdf*
8 *https://www.raspberrypi.org/*
9 *https://www.kali.org/kali-linux-nethunter/*
10 *Cunche M (2013) I know your MAC address: targeted tracking of individual using Wi-Fi. International Symposium on Research in Grey-Hat Hacking, Grenoble, Nov. 2013, https://hal.archives-ouvertes.fr/file/index/docid/858324/filename/Wi-Fi_Stalking.pdf*
11 *https://wigle.net/*
12 *Jäger S (2015) Wardriving – die unterschätzte Gefahr. FIfF-Kommunikation 2015(4):30–36, https://www.fiff.de/publikationen/fiff-kommunikation/fk-2015/fk-2015-4/fk-2015-4-content/fk-2015-4-p30*
13 *Golle P, Partridge K (2009) On the anonymity of home/work location pairs. Proc. 7th Int. Conf. on Pervasive Computing, S. 390–397, Springer-Verlag, Berlin, Heidelberg*
14 *Schwenk J (2014) Sicherheit und Kryptographie im Internet. Springer, Wiesbaden*
15 *http://droidsheep.de*
16 *https://sourceforge.net/projects/swatch/*
17 *https://wiki.debian.org/GmailAndExim4*
18 *http://www.aircrack-ng.org/doku.php?id=airodump-ng*
19 *Chothia T, Smirnov V (2010) A traceability attack against e-passports. In Sion R (eds) Financial cryptography and data security. Lecture Notes in Computer Science 6052, Springer, Berlin, Heidelberg, S. 20–34*
20 *https://github.com/sensepost/snoopy-ng*
21 *https://www.sensepost.com/blog/2014/release-the-hounds-snoopy-2.0/*
22 *http://forum.xda-developers.com/showthread.php?t=2631512*
23 *Kropeit T (2015) Don't trust open hotspots: Wi-Fi hacker detection and privacy protection via smartphone. Bachelorarbeit, Ruhr-Universität Bochum, 1.3.2015, https://www.emsec.rub.de/media/attachments/files/2015/03/BA_Kropeit.pdf*
24 *Cumplido T (2015) Android rooten – Vorteile, Nachteile und Cyanogen-Mod. Heise Download, 10.5.2015, https://www.heise.de/download/specials/Android-rooten-Vorteile-Nachteile-und-Cyanogen-Mod-3169058. Der Begriff Root kommt aus der Linux-Welt – Android basiert auf dem Linux-Kernel – und bezeichnet den Benutzer mit erhöhten System-Rechten, vergleichbar mit dem Admin-Konto unter Windows.*

Peter Wohlgenannt

Peter Wohlgenannt trat nach seinem Abitur und anschließendem Wehrdienst im Jahr 2000 der österreichischen Bundesgendarmerie bei. Im Anschluss an die Tätigkeit als Ermittler und Spurensicherer im Kriminaldienst wurde er im Jahr 2006 als Tatortbeamter beim Landeskriminalamt eingeteilt. In den letzten acht Jahren verschob sich sein Interesse hin zur Computerkriminalität, weshalb er ab 2009 als IT-Beweissicherer tätig war. Aktuell ist er stellvertretender Leiter der Kriminaltechnik und studiert seit 2014 im Rahmen des Projekts *Open Competence Center for Cyber Security* den Bachelorstudiengang Informatik/IT-Sicherheit an der Friedrich-Alexander-Universität in Erlangen-Nürnberg.

Hans-Jörg Kreowski

Cyberpeace-Forum

Am Freitag, dem 11. November 2016, von 18 bis 20 Uhr und am darauffolgenden Samstag von 14 bis 16 Uhr fand das Cyberpeace-Forum im Haus der Wissenschaft in der Bremer Innenstadt statt. Es war konzipiert als ein Bremer Beitrag zur Cyberpeace-Kampagne des FIfF zur Diskussion aktueller Entwicklungen zum Thema Cyberkrieg. Die Veranstaltung begann am Freitagabend mit einer Podiumsdiskussion anlässlich der Kooperation der Hochschule Bremen mit der Bundeswehr. Am Samstagnachmittag wurden aktuelle Entwicklungen und Gegenentwürfe zum Thema Cyber- und Drohnenkrieg vorgestellt und diskutiert. Beide Veranstaltungsteile waren mit je rund 80 Teilnehmenden passabel besucht. Das Publikum war gut gemischt: Jung und Alt, Frauen und Männer, viele Friedensbewegte, erstaunlich wenige mit direktem Informatikbezug.

Zu der Freitagsveranstaltung unter dem Motto *Zapfenstreich für die Zivilklausel?* wurde mit folgendem Text eingeladen:

> *Die Hochschule Bremen richtet mit Beginn des Wintersemesters 2016/17 einen dualen Studiengang für Informatikerinnen ein. Kooperationspartner hierfür ist die Bundeswehr. Erst 2012 hatte die Hochschule in ihrer Zivilklausel beschlossen: „Studium, Lehre und Forschung an der Hochschule Bremen dienen ausschließlich friedlichen Zwecken. Der Akademische Senat lehnt die Beteiligung von Wissenschaft und Forschung an Projekten mit militärischer Nutzung bzw. Zielsetzung ab […]". Die Entscheidung für die Kooperation mit der Bundeswehr hat innerhalb und außerhalb der Hochschule Bremen intensive Reaktionen und auch Protest ausgelöst. Droht eine Militarisierung der Bildung oder ist die Bundeswehr ein Kooperationspartner wie jeder andere? Auch bundesweit wird diese Entwicklung beobachtet und diskutiert. In der Podiumsdiskussion zwischen Vertreterinnen und Vertretern von Hochschulen, Politik, Gewerkschaften und Friedensbewegung soll das Für und Wider beleuchtet werden.*

Auf dem Podium saßen Susanne Grobien (Vorsitzende des Wissenschaftsausschusses der Bremischen Bürgerschaft), Hans-Jörg Kreowski (Universität Bremen und FIfF), Cornelia Mannewitz (Gewerkschaft Erziehung und Wissenschaft) und Axel Viereck (Hochschule Bremen, Konrektor Studium und Lehre). Die Diskussion wurde moderiert von Ralf E. Streibl in Vertretung von Tim Voss (Deutscher Gewerkschaftsbund Bremen-Elbe-Weser).

Zu der Vortrags- und Diskussionsveranstaltung am Samstag unter dem Motto *Aufrüstung zum Cyberkrieg* hieß es im Einladungstext:

> *Die Bundesministerin für Verteidigung Ursula von der Leyen hat im April angekündigt, in der Bundeswehr eine Organisationseinheit Cyber- und Informationsraum auf-*

Fotos von der Veranstaltung Hartmut Drewes

> *zubauen. Neben Land, Luft, Wasser und Weltraum wird damit ein fünftes Schlachtfeld offiziell eröffnet. Diese Maßnahme reiht sich ein in die weltweite Aufrüstung für den Cyberkrieg. Das bedroht vor allem auch zivile Infrastrukturen wie Strom- und Wasserversorgung, Verkehr, Gesundheitswesen und die Netzwerke von Staat und Wirtschaft in den Industriestaaten. Die nahezu täglichen Nachrichten über Cyber- und Drohnenangriffe zeigen, dass die Gefahr auch heute schon real ist. Aber auch die Kriegsgefahr allgemein wächst, weil Cyberwaffen vergleichsweise billig und einfach zu beschaffen und zu bedienen sind und weil die Schwelle, sie einzusetzen, eher niedrig ist. Es ist deshalb dringend erforderlich, sich der Gefahren des Cyberkriegs bewusst zu werden und ihnen friedliche Alternativen entgegenzusetzen.*

Es gab fünf kurze Impulsvorträge: *Cyberkrieg und Völkerrecht* von Rolf Gössner (Internationale Liga für Menschenrechte, Bremen), *Die Bundeswehr im Cyber- und Informationsraum* von Thomas Gruber (Informationsstelle Militarisierung, Tübingen), *Die Perversität autonomer Waffen* von Hans-Jörg Kreowski,

Hans-Jörg Kreowski

Hans-Jörg Kreowski ist Professor (i. R.) für *Theoretische Informatik* an der Universität Bremen und Vorstandsmitglied des *Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung*. Neben seinen fachlichen Schwerpunkten hat er seit vielen Jahren auch immer wieder zur unheilvollen Verflechtung von Informatik und Rüstung in Wort und Schrift Stellung genommen.

Techniken und Möglichkeiten digitaler Kriegsführung am Beispiel Stuxnet von Aaron Lye (Universität Bremen und FIfF) und *Wenn Big Data tödlich ist – Globale Überwachung und Drohnenkrieg* von Norbert Schepers (Rosa-Luxemburg-Stiftung, Bremen). Die Moderation hatten Eva Böller (Bremische Stiftung für Rüstungskonversion und Friedensforschung) und Barbara Heller (Bremer Friedensforum). Das Cyberpeace-Forum wurde organisiert vom Bremer Friedensforum, von der Bremischen Stiftung für Rüstungskonversion und Friedensforschung, vom Cyberpeace-Team Bremen, von der Bremer Regionalgruppe des FIfF und von der GEW Bremen. Die Podiumsdiskussion am Freitag wurde außerdem mitorganisiert vom DGB Bremen-Elbe-Weser. Die Veranstaltung wurde dankenswerterweise unterstützt von der Universität Bremen, der Hochschule Bremerhaven, dem AStA der Hochschule Bremen, dem Arbeitskreis Hochschulpolitik sowie vom Forum Friedenspsychologie.

Ich habe das Cyberpeace-Forum als Anregung zur Nachahmung relativ ausführlich beschrieben. Eine derartige Veranstaltung kann ein Publikum weit jenseits der an Informatik und Gesellschaft im engeren Sinne Interessierten erreichen und bietet die Chance zu Kooperationen mit Hochschuleinrichtungen, mit Gewerkschaften und mit Organisationen der Friedensbewegung. Im Falle des Cyberpeace-Teams Bremen wird die Kooperation auch fortgesetzt durch einzelne Veranstaltungen von April bis Juni 2017 mit dem Aufgreifen und Vertiefen der Vorträge von Norbert Schepers am 27. April und von Aaron Lye am 29. Juni sowie am 30. Mai mit einer Protestveranstaltung gegen die Konferenz und Messe *Undersea Defense Technology* in den Bremer Messehallen. Und im Herbst gibt es vielleicht das zweite Cyberpeace-Forum. Weitere Informationen lassen sich auf der Webseite *https://cyberpeace.fiff.de/Kampagne/CyberpeaceForum* finden. Insbesondere kann man dort auch Flyer und Plakat anschauen und das ziemlich beachtliche Medienecho nachvollziehen.

Von den fünf Vorträgen liegen drei in schriftlicher Fassung vor, die nachfolgend abgedruckt sind. Meinen eigenen Vortrag habe ich nicht verschriftlicht, weil ich auf der FIfFKon 2016 einen ganz ähnlichen Vortrag gehalten habe, der in der FIfF-Kommunikation 1/2017 nachzulesen ist.

Rolf Gössner

Cyberkrieg und Völkerrecht

Anlässlich der digitalen Aufrüstung der Bundeswehr im „Cyber- und Informationsraum"

Gegenwärtig wird die Bundeswehr mit einem neuen Kommando Cyber- und Informationsraum *aufgerüstet, das Anfang April 2017 in Dienst gestellt wurde – ergänzt von einem Forschungszentrum an der Bundeswehr-Universität in München.[1] Mit dieser digitalen Kampftruppe mit (geplant) fast 14.000 Dienstposten wird der „Cyber-Raum" zum potentiellen Kriegsgebiet erklärt, beteiligt sich die Bundesrepublik am globalen Wettrüsten im Cyberspace – bislang übrigens ohne Parlamentsbeteiligung, ohne demokratische Kontrolle und ohne gesetzliche Grundlagen.*

Diese Militarisierung des Internets und des gesamten Cyberraums dient nach Plänen des Bundesverteidigungsministeriums sowohl der Verteidigung gegen Cyberattacken von außen als auch eigener Cyberangriffe auf andere Staaten und deren IT-Systeme (laut *Geheimer Strategischer Leitlinie Cyber-Verteidigung* des Bundesverteidigungsministeriums von 2015).[2] Erstmals spielt im *Weißbuch zur Sicherheitspolitik 2016* der Krieg im Cyberraum eine gewichtige Rolle – inklusive Cyberkämpfer.innen.[3] Das bedeutet: Auch die Bundeswehr entwickelt Cyberwaffen, um in fremde IT-Systeme einbrechen und dort Manipulationen vornehmen oder diese zerstören zu können.

Schon jetzt existiert übrigens eine kleine, geheim agierende IT-Einheit in Rheinbach bei Bonn (*Computer Netzwerk Operationen*) mit 70/80 Soldaten, die für operative Maßnahmen zuständig ist. Diese Einheit wird nun erweitert und zusammen mit den bereits existierenden IT-Einheiten der Bundeswehr, etwa dem *Kommando Strategische Aufklärung,* in der neuen Organisationseinheit verschmolzen und zentralisiert. Darüber hinaus werden in großen Werbekampagnen neue IT-Fachleute angeworben.[4]

I. „Deutschlands Freiheit wird auch im Cyberraum verteidigt" *(Bundeswehr-Werbung)*

Wir haben es bei dieser digitalen Aufrüstung mit einer operativen Befähigung der Bundeswehr zu tun. Im Klartext: mit der Befähigung auch zur verdeckten Cyberkriegsführung im In- und Ausland – auch als Begleitmaßnahmen zu konventionellen Kriegseinsätzen der Bundeswehr im Ausland. Nicht allein militärische Ziele lassen sich damit treffen, sondern – zumindest als „Kollateralschäden" – auch zivile Infrastrukturen. Dies kann zu lang andauernden Ausfällen etwa der Strom- und Wasserversor-

gung, des Gesundheits- oder Verkehrswesens führen und damit die davon betroffene Zivilbevölkerung enorm schädigen.

Spätestens hier stellen sich dringliche Fragen nach der völkerrechtlichen Beurteilung und Regelung dieser Materie: Ab wann ist Cybergewalt zwischen Staaten völkerrechtswidrig, wann ist sie konventionellen bewaffneten Angriffen gleichzusetzen, wie den Urhebern zuzurechnen; inwieweit grenzen Regeln des Völkerrechts dieses digitale Schlachtfeld ein, ist all das überhaupt mit völkerrechtlichen Kategorien zu fassen und zu kontrollieren, oder müssen neue Regeln her – eine Art digitale Konvention? Diese Fragen sollen hier zumindest kursorisch behandelt werden, wobei wir uns im Klaren sein müssen, dass dieser völkerrechtliche Diskurs erst vor wenigen Jahren begonnen hat und noch in vollem Gange ist.

II. Völkerrecht und Menschenrechte gelten auch im Cyberspace und Cyberkrieg

Bislang reguliert und kontrolliert kein international verbindliches Abkommen die Aufrüstung im Cyberspace und den „Krieg der Zukunft". Aber so viel ist klar: Völkerrecht und Menschenrechte gelten auch hier – also auch das völkerrechtliche Gewaltverbot und das Recht zur angemessenen militärischen Selbstverteidigung gegen kriegerische Cyberangriffe von außen.[5]

Artikel 2 der UN-Charta untersagt den Staaten die *Androhung oder Anwendung von Gewalt.* Das bedeutet prinzipiell: Kriegsverbot zwischen Staaten und damit auch Verbot von Cyberkriegen. Jede zwischenstaatliche militärische Cyberoperation, die als Androhung oder Anwendung von Gewalt oder als Akt von *Cyber-Waffengewalt* definiert werden kann, stellt einen Völkerrechtsverstoß dar.

Doch nicht jeder Cyberangriff ist schon Cyberkrieg. Die meisten Cyberangriffe finden in Friedenszeiten statt und können grundsätzlich nicht als Kriegshandlung bezeichnet werden, auch wenn sie in feindlicher Absicht durchgeführt werden. Das gilt für Akte der digitalen Informationsmanipulation, Cyberkriminalität, Cyberspionage, Computersabotage und des Cyberterrorismus. In solchen – nicht-militärischen – Fällen von organisierter oder schwerer Kriminalität ist ein militärischer Gegenschlag zur Selbstverteidigung keinesfalls gerechtfertigt. Die Bekämpfung solcher Operationen unterfällt der nationalen „Inneren Sicherheit" und Rechtsprechung, weil es sich bei den Angreifern zumeist um Zivilpersonen, Organisationen, Firmen oder nichtmilitärische staatliche Institutionen handelt. Zuständig zur Sicherung, gezielten Abwehr und Ahndung mit angemessenen, nichtmilitärischen Gegenmaßnahmen sind hier: Nationales Cyber-Abwehrzentrum, Bundesamt für Sicherheit in der Informationstechnik (BSI), Geheimdienste, Bundes- und Länderpolizeibehörden sowie Staatsanwaltschaften/Bundesanwaltschaft und Justiz – die Bundeswehr nur dann, wenn es um Angriffe auf ihre eigene Militär-IT geht. Doch das Bundesverteidigungsministerium erhebt auch zum Schutz anderer staatlicher, kommunaler oder ziviler Netze den Anspruch der kooperativen Zuständigkeit der Bundeswehr für die „gesamtstaatliche Abwehr von Cyber-Angriffen" im Cyber-Raum – eine verfassungsrechtlich zumindest fragwürdige Zuständigkeit.

Wann handelt es sich demgegenüber um „Cyberkrieg", also um „bewaffnete Angriffe" oder um „Cyber-Waffengewalt"? Unter kriegerischen Cyberangriffen versteht man *militärische* IT-Attacken eines Staates auf computergestützte Systeme, kritische Infrastruktur und Netzwerke eines anderen Staates bzw. Landes, um in dessen Systeme einzudringen, diese – über Sicherheitslücken, Trojaner, Viren etc. – auszuspähen, zu manipulieren, zu schädigen, lahmzulegen oder zu zerstören. Angreifer und Angegriffene sind idealtypisch staatliche Akteure, deren Beziehungen durch das Völkerrecht geregelt werden.

Bislang gibt es jedoch keine völkerrechtliche Legal-Definition, wann ein (staatlicher) Cyberangriff als kriegerische Angriffshandlung gilt. Nach (noch) vorherrschender Auffassung in der juristischen Literatur liegt ein solcher Angriff nur dann vor, wenn die zerstörerischen Auswirkungen einer militärischen Cyberattacke mit denen konventioneller Waffengewalt vergleichbar sind – wenn also eine solche Attacke etwa Züge entgleisen, Flugzeuge abstürzen, Kraftwerke explodieren lässt und Menschen verletzt werden oder umkommen. Auch erhebliche Beschädigungen und Zerstörungen können ausreichen. Ob auch rein ökonomische Schädigungen genügen, ist umstritten. Insgesamt besteht aber die Gefahr, dass es aufgrund von Fehlinterpretationen zu verhängnisvollen militärischen Selbstverteidigungsschlägen und damit zu einer gefährlichen und folgenschweren Eskalation kommen kann.

Das Kriegsvölkerrecht beziehungsweise das humanitäre Völkerrecht – also das Recht zum Krieg und das Recht im Krieg – gelten auch im Fall des Cyberkriegs. Das Völkerrecht soll Kriege von vornherein verhindern oder nur in absoluten Ausnahmefällen zulassen, und das Humanitäre Völkerrecht verbietet – zum Schutz der Zivilbevölkerung – exzessive und unverhältnismäßige Handlungen im Kriegsfall.

So ist gemäß Genfer Konventionen verboten und als Kriegsverbrechen einzustufen, wenn ein Staat Cyberattacken gezielt gegen zivile Infrastrukturen (Strom, Wasser, Gesundheit etc.) eines anderen Staates führt und dadurch die Grundversorgung der Zivilbevölkerung unterbrochen oder nachhaltig gestört wird. Das gilt nicht für gezielte Cyberattacken gegen „rein" militärische IT- und Kommunikationssysteme. Problematisch dabei sind allerdings die möglichen, ja wahrscheinlichen *Kollateralschäden*, die bei vernetzten sowie Dual-Use-Systemen insbesondere die Zivilbevölkerung schwer treffen können. Digitale Waffen sind in

einer vernetzten Welt jedenfalls keine Präzisionswaffen, und die Streuwirkung kann immens sein.

III. Staatlich-militärische Reaktionen auf Cyberkriegshandlungen

Im Falle eines Cyberangriffs gegen einen Staat, der einem konventionellen bewaffneten Angriff gleichgesetzt werden kann, ist der angegriffene Staat nach Artikel 51 UN-Charta berechtigt, sein Recht auf angemessene Selbstverteidigung und Gefahrenabwehr auszuüben. Der angegriffene Staat darf dann gegenüber einem klar identifizierten Angreifer(staat) Selbstverteidigungsmaßnahmen im Cyberspace oder aber in der realen Welt durchführen. Die USA nehmen jedenfalls für sich in Anspruch, auch mit konventioneller militärischer Gewalt, also mit Raketen, Bomben und Granaten auf solche Cyberattacken zu reagieren.

Die Gegenmaßnahmen müssen zwar zur Abwehr des erlittenen, aber noch andauernden – also gegenwärtigen – Angriffs erforderlich und angemessen sein (Verhältnismäßigkeitsgrundsatz). Da die Streuwirkung eines Gegenangriffs jedoch immens sein kann, ist die Verhältnismäßigkeit von vornherein fraglich.

Da bewaffnete Auslandseinsätze der Bundeswehr dem sogenannten Parlamentsvorbehalt unterliegen, müsste ein solcher offensiver Cyber-Selbstverteidigungseinsatz der Bundeswehr im oder gegen das Ausland vom Bundestag genehmigt werden, genauso wie sonstige Kampfeinsätze im Ausland. Ob der Bundestag jedoch in der Lage ist, seine demokratische Kontrollfunktion vollumfänglich auszuüben und die Mittel und Folgen solcher Digitaleinsätze abzuschätzen, ist mehr als fraglich.

Ab wann und wie jeweils auf Cyberkriegsoperationen konkret reagiert werden soll, wird von Seiten der NATO und der Bundeswehr geheim gehalten, um „unberechenbar" zu bleiben und das Gegenschlagsrisiko unkalkulierbar zu machen (Abschreckungseffekt). Auch der UN-Sicherheitsrat könnte die Gewaltanwendung im Cyberspace oder Sanktionen als Gegenmaßnahme beschließen und ihren Vollzug delegieren. Und die NATO könnte den Bündnisfall erklären, sobald ein Mitglied angegriffen wird.

IV. Völkerrechtsrelevante Probleme bei der Beurteilung von Cyber-Operationen

1. Risiko einer Fehlzuordnung: Bei Cyberattacken und im Cyberkrieg gibt es keine Armeen, die sich gegenüberstehen und keine Soldaten in Uniform – stattdessen kommen etwa Viren, Würmer oder Trojaner verdeckt und häufig auf Umwegen zum Einsatz, also Software, die keine Uniform oder Staatsabzeichen trägt. Dabei lassen sich Datenspuren leicht manipulieren, verdecken oder anderen in die Schuhe schieben – um etwa unter falscher Flagge Konflikte zu schüren oder Kriegsgründe zu produzieren.

So ist einerseits nur schwer herauszufinden, ob es sich bei IT-Angriffen um zivil-kriminelle und wirtschaftliche oder um geheimdienstliche und militärische Operationen handelt. Andererseits hat der angegriffene Staat das Problem, die eigentlichen Urheber oder Angreifer zweifelsfrei zu identifizieren, um überhaupt rechtmäßig, angemessen und zielgenau durch die richtigen Institutionen reagieren bzw. sein Selbstverteidigungsrecht ausüben zu können. Hier besteht die Gefahr, dass es zu vorschnellen militärischen Selbstverteidigungsschlägen kommt – und damit zu einer gefährlichen und folgenschweren Eskalation. Die Beweisführung ist jedenfalls in aller Regel äußerst schwierig. Der Internationale Gerichtshof verlangt eine klare Beweislage, denn es gibt kein Recht auf Selbstverteidigung ins Blaue hinein oder aufgrund bloßer Indizien; ein Gegenschlag ohne klar identifizierbaren Aggressor ist völkerrechtswidrig.

2. Dual-Use-Problematik: Auch Cyber-Angriffe, die zielgenau nur auf militärische IT-Infrastrukturen gerichtet sind, können rasch zum Flächenbrand führen, wenn sie sich auf zivile Infrastrukturen ausbreiten, diese lahmlegen oder gar zerstören – etwa Energienetze, Kernkraftwerke, Wasserversorgung oder Krankenhäuser. Der Cyberraum kennt im Zeitalter digitaler Vernetzung und auch der gemischt zivil-militärischen Kooperation keine wirksamen Grenzen – weder nationale und geografische, noch physische oder technische. Dual-Use-IT-Objekte werden schon heute als legitime Ziele militärischer Angriffe gesehen – wobei ohnehin fast die gesamte Cyber-Infrastruktur dem Dual-Use dient, also sowohl zivil als auch militärisch genutzt wird, zumindest nutzbar ist.[6] Mit gravierenden Folgen für die Zivilgesellschaft.

V. Eskalationspotential durch Rechtsauslegung

Dieses technologische Eskalationspotential wird noch erhöht durch eine gefährliche Rechtsauslegung in einem NATO-Dokument, das völkerrechtliche Fragen des Cyberwars bislang am intensivsten behandelt: das *Tallinn Manual – ein Handbuch zur Anwendung des Völkerrechts auf die Cyberkriegsführung (von 2013)*. Zwanzig Rechtsexperten aus verschiedenen NATO-Staaten, auch Deutschland, haben diesen Leitfaden in Kooperation mit dem Internationalen Roten Kreuz und dem Cyber-Kommando der US-Armee erarbeitet. An den 95 Regeln sollen sich alle NATO-Staaten im Fall eines Cyberkriegs orientieren. Sie sind zwar rechtlich nicht bindend, aber richtungweisend.

Die Autoren stammen großteils aus dem Militär oder sind militärnahe Juristen – entsprechend militärfreundlich ist das Dokument auch ausgefallen. Und es offenbart eine *„sehr US-amerikanische Sicht auf das Völkerrecht"* (F. Delerue). So gelten danach selbst solche Operationen als Cyberwar-Angriffe, die bloße wirtschaftlich-finanzielle Schäden eines betroffenen Staates verursachen, wenn diese gewisse (katastrophische) Ausmaße annehmen, etwa ein Börsencrash. Dagegen wäre dann eine gewaltsame, auch konventionelle Selbstverteidigung rechtens, so der Leitfaden, was aber zu einer unkontrollierbaren Eskalation der Auseinandersetzungen führen könnte.

Das NATO-Tallinn-Manual sieht in Regel 15 zudem vor, dass ein Staat sein Recht auf Selbstverteidigung auch präventiv ausüben darf – also bevor überhaupt ein Angriff stattgefunden hat, dieser erst unmittelbar bevorsteht und nicht anders als durch Gewalt abwendbar scheint. Auch hier, wie bei konventionellen militärischen Erstschlägen, besteht hohe Missbrauchsgefahr und die Gefahr folgenreicher Eskalation.[7]

Laut Handbuch gelten zivile Hacker („Hacktivists“) als aktive Kriegsteilnehmer, wenn sie Cyber-Aktionen im Verlauf kriegerischer Konflikte ausführen; sie können daher angegriffen und getötet werden. Selbst das Suchen und Offenlegen von Schwachstellen in Computersystemen des Gegners gilt demnach als kriegerische Handlung. Auf diese Weise wird die Kampfzone praktisch auf Privatpersonen und deren Laptops ausgeweitet.

Auf Cyberangriffe mit konventioneller Waffengewalt antworten solle ein Staat jedoch nur dann, wenn die Attacken Menschenleben gekostet oder massive Schäden am Besitz eines Staates angerichtet hätten (Regel 22). Bei eigenen (Gegen-)Attacken soll besondere Rücksicht auf die Zivilbevölkerung genommen werden. Ebenso wie bei traditioneller Kriegsführung dürfen etwa Krankenhäuser und sonstige medizinische Einrichtungen im Falle eines Cyberkrieges nicht (gezielt) angegriffen werden.

Trotz solcher Einschränkungen: Mit der Eingriffsschwellen weit herabsenkenden Rechtsauslegung des NATO-Dokuments werden die Grenzen völkerrechtlich zulässiger Gewaltanwendung im Rahmen des Selbstverteidigungsrechts in problematischer Weise aufgeweicht. Was einflussreiche Völkerrechtler da an Regeln für die NATO zusammengestellt haben, ist geeignet, eine schwere Datenattacke blitzartig in einen echten Krieg mit Raketen, Bomben und Granaten eskalieren zu lassen.

VI. Gegen Aufrüstung und Militarisierung im Cyberbereich – für Ächtung des Cyberkriegs

Mit der Aufrüstung der Bundeswehr zum Cyberkrieg steigen Kriegsbereitschaft und Kriegsgefahr – und davor schützt auch die obligatorische Zustimmung des Bundestags im Einzelfall nur bedingt. Der militärische Einsatz von Cyberwaffen durch Staaten ist – auch wenn er „nur“ zur Selbstverteidigung erfolgt – eine Kriegshandlung mit enormem Eskalationspotential, die die internationale Sicherheit und die Zivilbevölkerung erheblich gefährdet. Das Cyber-Konzept der Bundesregierung für die Bundeswehr verwischt die Grenzen zwischen Krieg und Frieden, Angriff und Defensive, innerer und äußerer Sicherheit, zwischen staatlichen und nichtstaatlichen, militärischen und zivilen, kriminellen und politisch motivierten Angriffen und Zielen, Gegenmaßnahmen und Akteuren; es öffnet dem Missbrauch Tür und Tor und ist letztlich demokratisch kaum zu kontrollieren. Die Bestrebungen der NATO, die hohe Schwelle für einen bewaffneten Angriff herabzusenken sowie die restriktiven Kriterien des Selbstverteidigungsrechts weiter aufzuweichen, sind hochgefährlich. Denn all dies würde das völkerrechtliche Gewaltverbot untergraben und die internationalen Beziehungen gefährden.

Aus diesem Befund sind politische und rechtliche Konsequenzen zu ziehen:

1. Um eine unkontrollierbare Aufrüstungsspirale zu verhindern, müssen international verbindliche Konventionen und ein internationaler Verhaltenskodex geschaffen werden – eine Art Genfer Konvention für die Cyberwelt, mit dem Ziel, eine weitere Militarisierung des Cyberraums zu verhindern. Außerdem bedarf es eines effektiven Schutzes eigener IT-Infrastrukturen, und dazu gehört es, Schwachstellen zu identifizieren und Sicherheitslücken wirksam zu schließen.[8]

2. Auch militärische Cyberfähigkeiten sind auf rein defensive Maßnahmen – also auf Verteidigung – zu beschränken, um die Zivilbevölkerung effektiv zu schützen – flankiert von vertrauensbildenden Maßnahmen im Rahmen einer friedensorientierten Außenpolitik und Diplomatie (Stichwort: *Cyberpeace*). Dazu gehört auch ein striktes Verbot, Cyberattacken mit konventionellen Waffen zu beantworten.

3. Noch wichtiger wären darüber hinaus eine weltweite Rüstungskontrolle, Cyberabrüstung und die völkerrechtliche Ächtung von Cyberspionage und Cyberwaffen sowie

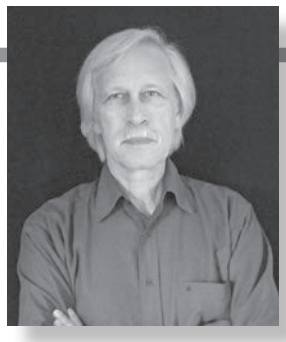
4. die Schaffung einer unabhängigen internationalen Instanz unter dem Dach der UN zur Untersuchung zwischenstaatlicher Cyberattacken und deren angemessener Abwehr.

Dieser Beitrag ist die überarbeitete Fassung eines Vortrags, den der Autor während des Cyberpeace-Forums am 12. Nov. 2016 im Bremer Haus der Wissenschaft gehalten hat.

Anmerkungen

1 Abschlussbericht Aufbaustab Cyber- und Informationsraum vom April 2016 sowie Dossier Cyber-Verteidigung, siehe Website des Bundesverteidigungsministeriums: https://www.bmvg.de

2 http://www.spiegel.de/politik/deutschland/bundesregierung-stellt-weissbuch-zur-sicherheitspolitik-vor-a-1102759.html ; https://netzpolitik.org/2016/weissbuch-zur-sicherheitspolitik-bundeswehr-geht-in-die-cyberoffensive/ ; https://netzpolitik.org/2015/geheime-cyber-



Rolf Gössner

Dr. **Rolf Gössner** ist Rechtsanwalt, Publizist und Vorstandsmitglied der *Internationalen Liga für Menschenrechte (www.ilmr.de)*. Seit 2007 stellv. Richter am Staatsgerichtshof der Freien Hansestadt Bremen. Sachverständiger in Gesetzgebungsverfahren des Bundestags und von Landtagen. Mitherausgeber des jährlich erscheinenden *Grundrechte-Report. Zur Lage der Bürger und Menschenrechte in Deutschland* (Fischer-TB). Mitglied in der Jury zur Verleihung des Negativpreises *BigBrotherAwards*. Autor und Herausgeber zahlreicher Bücher zum Thema *Innere Sicherheit und Bürgerrechte*, zuletzt: *Mutige Aufklärer im digitalen Zeitalter*, Ossietzky Verlag, Dähre 2015 sowie Gössner/Schuhler: *Terror. Wo er herrührt. Wozu er missbraucht wird. Wie er zu überwinden ist*, isw-spezial 29, München, Dez. 2016 *(www.isw-muenchen.de)*.

leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-digitale-angriffe/

3 https://www.heise.de/newsticker/meldung/Bundeswehr-Weissbuch-Planspiele-fuer-den-Krieg-im-Cyberraum-3270870.html m. w. N.

4 Die Bundeswehr sucht händeringend IT-Fachkräfte; auch an Hochschulen und Universitäten rekrutiert sie und entwickelt neue Karrierepfade. Plakataktion der Bundeswehr: „Deutschlands Freiheit wird auch im Cyberraum verteidigt", so lautet ein Slogan der Kampagne; vgl. Süddeutsche.de 2.4.2016.

5 http://www.spiegel.de/netzwelt/netzpolitik/ist-ein-cyberkrieg-ein-krieg-a-841096.html

6 Cordula Droege, Ist Cyberwar ein Krieg? In: Spiegel-online 2.7.2012.

7 Beispiel: der Computerwurm Stuxnet gegen das iranische Atomprogramm (2010) – gemäß Tallinn-Manual wäre dies als kriegerischer Akt zu werten, also als völkerrechtswidriger Angriffskrieg. Nicht aber, wenn dieser Angriff von den USA gestartet wird: Dann gilt der digitale Übergriff mit steuerndem Sabotage-Schadprogramm nur noch als „Akt der vorbeugenden Selbstverteidigung" gegen das iranische Atomprogramm, bevor damit Atomwaffen produziert werden können. (Die Urheberschaft von Stuxnet ist nicht eindeutig geklärt, es gibt aber starke Anhaltspunkte dafür, dass der Wurm eine Entwicklung des US-Geheimdienstes NSA in Zusammenarbeit mit Israel ist.) https://de.wikipedia.org/wiki/Stuxnet m. w. N.

8 Stattdessen werden aber IT-Sicherheitslücken, die für Cyberattacken nutzbar sind, als Angriffsoptionen offen und geheim gehalten, anstatt sie zum Schutz der eigenen Zivilbevölkerung aufzudecken und zu beseitigen. Auf diese Weise werden die Möglichkeiten zur Computerspionage und -kriminalität, zu Cyberterrorismus und -krieg gefördert.

Thomas Gruber

Onlineoffensive: Die Bundeswehr im Cyber- und Informationsraum

Die Gefährdung der Zivilgesellschaft durch Attacken im Cyberraum war im vergangenen Jahr ein äußerst präsentes Thema in der deutschen Presse. Die Angriffsszenarien reichten dabei von einer wirtschaftlichen Bedrohung durch „Hackerangriff[e] auf […] deutsche Banken"[1] bis hin zu einer existenziellen Gefahr für das Individuum „durch Cyber-Angriffe […] [auf] Krankenhäuser oder die Energieversorgung"[2]. Oft sind die Herkunft und die Intention der Attacken unbekannt – militärische Einheiten bestimmter Staaten oder Staatenbündnisse könnten geopolitische Interessen verfolgen, nationale Geheimdienste könnten Spionage betreiben oder kriminelle Organisationen könnten privatwirtschaftliche Akteur.innen anvisieren. Diese Unsicherheit eignet sich allerdings gut für den Aufbau und die Festigung von Feindbildern; die Sprache wird dabei suggestiver: „Warnung vor russischen Cyberattacken: Angriffsziel Deutschland"[3] oder „Massiver Hacker-Angriff auf Thyssen-Krupp – waren es Chinesen?"[4]

Bundeswehrstrukturen für den Cyberkrieg

Dieses Klima der Verunsicherung und der Bedrohung nutzen auch die Bundesregierung und das Bundesministerium für Verteidigung (BMVg), um die Ausweitung von militärischen Befugnissen im Cyberraum und die dementsprechende Aufrüstung der Bundeswehr zu rechtfertigen. Am 1. April 2017 ist die Struktur der Bundeswehr in diesem Zug um einen eigenen Organisationsbereich zum Cyber- und Informationsraum (CIR) gewachsen.[5] Das Kommando des CIR ist in Bonn Hardthöhe, dem Hauptsitz des BMVg, angesiedelt und befehligt 13.500 vorhandene Dienstposten. Die Aufgabenbereiche bestehen neben der Administration, Organisation und Bereitstellung von IT-Struktur vor allem in den verschiedenen Aspekten der Kriegsführung im Cyber- und Informationsraum. So fallen unter den neuen Organisationsbereich beispielsweise die psychologische Kriegsführung („operative Kommunikation"), die Störung feindlicher und Sicherung eigener Kommunikationsnetze („elektronische Kampfführung"), die Vernetzung und technische Ausstattung der Kriegseinheiten („Führungsunterstützung") sowie Angriff und Verteidigung im Cyberraum („Cyber-Operationen"). Neben den bereits bestehenden Stellen werden außerdem 300 neue geschaffen, von denen 230 auf die Führung des Organisationsbereiches, 40 auf den Fachbereich *Cybersicherheit* und 20 auf die Verbesserung von Cyber-Operationen entfallen.

Um die Funktionalität des neuen Organisationsbereiches gewährleisten zu können, fehlt der Bundeswehr allerdings vor allem eines: qualifiziertes Personal. Denn während der Verteidigungshaushalt jährlich immer großzügiger ausfällt, muss nach Wegfall der Wehrpflicht erheblich nachgeholfen werden, um das deutsche Militär als attraktiven Arbeitgeber darzustellen. Die Bundeswehr steigt mit riesigen Werbekampagnen, Kompromissbereitschaft und mit starkem Fokus auf ihre Zielgruppen in den Wettbewerb auf dem Arbeitsmarkt ein. Im Falle des Cyber- und Informationsraumes sind diese Bemühungen beispielsweise am Projekt *Digitale Kräfte* erkennbar, das mit 3,6 Millionen Euro Finanzierung[6] einen großen Teil der 12,5 Millionen Euro schweren Werbekampagne *Mach, was wirklich zählt*[7] der Bundeswehr ausmacht. Mithilfe von großflächigen Plakataktionen, Netzwerk-Sessions, auf Karrieremessen und in Jobcentern sollen IT-affine Personen, Gamer.innen und *Nerds*[8] für eine

Bundeswehr-Karriere begeistert werden. Dabei ist das Ziel, die Bundeswehr als moderne Arbeitgeberin mit Möglichkeiten zum Quereinstieg ohne starre Hierarchien darzustellen sowie das angehende Personal durch rührselige nationalistische Aussagen und gute Bezahlung ideologisch und finanziell an sich zu binden. Eine weitere Taktik der Nachwuchsgewinnung, die die Bundeswehr schon in anderen Fachbereichen erfolgreich einsetzt, ist die Anwerbung von Studierenden. An der Bundeswehruniversität München entsteht zu diesem Zweck beispielsweise der Masterstudiengang *Cyber-Sicherheit*, der ab 2018 jährlich 70 Absolvent.innen für eine anschließende Bundeswehrlaufbahn liefern soll.[9] In diesem Rahmen wird die Bundeswehruniversität um ein Forschungszentrum zur Cybersicherheit, 11 neue W3-Professuren und knapp 70 neue Stellen im Mittelbau und dem wissenschaftsstützenden Personal ergänzt. Neben der Neugewinnung von Personal sieht das BMVg außerdem die Gründung einer „Cyber-Reserve" vor, die aus ausscheidenden Berufs- und Zeitsoldat.innen, Freiwilligen Zivilist.innen oder Seiteneinsteiger.innen aus MINT-Berufen besteht und die Schlagkräftigkeit des CIR erhöhen soll.

Deutsche Strategien im Cyberkrieg und Darstellung in der Öffentlichkeit

Mit dem Organisationsbereich Cyber- und Informationsraum der Bundeswehr entsteht also ein neuer militärischer Akteur, der auf den deutschen Arbeitsmarkt drängt. Wie sieht aber die operative Strategie des CIR aus? Welche Einsatzgebiete gibt es? Die Aufgaben der deutschen Streitkräfte im Cyber- und Informationsraum werden in der öffentlichen Darstellung meist auf defensive Aktionen beschränkt – es gelte, der Verteidigung von „Staat, Wirtschaft und Gesellschaft" zu dienen. Zur Entwicklung wirksamer Verteidigungskonzepte müssten zwar auch Cyberattacken erforscht und verstanden werden, diese würden aber keinem Angriffszweck dienen. Sollte zur Landesverteidigung doch einmal eine offensive Nutzung der Cyber-Konzepte vonnöten sein, so seien diese laut Katrin Suder, der zuständigen Staatssekretärin des BMVg, wie jeder andere militärische Angriff der Bundeswehr auch durch ein Mandat des Bundestages zu legitimieren.[10] Diese Versuche, damit auch im Cyber- und Informationsraum über eine deutsche Politik der militärischen Zurückhaltung zu sprechen, wirken aufgrund der militärischen Strategiepapiere und des tatsächlichen Vorgehens von Bundeswehr und BMVg nahezu lächerlich. Während öffentlich ausufernd über das destruktive Potential von Cyberangriffen berichtet wird, die noch dazu nur schwer nachzuverfolgen sind, sind ebendiese Eigenschaften natürlich auch äußerst interessant für das deutsche Militär. Und so wird im Weißbuch der Bundeswehr 2016 zum Thema Cyber- und Informationsraum von „offensive[n] Hochwertfähigkeiten, die es zu beüben und weiterzuentwickeln gilt"[11] gesprochen. Wie diese „Hochwertfähigkeiten" verwendet werden, zeigt beispielsweise die seit kurzem bekannte Attacke der Gruppe *Computer Netzwerk Operationen*, die im CIR zukünftig im *Zentrum Cyber-Operationen* zu finden ist[12]: Bereits im Jahr 2015 attackierten deutsche Soldat.innen das afghanische Mobilfunknetz, um an Informationen zu einer Geiselnahme zu gelangen. Da dieser Einsatz weder ein Bundestagsmandat hatte, noch öffentlich gemacht wurde, ist zu vermuten, dass bei weitem nicht alle offensiven Cyberaktionen durch die vorgesehenen Kontrollinstanzen gehen.

Außer im Rahmen eines Militäreinsatzes soll die Bundeswehr auch verstärkt in die zivile Kommunikation eindringen. Im Abschlussbericht zum Aufbaustab des CIR ist diesbezüglich von einer verstärkten Zusammenarbeit des BMVg mit dem Bundesministerium des Inneren (BMI) die Rede, in deren Rahmen „gemeinsam ein neues Verständnis über die intensivere Kooperation und auch Beitragsfähigkeit der Bundeswehr […] auch in Friedenszeiten"[13] entwickelt werden soll. Nach den militärischen Publikationen ist außerdem der Begriff der Landesverteidigung ein äußerst biegsamer: So seien nicht nur militärische Attacken ein Grund für ein Eingreifen der Bundeswehr, sondern auch Wirtschaftsspionage oder Rekrutierungsbemühungen terroristischer Gruppierungen in sozialen Netzwerken. Gleichzeitig, so wird allerdings betont, sollen die sonst für solche Aufgaben zuständigen Polizeien und Geheimdienste nicht in ihren Kompetenzen beschnitten werden, sondern eine „Überlappung" mit den Arbeitsbereichen der Bundeswehr stattfinden. Der Trend der polizeilich-militärischen Zusammenarbeit im Cyberraum wird auch durch die Ansiedlung der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) auf dem Campus der Bundeswehruniversität in München verdeutlicht.[14] Die ZITiS ist eine Einrichtung, die das BMI mit Methoden der „digitalen Forensik, der Telekommunikationsüberwachung, der Kryptoanalyse (Dekryptierung), der Massendatenauswertung/Big-Data sowie […] technischen Fragen von Kriminalitätsbekämpfung, Gefahrenabwehr und Spionageabwehr"[15] unterstützen soll. Die Spionagebehörde und die militärische Hochschule sollen laut dem BMI eng kooperieren und perspektivisch sogar zusammenwachsen.

Bewertung und Bedeutung

Die Darstellung von Seiten des Staates und der Bundeswehr behandelt Cyberattacken auf staatliche Institutionen oder privatwirtschaftliche Unternehmen wie militärische Angriffe auf das eigene Land. So bekommen Probleme der IT-Sicherheit

Thomas Gruber

Thomas Gruber ist Mathematiker und promoviert an der Universität Bremen zum Thema *Verquickung mathematischer und informationstechnologischer Forschung an deutschen Forschungseinrichtungen mit der modernen Kriegsführung*. Er ist Stipendiat der *Rosa-Luxemburg-Stiftung* und Mitglied der *Informationsstelle Militarisierung* (IMI) in Tübingen.

oder allenfalls kriminelle Aktionen wie Wirtschaftsspionage und Eigentumsdelikte im Cyberraum schnell eine militärische Bedeutung.[16] Die Zivilgesellschaft wird dabei als zu schützendes Objekt vereinnahmt, um auf dieser Grundlage das bestehende Wirtschafts- und Herrschaftssystem im Cyberraum zu verteidigen. Zu diesem Zweck werden der Bundeswehr erhebliche finanzielle und personelle Kapazitäten sowie weitreichende Befugnisse im Cyber- und Informationsraum zur Verfügung gestellt. Da die Bundeswehr dabei in einem vorwiegend zivil genutzten Raum agiert, wird empfindlich in die digitale Privatsphäre einzelner Personen oder Personengruppen eingegriffen. So gerät die Zivilgesellschaft auch im virtuellen Raum zunehmend ins Kreuzfeuer staatlicher und militärischer Akteur.innen.

Die aktuellen Versuche, mit denen sich die Bundeswehr neben Polizeien und Geheimdiensten Verfügungsgewalt im Cyber- und Informationsraum verschaffen will, können als zusätzliches Alarmsignal für zivilgesellschaftliche Akteur.innen verstanden werden. Ob Privatpersonen, aktivistische Gruppen oder politische Vereinigungen – es gilt sowohl, eigene kritische Daten zu schützen, als auch den virtuellen Raum gegen staatlichen und militärischen Angriff zu verteidigen und wieder zivil zu vereinnahmen.

Referenzen

1 *Hackerangriff auf dreizehn deutsche Banken, faz.net, 5.1.2017*
2 *Die Bundeswehr sucht IT-Spezialisten für den Krieg im Cyberspace, sueddeutsche.de, 5.1.2017*
3 *Warnung vor russischen Cyberattacken: Angriffsziel Deutschland, tagesschau.de, 5.1.2017*
4 *Massiver Hacker-Angriff auf Thyssen-Krupp – waren es Chinesen?, derwesten.de, 5.1.2017*
5 *Kommando Cyber- und Informationsraum: Bundeswehr verteidigt die Freiheit – jetzt auch im Netz, heise.de, 3.4.2017; Abschlussbericht Aufbaustab Cyber- und Informationsraum, pdf, 5.1.2017*
6 *Folien CIR, pdf, 5.1.2017*
7 *„Mach, was wirklich zählt": So viel kostet die Bundeswehr-Werbung, fr-online.de, 5.1.2017*
8 *Abschlussbericht CIR, S. 32*
9 *Größtes Forschungszentrum für Cyber entsteht, unibw.de, 5.1.2017*
10 *Mandatierung, Attribution und offensive Fähigkeiten? Anhörung zur Bundeswehr im „Cyberraum", netzpolitik.org, 5.1.2017*
11 *Weißbuch der Bundeswehr 2016, pdf, S.93, 5.1.2017*
12 *Entführte Deutsche: Bundeswehr-Hacker knackten afghanisches Mobilfunknetz, spiegel.de, 5.1.2017*
13 *Abschlussbericht CIR, S. 37*
14 *Zivil-militärische Zusammenarbeit: ZITiS – Spionagebehörde des BMI zieht auf den Bundeswehr-Campus, imi-online.de, 3.4.2017*
15 *Startschuss für ZITiS, BMI, 3.4.2017*
16 *Kai Denker: Die Erfindung des Cyberwars, in: WeltTrends 113, S. 17–21*

Aaron Lye

Techniken und Möglichkeiten digitaler Kriegsführung am Beispiel Stuxnet

Der Computerwurm W32.Stuxnet, kurz Stuxnet, bekam weltweit von Analyst.innen, Forscher.innen, Hacker.innen, Medien und Politiker.innen in den Jahren 2010/2011, aber auch in den Folgejahren, große Aufmerksamkeit. Dieses lag daran, dass Stuxnet eine große und komplexe Bedrohung war und technisch einiges zu bieten hatte. Die Techniken und Möglichkeiten digitaler Kriegsführung sollen an diesem Beispiel verdeutlicht werden.

Technische Beschaffenheit von Stuxnet

Stuxnet ist ein Computerwurm, der sich in 32-Bit-Windowsnetzwerken verbreitet mit dem Ziel, eine spezielle Art von Anlagensteuerungssystemen der Firma Siemens – im Speziellen *SCADA Industrial Control Systems* – anzugreifen. Durch die Infektion des Steuerungsrechners war es dann möglich, auch auf *Programmable Logic Controllers* (PLC) zuzugreifen und diese umzuprogrammieren. Bei Stuxnet handelt es sich also um eine gezielte Attacke, die hochspezifisch für die Kompromittierung eines vorher genau spezifizierten Systems entwickelt wurde. Dies geht aus verschiedenen unabhängigen Analysen des Wurms hervor. Wesentliche Teile der technischen Analyse, bei der der Wurm *reverse-engineered* wurde, wurden gemeinsam von unterschiedlichen Unternehmen, wie Symantec und Microsoft, zusammen mit Einzelpersonen entwickelt, sind gut verstanden und der interessierten Öffentlichkeit zugänglich. Die Art und Beschaffenheit von Stuxnet, die Anzahl der Exploits und auch die Angriffe auf PLCs sind sehr ungewöhnlich. Ein PLC wird im Deutschen auch speicherprogrammierbare Steuerung (SPS) genannt und ist ein Digitalrechner zur Steuerung oder Regelung von Pumpen, Ventilen, Motoren oder im Allgemeinen von Maschinen oder Anlagen. Die Hardware ist üblich und wird weltweit in Millionen von Systemen verwendet. Die Einsatzgebiete erstrecken sich von Produktionsanlagen mit relativ simplen Steuerungen bis hin zur Steuerung von Robotern und Zentrifugen mit komplexen Abläufen, Kraftwerken (Kern, Kohle, Wasser, Wind), Mineralabbau, petrochemischer Industrie, Wasserwiederaufbereitung und Wassertransport, Zügen etc. Anzumerken ist, dass dieselbe Hardware sowohl in zivilen als auch in militärischen Anlagen benutzt wird.

Der Wurm lässt sich in zwei Teilen betrachten, die jeder für sich interessant sind. Der erste Teil ist die Infektion und Verbreitung des Wurms auf Betriebssystemebene; der zweite Teil ist die Infektion des PLC. Beide Teile sollen im Folgenden kurz erläutert werden. Details zu den Exploits sind beispielsweise in Symantecs Analyse[1] zu finden.

Für die Infektion und Verbreitung des Wurms auf Betriebssystemebene werden vier Zero-Day-Exploits genutzt. Ein Exploit ist ein Programm, das eine Sicherheitslücke ausnutzt, um nicht intendiertes Verhalten zu ermöglichen. Bei einem Zero-Day-Exploit ist die Sicherheitslücke nur wenigen bekannt bzw. existiert kein Patch, der diese Lücke schließt. Zwei dieser Exploits dienten dem Zugang und der Verbreitung. Die zwei anderen waren *Privilege Escalation Exploits* – dienten also dem Erlangen höherer Nutzerrechte.

Als Propagationsmethode verwendet der Wurm Wechseldatenträger wie USB-Sticks, des Weiteren Netzwerkdrucker und gemeinsame Verzeichnisse. Der erste Exploit ermöglicht, dass der Wurm automatisch beim Laden des USB-Sticks ausgeführt wird, wobei sich der Wurm allerdings nach drei Infektionen automatisch vom USB-Stick löscht. Der zweite Exploit nutzt einen Fehler im Rechtesystem von gemeinsam genutzten Druckern unter Windows-XP aus und kann so beliebige Dateien auf dem Zielsystem schreiben.[1] Anzumerken ist, dass sich der Wurm durch diese beiden Methoden nur lokal verbreiten kann. Es ist beachtlich, dass sich Stuxnet so weit verbreitet hat.

Außerdem ist interessant, dass zwei Privilege Escalation Exploits verwendet wurden, um sowohl Windows-2000-Systeme als auch -Vista und Folgesysteme anzugreifen. So funktioniert der Wurm auf einer Reihe von 32-Bit-Windows-Betriebssystemen: Win2k, XP, 2003, Vista, Server 2008, Win7, Server 2008 R2. Er nutzt die erweiterten Rechte von Antivirenprogrammen offensiv, indem er je nach installiertem Programm unterschiedliche infizierte dynamisch gelinkte Bibliotheken (DLLs) in das System injiziert.[1] So kann sich der Wurm an einen vertrauenswürdigen Prozess hängen.

Außerdem kann Stuxnet auch beim Starten des Betriebssystems geladen werden.[1] Dafür nutzt er einen digital signierten Treiber mit gestohlenem Zertifikat. Der signierte Treiber half, ein *Kernel Mode Rootkit* zu installieren, ohne dass der Nutzer darüber benachrichtigt wird, um länger unerkannt zu bleiben.

Ebenfalls kann der Wurm eine Verbindung zu einem Command-and-Control-Server aufbauen, die Konfiguration des Systems übermitteln und Updates herunterladen. Dabei umgeht er viele Firewalls und Intrusion-Detection-Systeme, da die Kommunikation auf HTTP basiert und wie normale Webseitenanfragen aussieht. Die Konfiguration des Systems wird dabei als Argument der Anfrage übergeben. Er kann sich aber auch lokal durch eine neue Infektion aktualisieren.[1]

Einem Mitarbeiter von Microsoft gemäß, der sich ebenfalls mit dem Wurm beschäftigt hat, waren zwei der vier Zero-Day-Exploits allerdings seit Jahren (mehr oder weniger) bekannt. Die Sicherheitslücke der Wechseldatenträger zum Ausführen von beliebigem Code mit den angemeldeten Nutzerrechten war 2011 schon seit sieben Jahren bekannt. Da die beiden Sicherheitslücken aber nicht oft ausgenutzt wurden, wurden sie von Microsoft nicht durch einen Security-Patch gefixt, was nach Stuxnet allerdings nachgeholt wurde.[2]

Der PLC war das eigentliche Ziel. Zunächst scannt Stuxnet das infizierte System, um die Systemkonfiguration zu analysieren. Siemens Step-7-Software oder WinCC, die üblicherweise zur Wartung von PLCs verwendet werden, muss installiert sein. Falls die Software vorliegt, werden mit Schadcode infizierte DLLs injiziert, über die der Wurm mit dem PLC kommuniziert. Außerdem muss eine Verbindung zu einem PLC mit spezifischen CPUs vorhanden sein. Nur dann wird der Wurm aktiv.[1]

By Starkus01 (Own work), CC BY-SA 4.0

Aus der Analyse des Wurms geht hervor, dass er nach niedrigharmonischen Frequenzumrichtern *(low-harmonic Frequency Converter Drives)* der Unternehmen Vacon (Finnland) und Fararo Paya (Iran) suchte, und zwar anhand eines 16-Bit-Wortes, mit dem Geräte identifiziert werden, die am Profibus des PLC angeschlossen sind.[3] Diese Frequenzumrichter, die von den PLCs gesteuert werden, steuern wiederum die Geschwindigkeit eines anderen Geräts, wie beispielsweise eines Motors. (Anmerkung: Diese Art von Frequenzumrichtern sind in vielen Ländern exportbeschränkt; in den USA sind beispielsweise Frequenzumrichter über 600 Hz von der U.S. Nuclear Regulatory Commission exportbeschränkt, da sie sich für die Urananreicherung nutzen lassen.[4])

Stuxnet hatte zwei Payloads für die PLCs: Der erste veränderte die Rotationsgeschwindigkeit des Motors, um das angetriebene Gerät zu beschädigen. Iterativ wird die Geschwindigkeit in kurzen Abständen von 1410 Hz auf 2 Hz und dann wieder auf 1064 Hz gesetzt. Die normale Frequenz liegt zwischen 807 und 1210 Hz. Der zweite war eine Art *Man-in-the-Middle-Attack*, um die Aktion des ersten Payloads zu verstecken, indem normales Verhalten vorgetäuscht wird. Dafür zeichnete es die Kommunikation zwischen PLC und Steuerungsrechner auf und sendete diese Daten anstatt den tatsächlichen, während es die modifizierten Operationen des PLC ausführte (nach Mikko Hypponen, Chief-Research-Officer, F-Secure[5]).

Einordnung

Das eigentliche Ziel von Stuxnet war also nicht die Infektion von Millionen von Systemen, sondern die Zerstörung eines vorher genau spezifizierten Systems. Der Wurm wurde am 17. Juni 2010 von Sergey Ulasen, Leiter des russischen IT-Security-Unternehmens VirusBlokAda, entdeckt, als er über ein ungewöhnliches

Problem auf Rechnern informiert wurde, die im Zusammenhang mit dem Iranischen Atomprogramm stehen.[5] Die Umstände seines Auftretens im Zusammenhang mit Anlagen des iranischen Atomprogramms, der primäre Offline-Verbreitungsweg und der extrem hohe Aufwand zur Programmierung des Wurms legten den Schluss nahe, dass Stuxnet eine gezielte Attacke auf das iranische Atomprogramm war.[6] Wahrscheinliches Ziel war die Urananreicherungsanlage in Natanz, Iran.[5] Aber auch in China waren mehrere Millionen Systeme infiziert.[6] Allerdings hat im November 2010 der damalige iranische Präsident Ahmadinejad öffentlich zugegeben, dass ein Angriff auf die Zentrifugen der Anlage stattfand.[5] Laut Symantec erfolgte der Angriff in drei Wellen mit drei leicht geänderten Varianten des Wurms.[1]

Durch die Anzahl an Exploits und die Vielzahl an Möglichkeiten, durch die sich der Wurm verbreiten und seine Schadroutinen ausführen konnte, lässt sich schließen, dass die Angreifer eine hohe Infektionsrate beabsichtigt haben. Es ist außerdem davon auszugehen, dass die Komponenten des Wurms von unterschiedlichen Personen entwickelt wurden und dann in ein gemeinsames Framework gefügt wurden.[6] Hier ist auch die Zuverlässigkeit des Wurms bemerkenswert. Die Angreifer zielten auf 100 %ige Zuverlässigkeit. So funktionieren die Exploits und Rootkits nicht probabilistisch – sie hätten damit auch zu Fehlern führen können, die das System zum Absturz gebracht hätten –, sondern exakt und wie bereits angemerkt mit einem hohen Wirkungsgrad.

Die Angreifer mussten eingehende Kenntnisse gehabt haben und auch die Möglichkeit, die Angriffe in realen Systemen zu testen.[6] Das heißt, sie mussten die Rechner- und Netzwerkarchitektur relativ gut kennen; wichtiger ist aber die genaue Spezifikation der Zentrifugen, um diese tatsächlich zu zerstören. Diese Informationen wurden wahrscheinlich durch Geheimdienste beschafft. Anzumerken ist, dass weltweit in Urananreicherungsanlagen zwar zum Teil unterschiedliche Hardware eingesetzt wird, der Prozess zur Urananreicherung aber überall derselbe ist (nach Olli Heinonen, *International Atomic Energy Agency*).[3] Diese Kenntnisse waren aber offensichtlich vorhanden, da beispielsweise die genaue Anzahl der Zentrifugen im Quellcode einprogrammiert wurde. So berichtet der Control-System-Security-Consultant Ralph Langner[7,8], dass es sechs Gruppen von Zentrifugen gab, wobei jede Gruppe aus 164 Einträgen bestand. Diese Zahlen stehen im Quellcode und sind in öffentlich zugänglichem Bildmaterial zu finden. Es ist also anzunehmen, dass den Angreifern die Hardware zur Evaluation der Schadensroutinen zur Verfügung stand, da Testen durch reine Simulation hier extrem unwahrscheinlich ist.[6,8] Dadurch sind erhebliche Kosten entstanden. Da es sich aber um Standard-Hardware handelt, ist das Beschaffen ohne Weiteres möglich.

Stuxnet selbst ist vollkommen konstruiert und auch aus den Command-and-Control-Servern lässt sich nichts folgern – es gibt aus technischer Sicht keine Indizien, wer hinter dem Angriff steckt. Folglich ist so keine sichere Attribution möglich. Die oben ausgeführten Indikatoren wie Komplexität und Kosten sind starke Indizien für staatliches Mitwirken.

Die am weitesten verbreitete Theorie, wer hinter diesem Angriff steckt, wurde vor allem durch den Autor David Sanger propagiert. Er ist der Washington-Korrespondent der *New York Times* sowie National-Security-Korrespondent und schrieb in dem 2012 erschienenen Buch *Confront and Conceal* über Stuxnet. Laut Sanger wurde Stuxnet vom US-Geheimdienst NSA gemeinsam mit einer geheimen israelischen Einheit entwickelt.[9,10,11] Seine Darstellung basiere auf in 18 Monaten geführten Interviews mit gegenwärtigen und ehemaligen amerikanischen, europäischen und israelischen Beamten, die in das Programm involviert gewesen sein sollen. Keine der Quellen wird namentlich genannt und weite Teile des Programms seien „bis heute streng geheim“[11]. Es gab allerdings nie öffentlich einen stichhaltigen Beweis, Israel oder die USA mit Stuxnet in Verbindung zu bringen, weder Israel noch die USA haben offiziell zugegeben, in irgendeiner Weise in die Entwicklung oder Verbreitung von Stuxnet involviert gewesen zu sein. Die *New York Times* berichtete,[10] dass Stuxnet Teil einer größeren Operation mit dem Namen *Olympic Games* sei. Später berichtete die *Washington Post*[12], dass die Malware mit dem Namen *Flame* ebenfalls Teil dieser Operation sei. Nach der Analyse des Codes berichtete *Kaspersky Lab*, dass es eine starke Beziehung zwischen Stuxnet und Flame gibt.[13]

2016 veröffentlichte Alex Gibney eine Dokumentation über Stuxnet mit dem Titel *Zero Days*[3]. Hier wird die gleiche Argumentation geführt. Im Film werden mindestens fünf geheime US-Militär- oder Geheimdienstquellen mit direktem Wissen von den Programmen und Operationen zitiert. Um die Identität zu verbergen, werden sie als „NSA Source“ zusammengefasst. Diese fiktive Quelle gibt zu, dass die NSA an Stuxnet beteiligt war und dass es sich um eine große internationale Operation handelt, bei der viele Militärs und Geheimdienstorganisationen beteiligt waren. Von US-Seite waren die USA Geheimdienste CIA und NSA wie auch das Military Cyber Command beteiligt. Der britische Geheimdienst GCHQ war für die Aufklärung zuständig. An anderer Stelle heißt es, er sei auch für das Deployment des Angriffes gegen die iranischen Anlagen zuständig gewesen. Der wesentliche Teil wurde allerdings von Israel durchgeführt. So war der israelische Auslandsgeheimdienst Mossad beteiligt und der technische Teil wurde von einer Einheit mit dem Namen *Unit 8200* durchgeführt. Durch die Ansiedlung des Cyber Commands beim Militär hat es die Autorität, solche Waffen zu entwickeln. Michael Hayden, der ehemalige Direktor der NSA und auch der CIA, hat es wie folgt kommentiert: „The NSA has the ability to do these things; Cyber-Command has the authority to do these things“.[3] Anzumerken ist, dass das *U.S. Cyber Command* in demselben Gebäude wie die NSA sitzt und die Zusammenarbeit äußerst eng ist. Es wird behauptet, dass Israel den Wurm vor dem Deployment modifiziert hat, um die Iranischen Atomanlagen anzugreifen. Sie machten ihn viel aggressiver im Vergleich zur vorherigen Version. Diese Version wurde dann eigenmächtig ausgeliefert und später von Security-Forschern entdeckt und analysiert.

Stuxnet sei aber auch im Zusammenhang mit der Operation NITRO ZEUS zu sehen. Im Film werden dazu folgende Behauptungen aufgestellt:[3] Die Operationen unter NITRO ZEUS beinhalten als Ziel Irans Industrieanlagen, Command-and-Control, Luftverteidigung, Transportwesen, aber auch das Stromnetz. Die Quellen behaupten, dass in NITRO ZEUS Hunderte von Personen über mehrere Jahre involviert waren und es schon Hunderte von Millionen Dollar gekostet hat. Das Ziel sei stören, abwarten und zerstören (*disrupt, degrade and destroy*) iranischer Infrastruktur mit Code, der keine Beweise liefert, wer für die An-

griffe verantwortlich ist. US-Hacker, die im Remote Operations Center (ROC) in Fort Meade, Maryland, USA, arbeiten, haben große Teile von Irans kritischer Infrastruktur unter ihre Kontrolle gebracht und sind in der Situation, diese jederzeit, beispielsweise zeitgleich mit militärischen Operationen, herunterfahren zu können. Im Film heißt es aber auch, dass es innerhalb des U.S. State Department und der NSA Menschen gibt, die diese Operation, also die Deaktivierung von ziviler als auch militärischer Infrastruktur, legal und ethisch bedenklich finden.

Diese Darstellung klingt plausibel. Andererseits ist diese Behauptung, die rein auf Interviews basiert, ohne jeglichen Beweis auch sehr zweifelhaft. Zwar ist spätestens durch die Enthüllungen von Edward Snowden bekannt, dass die NSA massiv an der Entwicklung von Exploits arbeitet, aber es sollte jeder/m auch klar sein, dass das Knowhow weltweit verfügbar ist und mindestens alle Industrieländer massiv an offensiven Waffen arbeiten. Die Komplexität und Kosten für Malware, die mit Stuxnet vergleichbar ist, sind zwar für die meisten Angreifer unrealistisch, für Nationalstaaten ist dieses aber keineswegs der Fall: Diese Waffen sind vergleichsweise günstig.

Fazit

Nationalstaaten haben die Ressourcen und das Know-how, um sowohl zivile als auch militärische Infrastruktur durch Schadsoftware anzugreifen und gegebenenfalls auch zu zerstören. Wahrscheinlich war Stuxnet der erste Fall, bei dem das auf einem hohen technischen Niveau passiert ist.

Weil die Attribution so schwierig bzw. oft unmöglich ist, wird bei der Suche nach den Verursachern oft nach dem Prinzip des *cui bono* (w*em zum Vorteil?)* verfahren. Diese Argumentation ist äußerst problematisch, da bestimmte Ereignisse sich aus unterschiedlichsten Gründen für unterschiedliche Akteure zum Vorteil entwickeln können. Oft werden Angriffe politisch instrumentalisiert, ohne dass eine klare Attribution gegen die Gegner möglich ist. Oft wird dabei wie folgt verfahren: Aus einer schwachen Argumentation beim ersten Fund wird ein leichter Verdacht beim zweiten Fund und ein erhärteter Verdacht beim dritten Fund, obwohl zu keinem Zeitpunkt echte Beweise vorliegen. Metadaten sind nachträglich fälschbar und echte Profis würden die Informationen nicht in der Malware mit ausliefern. Der Punkt ist aber: Aus Indizien werden – auch durch die Medien – Fakten. Deshalb bleibt es wichtig, die offensiven Fähigkeiten auf unterschiedlichen Ebenen genau zu analysieren. Das umfasst sowohl technische Analysen, um fundierte Kenntnisse und Beweise zu liefern, als auch strukturelle Analysen zu Gesetzesänderungen, dem Ausbau von Streitkräften, Hochrüsten von Geheimdiensten und Militärs, etc. Wichtig bleibt auch, Infrastrukturen und Rechte von Journalist.innen und Medien aufrecht zu halten, damit Whistleblower sicher Dokumente befreien können, um Licht ins Dunkel zu bringen.

Referenzen

1 *Falliere N, O'Murchu L, Chien E (2011) W32.Stuxnet Dossier. Symantec Security Response, Version 1.4, Feb. 2011, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf*

2 *Dang B, Ferrie P (2010) Adventures in analyzing Stuxnet, 27. Chaos Communication Congress (27c3), https://media.ccc.de/v/27c3-4245-en-adventures_in_analyzing_stuxnet*

3 *Gibnez A (2016) Zero Days. Dokumentation*

4 *Halliday J (2010) Stuxnet worm is aimed to sabotage Iran's nuclear ambition, new research shows. The Guardian, 16.11.2010, https://www.theguardian.com/technology/2010/nov/16/stuxnet-worm-iran-nuclear*

5 *Hammersley B (2014) Cybercrimes Episode 5: Cyber War. BBC News, Reportage*

6 *Gaycken S (2011) Cyberwar*

7 *Langner R (2013) To kill a centrifuge: A technical analysis of what Stuxnet's creators tried to achieve. The Langner Group, Nov. 2013, https://www.langner.com/wp-content/uploads/2017/04/To-kill-a-centrifuge.pdf*

8 *Langner R (2012) Stuxnet attack code deep dive. SCADA Security Scientific Symposium, https://www.youtube.com/watch?v=zBjmm48zwQU*

9 *Sanger DE (2012) Confront and conceal: Obama's secret wars and surprising use of American power. Crown*

10 *Sanger DE (2012) Obama order sped up wave of cyberattacks against Iran. The New York Times, 1.6.2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1&hp&pagewanted=all*

11 *Stöcker C (2012) Enthüllung über Stuxnet-Virus: Obamas Cyber-Angriff auf Irans Atomanlagen. Spiegel Online, 1.6.2012, http://www.spiegel.de/netzwelt/netzpolitik/usa-und-israel-sollen-stuxnet-virus-gegen-iran-entwickelt-haben-a-836401.htm*

12 *Nakashima E, Miller G, Tate J (2012) U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say. The Washington Post, 19.6.2012, http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html*

13 *Kaspersky Lab (2012) Resource 207: Kaspersky Lab Research proves that Stuxnet and Flame developers are connected. Press Release, 11.6.2012, http://newsroom.kaspersky.eu/fileadmin/user_upload/en/Images/Lifestyle/20120611_Kaspersky_Lab_Press_Release_Flame_Stuxnet_cooperation_final_-_UK.pdf*

Aaron Lye

Aaron Lye ist Informatiker und wissenschaftlicher Mitarbeiter in der Arbeitsgruppe *Technische Informatik und IT-Sicherheit* an der Universität Bremen. Darüber hinaus engagiert er sich im Bereich Kriegsführung, Überwachung und Repression durch Informationstechnik unter anderem im FIfF.

Humanistische Union e. V. u. a. – Gemeinsame Pressemitteilung von Verlag und Redaktion

Grundrechte-Report 2017

„Sicherheit bedeutet Gefahr – jedenfalls für die Grundrechte“

23. Mai 2017 – Am Verfassungstag, dem 23. Mai 2017, stellen in Karlsruhe acht deutsche Bürger- und Menschenrechtsorganisationen den neuen Grundrechte-Report vor. Der Bericht listet in 41 Beiträgen verschiedener Autor/innen die Defizite (und einen kleinen Fortschritt) in der Anerkennung und Durchsetzung einzelner Grundrechte in Deutschland auf. Zu den Themen des Grundrechte-Reports zählen die zahlreichen „Verschlimmbesserungen“ in der Anerkennung bzw. **Abweisung von Geflüchteten,** die der Gesetzgeber nach dem kurzen „Sommer der Migration“ in Gang setzte, ebenso wie **diskriminierende Praktiken** aufgrund des Geschlechts, der Rasse, Herkunft oder anderer Merkmale. Einen breiten Raum nehmen auch die zahlreichen neuen gesetzlichen Beschränkungen des Rechts auf informationelle Selbstbestimmung, des Post- und Fernmeldegeheimnisses sowie rechtsstaatlicher Grundprinzipien ein, die immer häufiger mit der Notwendigkeit **sicherheitspolitischer Maßnahmen** und der Terrorbekämpfung begründet werden.

Den diesjährigen Grundrechte-Report stellt der Journalist und Leiter des TV-Magazins Monitor, **Georg Restle,** vor. Er appelliert angesichts der negativen Bilanz des Reports daran, die Werteordnung unserer Verfassung nicht aus dem Blick zu verlieren: *„In einer Zeit, in der Sicherheit über allem steht, gerät die Freiheit in Gefahr. Wie selten zuvor in der Geschichte des Grundgesetzes stehen Grundrechte in diesem Land unter Druck. ‚In dubio pro libertate‘ wurde abgelöst durch ‚in dubio pro securitate‘: Im Zweifel für die Sicherheit. Der Grundrechte-Report 2017 liefert eine erschreckende Chronik der Einschränkung von Bürger- und Menschenrechten und zeigt: Der Kampf um die Grundrechte muss in diesem Land neu aufgenommen werden.“*

Ein besonderer Schwerpunkt des diesjährigen Berichtes sind zahlreiche **Einschränkungen sozialer Grundrechte,** etwa bei der lückenhaften Umsetzung des Mindestlohns, der Ungleichbehandlung durch die Erbschaftssteuerreform oder die Kostenvorbehalte im Bundesteilhabegesetz. Besondere Aufmerksamkeit widmet die Redaktion den **Gefangenen.** Martin Singe prangert den Zynismus einer „aufgeschobenen Inkraftsetzung“ von § 190 ff Strafvollzugsgesetz an, das seit 1977 eine gesetzliche Rentenversicherung für Gefangene vorschreibt. Sie führt dazu, dass Gefangene zusätzlich zur menschenunwürdigen Bezahlung ihrer Arbeit weit unterhalb des Mindesteinkommens auch noch dadurch bestraft werden, dass ihr Verdienst nicht in die Rentenversicherung einfließt – Altersarmut vorprogrammiert ist. Die Begründungen für die Verweigerung dieser Sozialstandards sind so verschieden wie widersprüchlich und belegen vor allem eines: dass sich Bund und Länder wechselseitig aus der Verantwortung stehlen wollen.

Grundrechte-Report 2017 – Zur Lage der Bürger- und Menschenrechte in Deutschland.
Herausgeber: Till Müller-Heidelberg, Elke Steven, Marei Pelzer, Martin Heiming, Cara Röhner, Rolf Gössner, Julia Heesen und Arthur Helwich.
Fischer Taschenbuch Verlag, Frankfurt am Main, Juni 2017
ISBN 978-3-596-29819-8,
224 Seiten, 10.99 Euro.

Vanessa Hellmann berichtet von der verweigerten Substitutionstherapie für einen Langzeit-Drogenabhängigen im bayerischen Strafvollzug, die den Europäischen Gerichtshof für Menschenrechte beschäftigte. Auf eine weitere Entrechtung von Gefangenen macht Kirstin Drenkhahn aufmerksam: Sie geht der Frage nach, ob Gefangene eine Gewerkschaft gründen und betreiben dürfen. Während die Länder dies bisher bestreiten – bei Gefangenenarbeit handle es sich um Zwangsdienste (was nicht mehr für alle Bundesländer gilt) und Gefangene seien deshalb keine echten Arbeitnehmer/innen (was auch für Wehrdienstleistende galt, die eine Gewerkschaft gründen durften) – sieht Drenkhahn keine überzeugenden Gründe dafür, Gefangenen ihr Recht auf Koalitionsfreiheit gem. Artikel 9 Abs. 3 Grundgesetz abzusprechen. Bei der Präsentation wird stellvertretend für viele Betroffene Oliver Rast, Sprecher der Gefangenen-Gewerkschaft / Bundesweite Organisation anwesend sein und über den aktuellen Stand der Anerkennung seiner Organisation informieren.

Trägerkreis: Der Grundrechte-Report 2017 wird gemeinschaftlich herausgegeben von Humanistische Union vereinigt mit der Gustav Heinemann-Initiative | Bundesarbeitskreis Kritischer Juragruppen | Internationale Liga für Menschenrechte | Komitee für Grundrechte und Demokratie | Neue Richtervereinigung | PRO ASYL | Republikanischer Anwältinnen- und Anwälteverein | Vereinigung Demokratischer Juristinnen und Juristen.

http://www.grundrechte-report.de/

Ute Bernhardt

Aktualisierte Neuauflage: „Naturwissenschaft – Rüstung – Frieden. Basiswissen für die Friedensforschung“

Welchen Unterschied zehn Jahre für Frieden und Freiheit in der Welt ausmachen können, macht die aktuelle Neuauflage des Buches „Naturwissenschaft – Rüstung – Frieden. Basiswissen für die Friedensforschung“ aus der Reihe Friedens- und Konfliktforschung deutlich.

Jürgen Altmann, Ute Bernhardt, Kathryn Nixdorff, Ingo Ruhmann, Dieter Wöhrle
Naturwissenschaft – Rüstung – Frieden. Basiswissen für die Friedensforschung.
Reihe Friedens- und Konfliktforschung, Springer-Verlag Wiesbaden, 2. Auflage, 2017
ISBN: 9783658019730
Auch als eBook erhältlich

Ging es der ersten Auflage 2007 darum, zentrale Sachfragen moderner Rüstung, ABC-Waffen und Information Warfare aufzubereiten für den damaligen Weiterbildungsstudiengang „Konflikt und Frieden“ der Fernuniversität Hagen und für die daraus erwachsenden Konfliktbeobachter, so hatten sich die Autor.innen für die Neuauflage 2017 mit einer Fülle neuer Bedrohungen auseinanderzusetzen. Chemiewaffen kamen in Syrien wiederholt zum Einsatz. Drohnen und andere automatische Abstandswaffen sind zum Bestandteil der Kampfhandlungen auch in wenig technisierten Konflikten geworden. Die Allgegenwart von Information Warfare auch im zivilen Leben und die aktuelle rasante Aufrüstung in aller Welt haben die Enthüllungen Edward Snowdens dokumentiert.

Konflikte werden nicht mehr nur durch Waffenexporte angeheizt, der Zugang zu gesellschaftlich disruptiver und oft tödlicher Kriegstechnologie ist leichter geworden durch die Abhängigkeit verletzlicher IT-Infrastrukturen auf der einen Seite und die Tendenzen auf der anderen Seite, Waffen, Trägersysteme, Sprengstoffe und schädigende Chemikalienmixturen im Selbstelaborat herzustellen – in naher Zukunft noch viel leichter aus dem 3D-Drucker.

Aus einem ursprünglich für Beobachter klassischer Konflikte konzipierten Buch wurde durch die aktuellen Entwicklungen daher mehr und mehr ein Buch zum Verständnis für naturwissenschaftliche Fakten und Hintergründe in den global um sich greifenden Konflikten. Dementsprechend umfangreich fiel die Aktualisierung der Beiträge aus, die sich weiterhin an den für die Kriegsführung bedeutsamen Disziplinen Physik, Chemie, Biologie und Informatik ausrichten. Allen düsteren Aussichten und Rüstungsbemühungen zum Trotz kommen die Ansätze zur Rüstungskontrolle nicht zu kurz.

Entstanden ist damit ein hoch aktuelles und umfassendes Werk über jene Wissenschaften und Technologien, mit deren Produkten die Konflikte von heute ausgetragen werden.

Wissenschaft & Frieden 2/2017 „Flucht und Konflikt“

Seit 2015 beherrscht die Debatte über Zuwanderung die deutsche und europäische Politik. Weltweit fliehen Millionen von Menschen, besonders aus den Krisenregionen Afrikas und des Nahen Ostens; Hunderttausende kamen nach Europa. W&F 2/2017 „Flucht und Konflikt“ befasst sich exemplarisch mit Fluchtursachen, untersucht (sozial-)psychologische Aspekte von Flucht und die europäische Flüchtlingspolitik, kritisiert fehlende Bürgerrechte für Flüchtlinge und die zunehmende Vergrenzung der EU und ruft am Schluss zur Solidarität auf.

Es schreiben:

- *Jürgen Scheffran* und *Christiane Fröhlich*: Klima – Gewalt – Flucht. Das Beispiel Syrien
- *Katja Mielke*: Fluchtursachen und Verantwortung. Das Beispiel Afghanistan
- *Yuriy Nesterko* und *Heide Glaesmer*: Migration und Flucht als Prozess. Die individuelle und gesellschaftliche Perspektive
- *Ulrich Wagner* und *Patrick F. Kotzur*: Die Fluchtkrise. Sozialpsychologische Analysen und Implikationen
- *Helen Landmann*, *Anette Rohmann* und *Stefan Stürmer*: Sozialpsychologie und Flucht

- *Nadine Knab*: Wolf im Schafspelz. Welche Hilfe ist im Asylkontext hilfreich?
- *Anna Lübbe*: Flüchtlingsverantwortung. Europäische Asylpolitik in der Krise
- *Catherine Götze*: Bürgerschaftslose Flüchtlinge
- *Jacqueline Andres*: Vergrenzung der EU. Grenzvorverlagerung, Profit und Behinderung der Demokratie
- *Dirk Vogelskamp*: Solidarische Städte – Städte der Zuflucht

Außerhalb des Schwerpunkts

- befasst sich *Hartwig Hummel* damit, wie Zivilklauseln an japanischen Universitäten unter Druck geraten;
- geht *Annette Ripper* der Frage nach, wie die Erinnerungen an den Atombombenabwurf auf Hiroshima verarbeitet wurden;
- untersuchen *Mirko Himmel*, *Gesine Rempp* und *Volkmar Vill* die aktuellen Herausforderungen an das Chemiewaffenübereinkommen und
- legt *Till Bastian* dar, warum die pazifistischen Schriften von Erasmus von Rotterdam auch nach 550 Jahren noch aktuell sind.

In einem Gastkommentar fordert der Vorsitzende der Vereinigung Deutscher Wissenschaftler, *Hartmut Graßl*, dass die Wissenschaft auch in der Öffentlichkeit mehr Verantwortung übernehmen muss, und in einer kommentierten Presseschau gibt *Regina Hagen* einen Überblick über die Reaktionen auf das türkische Referendum.

Ergänzt werden die Artikel wie immer durch Berichte von Tagungen und Kongressen, Rezensionen und Informationen aus Friedensforschung und Praxis.

Wissenschaft & Frieden 2/2017 „Flucht und Konflikt" 9,00 € plus Porto.

W&F erscheint vierteljährlich. Jahresabo 35 €, ermäßigt 25 €, Ausland 45 €, ermäßigt 35 €, Förderabo 60 €. W&F erscheint auch in digitaler Form – als PDF und ePub. Das Abo kostet für Bezieher der Printausgabe zusätzlich 5 € jährlich – als elektronisches Abo ohne Printausgabe 20 € jährlich.

Bezug: W&F, Beringstr. 14, 53115 Bonn,
E-Mail: *buero-bonn@wissenschaft-und-frieden.de,*
www.wissenschaft-und-frieden.de

Eberhard Zehendner

Aktuelle Juristische Praxis (AJP) / Pratique Juridique Actuelle (PJA) 2/2017 „Roboterrecht". Einführung: Isabelle Wildhaber und Melinda F. Lohmann

Das vorliegende Sonderheft dokumentiert die Tagung *Roboterrecht*, die am 28. und 29. Oktober 2016 in St. Gallen stattfand, in Form der verschriftlichten Referate; ergänzt wird die Sammlung durch eine ganze Reihe weiterer Beiträge zur selben Thematik. Bereits der Einführungsbeitrag macht deutlich, dass das Roboterrecht noch weit hinter den Erfordernissen zurückhängt, und dies beginnt schon mit terminologischen Problemen.

In dem insgesamt sehr spannenden Band hat insbesondere der Beitrag *Roboter und Privacy* von *Alfred Früh* einen direkten Bezug zu unserem Schwerpunkt *Datenschutz handhabbar*. Früh argumentiert, dass Roboter (als datenbasierte Systeme verstanden) die Rechtsordnung aus informationsrechtlicher Sicht vor erhebliche Probleme stellten, und dies liege insbesondere am Datenschutzrecht. Dieses sei – aber das dürfte im FifF wohl mehrheitlich anders beurteilt werden – einerseits zu weit, da es „aufgrund seines weiten Anwendungsbereiches, seines präventiven Charakters und der strengen Grundsätze der Datenbearbeitung zunehmend zu einer erheblichen Hürde für unternehmerische und wissenschaftliche Tätigkeit" werde. Andererseits reiche es nicht weit genug, da „trotz des weiten Anwendungsbereichs […] die Interessen der betroffenen Personen, insbesondere deren Privacy, oft nicht oder nicht ausreichend geschützt" seien. Früh zeigt dann auf, dass es zwischen reflexartigem „Für und Wider den Datenschutz" vielfältige Lösungsmöglichkeiten gibt, die teilweise nur kleine Veränderungen datenschutzrechtlicher Normen erfordern.

AJP/PJA 02/2017 „Roboterrecht"
Einzelheft «Aktuelle juristische Praxis - Pratique juridique Actuelle»
Dike Verlag, Zürich/St.Gallen, 2017, ISSN: 1660-3362
151 Seiten, broschiert, Sprache: Deutsch, Französisch, Preis: CHF 41,00

FIfF e.V.

Im FIfF haben sich rund 700 engagierte Frauen und Männer aus Lehre, Forschung, Entwicklung und Anwendung der Informatik und Informationstechnik zusammengeschlossen, die sich nicht nur für die technischen Aspekte, sondern auch für die gesellschaftlichen Auswirkungen und Bezüge des Fachgebietes verantwortlich fühlen. Wir wollen, dass Informationstechnik im Dienst einer lebenswerten Welt steht. Das FIfF bietet ein Forum für eine kritische und lebendige Auseinandersetzung – offen für alle, die daran mitarbeiten wollen oder auch einfach nur informiert bleiben wollen.

Vierteljährlich erhalten Mitglieder die Fachzeitschrift FIfF-Kommunikation mit Artikeln zu aktuellen Themen, problematischen Entwicklungen und innovativen Konzepten für eine verträgliche Informationstechnik. In vielen Städten gibt es regionale AnsprechpartnerInnen oder Regionalgruppen, die dezentral Themen bearbeiten und Veranstaltungen durchführen. Jährlich findet an wechselndem Ort eine Fachtagung statt, zu der TeilnehmerInnen und ReferentInnen aus dem ganzen Bundesgebiet und darüber hinaus anreisen. Darüber hinaus beteiligt sich das FIfF regelmäßig an weiteren Veranstaltungen, Publikationen, vermittelt bei Presse- oder Vortragsanfragen ExpertInnen, führt Studien durch und gibt Stellungnahmen ab etc. Das FIfF kooperiert mit zahlreichen Initiativen und Organisationen im In- und Ausland.

FIfF-Mailinglisten

FIfF-Mailingliste
An- und Abmeldungen an:
http://lists.fiff.de/mailman/listinfo/fiff-L
Beiträge an: *fiff-L@lists.fiff.de*

FIfF-Mitgliederliste
An- und Abmeldungen an:
http://lists.fiff.de/mailman/listinfo/mitglieder

Mailingliste Videoüberwachung:
An- und Abmeldungen an:
http://lists.fiff.de/mailman/listinfo/cctv-L
Beiträge an: *cctv-L@lists.fiff.de*

FIfF online

Das ganze FIfF
www.fiff.de
Twitter FIfF e.V. – *@FIfF_de*

Cyberpeace
cyberpeace.fiff.de
Twitter Cyberpeace – *@FIfF_AK_RUIN*

Faire Computer
blog.faire-computer.de
Twitter Faire Computer – *@FaireComputer*

Mitglieder-Wiki
https://wiki.fiff.de

FIfF-Beirat

Ute Bernhardt (Berlin); **Peter Bittner** (Kaiserslautern); **Dagmar Boedicker** (München); Dr. **Phillip W. Brunst** (Köln); Prof. Dr. **Wolfgang Coy** (Berlin); Prof. Dr. **Wolfgang Däubler** (Bremen); Prof. Dr. **Leonie Dreschler-Fischer** (Hamburg); Prof. Dr. **Christiane Floyd** (Hamburg); Prof. Dr. **Klaus Fuchs-Kittowski** (Berlin); Prof. Dr. **Michael Grütz** (Konstanz); Prof. Dr. **Thomas Herrmann** (Bochum); Prof. Dr. **Wolfgang Hesse** (Marburg); Prof. Dr. **Eva Hornecker** (Weimar); **Werner Hülsmann** (Konstanz); **Ulrich Klotz** (Frankfurt); Prof. Dr. **Klaus Köhler** (Mannheim); Prof. Dr. **Herbert Kubicek** (Bremen); Dr. **Constanze Kurz** (Berlin); Prof. Dr. **Klaus-Peter Löhr** (Berlin); **Werner Mühlmann** (Oppung); Prof. Dr. **Frieder Nake** (Bremen); Prof. Dr. **Rolf Oberliesen** (Bremen); Prof. Dr. **Arno Rolf** (Hamburg); Prof. Dr. **Alexander Rossnagel** (Kassel); **Ingo Ruhmann** (Berlin); Prof. Dr. **Gerhard Sagerer** (Bielefeld); Prof. Dr. **Gabriele Schade** (Erfurt); **Ralf E. Streibl** (Bremen); Prof. Dr. **Marie-Theres Tinnefeld** (München); Dr. **Gerhard Wohland** (Waldorfhäslach)

FIfF-Vorstand

Stefan Hügel (Vorsitzender) – Frankfurt am Main
Prof. Dr. **Dietrich Meyer-Ebrecht** (stellv. Vorsitzender) – Aachen
Michael Ahlmann – Bremen
Sylvia Johnigk – München
Benjamin Kees – Berlin
Prof. Dr. **Hans-Jörg Kreowski** – Bremen
Kai Nothdurft – München
Rainer Rehak – Berlin
Jens Rinne – Mannheim
Prof. Dr. **Britta Schinzel** – Freiburg im Breisgau
Ingrid Schlagheck – Bremen
Prof. Dr. **Werner Winzerling** – Fulda
Prof. Dr. **Eberhard Zehendner** – Jena

FIfF-Geschäftsstelle

Ingrid Schlagheck (Geschäftsführung) – Bremen

Impressum

Herausgeber	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FIfF)
Verlagsadresse	FIfF-Geschäftsstelle Goetheplatz 4 28203 Bremen Tel. (0421) 33 65 92 55 *fiff@fiff.de*
Erscheinungsweise	vierteljährlich
Erscheinungsort	Bremen
ISSN	0938-3476
Auflage	1 200 Exemplare
Heftpreis	7 Euro. Der Bezugspreis für die FIfF-Kommunikation ist für FIfF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die FIfF-Kommunikation für 28 Euro pro Jahr (inkl. Versand) abonnieren.
Hauptredaktion	Dagmar Boedicker, Stefan Hügel (Koordination), Sylvia Johnigk, Hans-Jörg Kreowski, Dietrich Meyer-Ebrecht, Ingrid Schlagheck, Eberhard Zehendner
Schwerpunktredaktion	Eberhard Zehendner, Stefanie Jäckel (Datenschutz); Hans-Jörg Kreowski (Cyber-Forum)
V.i.S.d.P.	Stefan Hügel
FIfF-Überall	Beiträge aus den Regionalgruppen und den überregionalen AKs. Aktuelle Informationen bitte per E-Mail an *hubert.biskup@gmx.de*. Ansprechpartner für die jeweiligen Regionalgruppen finden Sie im Internet auf unserer Webseite *http://www.fiff.de/regional*
Retrospektive	Beiträge für diese Rubrik bitte per E-Mail an *redaktion@fiff.de*
Lesen, SchlussFIfF	Beiträge für diese Rubriken bitte per E-Mail an *redaktion@fiff.de*
Layout	Berthold Schroeder
Titelbild	Videostill, Motion Ensemble, Alexander Lehmann
Druck	Meiners Druck oHG, Bremen

Die FIfF-Kommunikation ist die Zeitschrift des „Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V." (FIfF). Die Beiträge sollen die Diskussionen unter Fachleuten anregen und die interessierte Öffentlichkeit informieren. Namentlich gekennzeichnete Artikel geben die jeweilige Autor.innen-Meinung wieder.

Die FIfF-Kommunikation ist das Organ des FIfF und den politischen Zielen und Werten des FIfF verpflichtet. Die Redaktion behält sich vor, in Ausnahmefällen Beiträge abzulehnen.

Nachdruckgenehmigung wird nach Rücksprache mit der Redaktion in der Regel gern erteilt. Voraussetzung hierfür sind die Quellenangabe und die Zusendung von zwei Belegexemplaren. Für unverlangt eingesandte Artikel übernimmt die Redaktion keine Haftung.

Wichtiger Hinweis: Wir bitten alle Mitglieder und Abonnenten, Adressänderungen dem FIfF-Büro möglichst umgehend mitzuteilen.

Aktuelle Ankündigungen

(mehr Termine unter *www.fiff.de*)

33. FIfF-Konferenz (#FIfFKon17)
20. bis 22. Oktober, Universität Jena (siehe auch Seite 15)

FIfF-Mitgliederversammlung
22. Oktober, Universität Jena, 12:30 bis 14:00 Uhr

FIfF-Kommunikation

3/2017 „Freiheit 2.0"
Britta Schinzel
Redaktionsschluss: 4. August 2017

4/2017 „Staats-Hacking – Die ‚Gerätchenfrage'"
Rainer Rehak u.a.
Redaktionsschluss: 3. November 2017

1/2018 „TRUST – Wem kann ich trauen im Netz und warum?"
Stefanie Jäckel, Eberhard Zehendner u. a.
Redaktionsschluss: 2. Februar 2018

W&F – Wissenschaft & Frieden

3/16 Politischer Islam
4/16 Weltordnungskonzepte (mit Dossier 83: Ziviles Peacekeeping)
1/17 Facetten des Pazifismus (mit Dossier 84: Gender, Frauen und Friedensengagement)
2/17 Flucht & Migration

vorgänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik

#216 Rechtspopulismus/Rechtsextremismus
#217 Der Islam als Herausforderung für das deutsche Religionsverfassungsrecht
#218 Rückkehr zum gerechten Krieg?
#219 Soziale Menschenrechte

DANA – Datenschutz-Nachrichten

3/16 – Beschäftigtendatenschutz in neuen Gewändern
4/16 – Tracking, Profiling, Werbung, Marketing
1/17 – Verbraucherschutz
2/17 – BDSG-Nachfolgegesetz (alternativ: Geheimdienste)
3/17 – 40 Jahre DVD

Das FIfF-Büro

Geschäftsstelle FIfF e. V.
Ingrid Schlagheck (Geschäftsführung)
Goetheplatz 4, D-28203 Bremen
Tel.: (0421) 33 65 92 55, Fax: (0421) 33 65 92 56
E-Mail: fiff@fiff.de
Die Bürozeiten finden Sie unter *www.fiff.de*

Bankverbindung
Bank für Sozialwirtschaft (BFS) Köln
Spendenkonto:
IBAN: DE79 3702 0500 0001 3828 03
BIC: BFSWDE33XXX

Kontakt zur Redaktion der FIfF-Kommunikation:
redaktion@fiff.de

Schluss