HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

BACHELORARBEIT

Herr
Andreas Thomas Kayser

Die digitale Forensik im Datenschutz

Mittweida, 2018

Fakultät „Angewandte Computer- und Biowissenschaften“

BACHELORARBEIT

Die digitale Forensik im Datenschutz

Autor:
Herr

Andreas Thomas Kayser

Studiengang:
Allgemeine und Digitale Forensik

Seminargruppe:
Fo15w3-B

Erstprüfer:
Herr Prof. Dr. rer. Nat. Dirk Labudde

Zweitprüfer:
Herr Dipl. Ing. Heinz Thoma

Einreichung:
Mittweida, 08.10.2018

Verteidigung/Bewertung:
Mittweida, 2018

Faculty Angewandte Computer- und Biowissenschaften

BACHELOR THESIS

Digital forensics in the field of data protection

author:
Mr.

Andreas Thomas Kayser

course of studies:
Allgemeine und Digitale Forensik

seminar group:
F015w3-B

first examiner:
Mr. Prof. Dr. rer. Nat. Dirk Labudde

second examiner:
Mr. Dipl. Ing. Heinz Thoma

submission:
Mittweida, 08.10.2018

defence/ evaluation:
Mittweida, 2018

Bibliografische Beschreibung:

Kayser, Andreas Thomas:
Digitale Forensik im Datenschutz. - 2018. - VI, 58, II S.
Mittweida, Hochschule Mittweida, Fakultät Angewandte Computer- und Biowissenschaften, Bachelorarbeit, 2018

Referat:

Die vorliegende Arbeit befasst sich mit der Kombination der digitalen Forensik mit dem Organisationsziel des Datenschutzes. Es wird untersucht, wie forensische Arbeiten im Rahmen der bestehenden Datenschutzgesetze anzusiedeln sind. Dafür werden die gesetzlichen Grundlagen, welche in Deutschland gelten, thematisiert sowie wird in einem praktischen Beispiel das Auskunftsrecht bei einem sozialen Netzwerk wahrgenommen und die erhaltenen Daten analysiert. Des Weiteren wird in dieser Arbeit dargestellt, welche forensischen Hilfstools und Methoden angewandt werden können, um Datenschutzverletzungen oder das datenschutzkonforme Arbeiten eines Verantwortlichen nachweisen zu können.

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

BDSG	Bundesdatenschutzgesetz neue Fassung
BDSG alt	Bundesdatenschutzgesetz alte Fassung
EU-DSGVO	Europäische Datenschutz-Grundverordnung
KDG	Gesetz über den Kirchlichen Datenschutz
HTML	Hypertext Markup-Language
TXT	Textdatei im Windows-Betriebssystem
JSONS	JavaScript Object Notation
GG	Grundgesetz
EU	Europäische Union
EMRK	Europäische Menschenrechtskonvention
DSAnpUG-EU	Datenschutz-Anpassungs- und Umsetzungsgesetz EU
MB	Megabytes (1 Megabyte= 1000000 Byte)
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IpV6	Internet Protocol Version 6
EG	Europäische Gemeinschaft
JPG	JPEG File Interchange Format
AGB	Allgemeine Geschäftsbedingungen
CSV	Comma-seperated values
XML	Extensible Markup Language
STPO	Strafprozessordnung
ODS	OpenDocumentSpreadsheet
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
DART	Digital Advanced Response Toolkit

DEFT	Digital Evidence & Forensics Toolkit
WINE	Wine is not an Emulator
EXE	Endung für Ausführbare Dateien im Windows-Betriebssystem
DSG-EKD	Kirchengesetz über den Datenschutz der evangelischen Kirche in Deutschland
KDO	Bischöfliche Verordnung über den kirchlichen Datenschutz im Katholischen Bistum der Alt-Katholiken in Deutschland

1 Motivation, Zielstellung und Aufbau der Arbeit

Im modernen Zeitalter wird vermehrt auf Digitalisierung gesetzt. Mittlerweile ist es nicht unüblich, dass sogar Haushaltsgeräte im sogenannten Internet of Things mit anderen Diensten und Geräten vernetzt sind. Dabei fallen nicht nur Unmengen von technischen Daten an, sondern auch personenbezogene Daten, die Informationen über den Besitzer oder Nutzer bereitstellen.

Um die Dateninhaber zu schützen hat es sich die Politik weltweit zum Ziel gesetzt, mit effektiven Datenschutzgesetzen gegen einen Missbrauch dieser Daten vorzugehen und nur rechtmäßige und durchdachte Datenverarbeitungen zuzulassen.

Datenschutzgesetze existieren in Deutschland bereits seit 1970, als Hessen das weltweit erste Datenschutzgesetz verabschiedete. Die Bundesregierung zog mit dem Bundesdatenschutzgesetz im Jahr 1977 nach, die übrigen Bundesländer folgten bis Anfang der 1980er. Ein weiterer Meilenstein war das 1983 gesprochene Volkszählungsurteil, in dem das informationelle Selbstbestimmungsrecht aus Art. 1 Abs. 1 GG abgeleitet und somit bestätigt wurde. Damit wurde Datenschutz erstmals ein Grundrecht und die bis dahin geltenden Gesetze wurden reformiert. Erst 1995 folgte eine europaweite Richtlinie (95/46/EG), welche freien Datenverkehr und den Schutz der Verarbeitung personenbezogener Daten regelte. Als Richtlinie musste diese in nationalem Gesetz umgesetzt werden, was in Deutschland 2001 durch eine Anpassung des BDSG erfolgte. (1)

Durch diese notwendige Umsetzung und den gegebenen Abweichungsmöglichkeiten zu den Richtlinien unterschieden sich die Datenschutzgesetze in Europa teils stark voneinander. Um dem Abhilfe zu schaffen und auch die mittlerweile rasanten Entwicklungen in Technik und der Digitalisierung zu beachten, sollte ein neues, in der gesamten Europäischen Union geltendes Gesetz geschaffen werden: die Europäische Datenschutzgrundverordnung. Nach vierjähriger Verhandlung am 04.Mai 2016 final beschlossen und ab dem 24. Mai 2016 in Kraft getreten, gilt diese für alle europäischen Mitgliedsstaaten (2). Im Zuge dessen wurden die meisten Datenschutzgesetze wie das BDSG überarbeitet, und so erfährt der Datenschutz eine neue Reformation.

1.1 Motivation und Zielstellung

Doch was bedeutet diese Reformation im Datenschutz für konkrete Anwendungsfelder? War Datenschutz früher ein rein organisatorisches Problem so ist im Zuge der Digitalisierung dieses Problem vermehrt technisch geworden. Auch enthält der Datenschutz Querschnitte mit diversen anderen Fachbereichen, darunter fallen insbesondere Recht, IT-Sicherheit, Risikomanagement, und auch die digitale Forensik.

Die digitale Forensik ist analog zur klassischen Forensik zu sehen, nur auf den speziellen Bereich von digitalen Spuren. Allgemein umfasst die Forensik alle Teilbereiche, „in denen systematisch kriminelle Handlungen identifiziert, analysiert bzw. rekonstruiert werden“ (3). Für den digitalen Raum bezieht sich dies insbesondere auf Computersysteme und den dadurch anfallenden digitalen Spuren. Diese können in den unterschiedlichsten Formen vorliegen, beispielsweise als Dateien oder nur auf Bitebene. Hierbei können dann auch Verstöße gegen die Datenschutzgesetze nachgewiesen und rekonstruiert werden.

Der Ansatz, die digitale Forensik mit dem Ziel des Datenschutzes zu kombinieren, soll als zielführende Aufgabe dieser Arbeit dienen. Ziel dieser Arbeit soll es sein, den Datenschutz und die neu geschaffenen Gesetze mit dem Gebiet der digitalen Forensik zu vereinen und zu beschreiben, wie die Arbeit in den neu geschaffenen Umgebungen des Datenschutzes aussehen kann. Untersucht werden soll, welche gesetzlichen Grundlagen für eine forensische Arbeit im Datenschutz existieren und welche Aspekte es zu beachten gilt, aber ebenso, welche Möglichkeiten zur Verbesserung für die digital forensische Arbeit existieren und wie diese in der Praxis umgesetzt werden können.

Ein weiteres Ziel soll sein, wie die digitale Forensik mit ihren Methoden und Hilfsmitteln die Arbeit im Bereich des Datenschutzes beeinflussen kann. Oberstes Ziel der Methoden soll stets die praktische Anwendung sein, dazu werden verschiedene Aspekte untersucht, wie die Arbeit besonders in der Umsetzung aussehen kann, ihre Wirtschaftlichkeit und ob sie überhaupt anwendbar ist. Ebenso soll unterschieden werden, wozu diese einzelnen Methoden dienen können sowie stets die rechtlichen Grundlagen beachten. Praktische Anwendbarkeit der forensischen Methoden können insbesondere Untersuchungen im Rahmen von gerichtsverwertbaren Gutachten sein, sowie interne Untersuchungen innerhalb von Organisationen, um Verletzungen des Datenschutzes nachweisen zu können. Auch Sinnhaftigkeit und mögliche Verbesserungen sollen thematisiert werden.

1.2 Aufbau der Arbeit

Die Arbeit ist gestaffelt nach fünf Kapiteln aufgebaut. Nachdem in Kapitel 1 die Motivation und Zielstellung dargelegt worden sind, soll in Kapitel zwei näher auf die neu geschaffenen Gesetze eingegangen werden, die den Grundstein für die gesamte Arbeit darstellen. Die einzelnen Aspekte werden dann pro Kapitel einzeln aufgegriffen, um so detailliert beschreiben zu können, welche Aspekte entsprechend zu beachten sind oder welche Möglichkeiten sich ergeben können.

Kapitel drei beschäftigt sich dann mit dem Thema der Informationspflichten und Auskunftsrechte von Betroffenen Personen. Hauptziel dieses Kapitels ist zu untersuchen, ob die durch die Datenschutzgesetze geschaffenen neuen Rechte die forensische Arbeit

erleichtern können, und wie dies praktisch aussehen könnte. Als praktische Beispiel wurde das Recht auf Auskunft nach Art. 15 EU-DSGVO bei dem sozialen Netzwerk Facebook eingefordert und die dadurch erhaltenen Daten analysiert und ausgewertet, besonders hinsichtlich ihrer Verwendbarkeit für forensische Untersuchungen und dem daraus entstehenden praktischen Nutzen.

Nachdem im vorhegenden Kapitel die Möglichkeiten der Datenschutzgesetze für die digitale Forensik dargelegt worden sind, soll Kapitel vier umgekehrt aufgebaut sein: was können digital forensische Methoden für den Datenschutz nützen? Denn auch wenn die Rechenschaftspflicht festlegt, dass das datenschutzkonforme Arbeiten von vornherein nachgewiesen sein muss, so kommen in der Praxis doch immer wieder Unterschiede zwischen Theorie und Praxis vor. Deshalb werden praktische Methoden und Tools vorgestellt, die dem Nachweis von Datenschutzverletzungen dienen sollen, die aber auch durchaus zur Einhaltung und Überprüfung von Datenschutzbestimmungen dienen können. Interessant dürfte dies insbesondere für Datenschutzbehörden sein, welche einzelnen Datenschutzverstößen nachgehen müssen, um so konkrete Beweise vorlegen zu können, die zu den verhängenden Bußgeldern führen können, aber auch, nach Datenschutzgesetzen definierte, Verantwortliche können sich diese Methoden zu Nutze machen, um die durchzusetzenden Maßnahmen und Regelungen auf ihrer Einhaltung zu prüfen.

Im letzten Kapitel sollen eine Zusammenfassung und Einschätzung der Ergebnisse erfolgen. Wieder sollen die praktische Anwendbarkeit bewertet und verglichen werden, sowie die Notwendigkeit und Sinnhaftigkeit der einzelnen Methoden. Auch soll ein Ausblick geschaffen werden, was mithilfe der Erkenntnisse dieser Arbeit geschehen kann, beziehungsweise wie die gemeinsame Schnittmenge zwischen Datenschutz und digitaler Forensik genutzt werden kann.

2 Gesetzliche Grundlagen

In diesem Kapitel sollen die Grundlagen beschrieben und dargelegt werden, die für diese Arbeit notwendig sind. Insbesondere handelt es sich hierbei um die Gesetzestexte, welche sich mit dem Datenschutz befassen. Eingegrenzt wurde dies auf die Gesetze, die in der Bundesrepublik Deutschland ihre Anwendung finden. Zum einen ist dies die Europäische Datenschutzgrundverordnung (EU-DSGVO), sowie das Bundesdatenschutzgesetz (BDSG n.F.). Zusätzlich wird noch das Gesetz über den Kirchlichen Datenschutz (KDG) herangezogen, welches in Deutschland für geistliche Einrichtungen der katholischen Kirche gilt. Andere kirchliche Gemeinschaften besitzen ebenfalls ihre eigenen Gesetze, beispielsweise hat die evangelische Kirche das EKD-Datenschutzgesetz (DSG-EKD) und die altkatholische Kirche die Ordnung über den Schutz von personenbezogenen Daten (Datenschutzordnung, DSO). Zur einfacheren Betrachtung wird von den kirchlichen Gesetzen allerdings nur das KDG exemplarisch betrachtet.

Alle diese Gesetze sind im Zuge der Einführung der Europäischen Datenschutzgrundverordnung überarbeitet worden und im Mai 2018 in der aktuellsten Form (Stand: August 2018) erschienen. Generell soll hier ein grober Überblick über Neuerungen, Inhalte sowie die verschiedenen Anwendungsbereiche der einzelnen Datenschutzgesetze gegeben werden.

2.1 Europäische Datenschutzgrundverordnung (EU-DSGVO)

„*Die Datenschutz-Grundverordnung ist ein Meilenstein des Datenschutzes in Europa, denn sie verknüpft bewährte Prinzipien des grundrechtsorientierten Datenschutzrechts mit einer stärkeren Harmonisierung und einer maßvollen Modernisierung.“* (2)

Mit diesen Worten beschreibt die Bundesbeauftragte für Datenschutz und Informationssicherheit Andre Voßhoff im September 2017 die Europäische Datenschutzgrundverordnung (EU-DSGVO), welche nach vierjähriger Verhandlung im Frühjahr 2016 vom Europäischen Rat und dem europäischen Parlament verabschiedet worden ist. Die Grundlage für das Gesetz soll das informationelle Selbstbestimmungsrecht des Einzelnen sein. (2)

Das Recht auf informationelle Selbstbestimmung leitet sich auf EU-Ebene aus Art. 8 Abs. 1 EMRK der Europäischen Menschenrechtskonvention ab:

„Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.“ (Art. 8 Abs. 1 MRK)

Prinzipiell würde damit jeder Person eingeräumt, selbst über Informationen zu bestimmen, die sie selbst betrifft. Auf den Datenschutz übertragen bedeutet das, dass jeder Person selbst entscheiden darf, welche eigenen personenbezogenen Daten verarbeitet oder genutzt werden dürfen. Die Grundverordnung setzt sich also als Hauptziel, dem Betroffenen mehr Möglichkeiten zur Wahrung seines informationellen Selbstbestimmungsrechts zu gewährleisten. Dafür werden die Regelungen innerhalb der Grundverordnung nach dem Verbotsprinzip geschaffen, was bedeutet, dass grundsätzlich alle Datenverarbeitungen verboten sind, sofern sie nicht auf gesetzlicher Erlaubnis oder einer ordnungsgemäßen Einwilligung beruhen. Dadurch wird auch die Darlegungslast für die Notwendigkeit des Eingriffs weiterhin bei demjenigen liegen, welcher einen solchen Eingriff vornimmt, wie beispielsweise in Art. 8 Abs.2 EMRK definiert.

Weitere in die Grundverordnung eingebauten Prinzipien sind die Angemessenheit, Erforderlichkeit sowie die Zweckbindung, welche alle im Prinzip der Datensparsamkeit aufgegriffen werden. Dieses beschreibt, dass nur solche Daten erhoben werden dürfen, welche für die Verarbeitung notwendig sind, die wiederum auf einem konkreten Zweck beruhen muss. Wert wurde ebenfalls auf die Transparenz und die Gewährleistung der Datensicherheit gelegt, um Datenverarbeitungen für jeden Betroffenen erkenntlich zu machen sowie die Sicherheit der einzelnen Verarbeitungsschritte zu gewährleisten.

Datenverarbeitungen werden mittlerweile international ausgeführt. Viele Unternehmen nutzen die Möglichkeiten, ihre eigenen Geschäftszweige outzusourcen, das heißt andere Unternehmen mit der Erfüllung der eigenen Aufgaben beauftragen, um so Kosten und Aufwand zu sparen. Doch an welche Gesetze muss sich nun ein Auftragsverarbeiter, ein Verantwortlicher, welcher im Auftrag Daten verarbeitet, halten, wenn er die Daten seines Auftraggebers verarbeitet? Diese Frage sollte mit der Vereinheitlichung des Datenschutzes innerhalb der EU in Form der Europäischen Datenschutzgrundverordnung beantwortet werden. Somit müssen sich alle Länder der EU an diese Gesetze halten, solange nicht für einzelne Regelungen Gesetzesvorbehalte vorgesehen sind und angewendet werden können.

Durch den in Art. 3 EU-DSGVO geregelten örtlichen Anwendungsbereich erstreckt sich der Geltungsraum des Gesetzes unter bestimmten Umständen auch über die europäische Union hinaus. Es müssen sich alle nach Art. 4 Abs. 7 EU-DSGVO definierten Verantwortlichen an die EU-DSGVO halten, sobald dieser oder sein Auftragsverarbeiter in der Union seinen Sitz hat, egal ob die Verarbeitung auch in der Union stattfindet. Ebenso gilt sie für die Verarbeitung personenbezogener Daten von Personen, die sich in der Union befinden, und wenn die Verarbeitung darauf zielt, Waren und Dienstleistungen anzubieten oder Verhalten zu beobachten. Bezeichnet wird dies als das Marktortprinzip und soll gewährleisten, dass alle Verarbeitungen innerhalb der EU sowie Verarbeitungen, die sich auf den europäischen Markt beziehen den gleichen Regelungen unterliegen. Ziel hierbei ist, einen einheitlichen Wettbewerb zu schaffen und keine Möglichkeiten des Missbrauchs zu ermöglichen, beispielsweise durch das Outsourcen von Datenverarbeitungen in Nicht-EU-Länder um anderen Gesetzen zu unterliegen.

Zusätzlich regelt das Gesetz die unabhängige Aufsicht und wirksame Sanktionierung. Die Regelungen bezüglich der Aufsichtsbehörden wurden verschärft, beispielsweise muss nun jede Datenschutzverletzung der zuständigen Behörde gemeldet werden, und die Bußgelder wurden deutlich angehoben. So sprach das BDSG alt noch von bis zu 50.000 und bis zu 300.000 Euro, so können nach der EU-DSGVO nun Summen von bis zu zehn Millionen oder bis zu 20 Millionen gefordert werden, alternativ zwei oder vier Prozent des Jahresumsatzes der verarbeitenden Stelle. Die ausgesprochenen Strafen sollen dabei in jedem Einzelfall wirksam, verhältnismäßig und abschreckend (Art. 83 Abs.1 EU-DSGVO) sein.

Inhaltlich gliedert sich die EU-DSGVO in elf Kapitel mit insgesamt 100 Artikeln. Nach der Verabschiedung am 27. April 2016 trat sie am 20. Tag nach der Veröffentlichung in Kraft und gilt ab dem 25. Mai 2018 in allen EU-Mitgliedsstaaten. Den Mitgliedsstaaten ist es allerdings freigestellt, weitere nationale Gesetze zu erlassen, die ergänzend zur EU-DSGVO stehen sollen.

2.2 Bundesdatenschutzgesetz neue Fassung (BDSG n.F.)

Nach dem Beschluss der Europäischen Datenschutzgrundverordnung musste das damals geltende Bundesdatenschutzgesetz in Deutschland angepasst werden. Daher erließ der Bundestag mit Zustimmung des Bundesrates am 30. Juni 2017 das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU–DSAnpUG-EU). Dieses staffelt sich in acht Artikel und enthält unter Artikel 1 das gesamte Bundesdatenschutzgesetz neue Fassung (BDSG n.F.). Daher ist es auch, anders als die EU-DSGVO in Paragraphen gestaffelt und nicht in Artikeln, da das gesamte Gesetz an sich ein Gesetzesartikel ist. Es ist gegliedert in vier Teile mit insgesamt 19 Kapiteln und 85 Paragraphen.

Ziel und Zweck des neuen Bundesdatenschutzgesetzes ist es, die durch die EU-DSGVO geschaffenen Richtlinien und Regelungen zu konkretisieren und, sofern die Möglichkeiten bestehen, entsprechend eigene Anpassungen vorzunehmen. Besonders der Teil drei des BDSG ist spezifisch, da er sich rein mit der Datenverarbeitung durch öffentliche Stellen beschäftigt. Auch wenn das BDSG für Nicht-Öffentliche Stellen, beispielsweise Vereine und Unternehmen, gilt, so sind dort doch viele Regelungen deckungsgleich mit der EU-DSGVO.

Die Konkretisierungen der EU-Regelungen sind dabei sehr unterschiedlich, fallen aber im Rahmen der Möglichkeiten aus. So muss laut BDSG bereits ab 10 Personen, die regelmäßig personenbezogene Daten verarbeiten ein Datenschutzbeauftragter bestellt werden, während die EU-DSGVO eine Bestellung vorsieht, sobald die Kerntätigkeit des Verantwortlichen in der Verarbeitung personenbezogener Daten besteht. Hier ist also doch ein

signifikanter Unterschied, der sich insbesondere in der Praxis bemerkbar macht, denn eine regelmäßige Verarbeitung der Daten zur Erfüllung des eigentlichen Kernbereichs einer Organisation existiert häufiger als eine Organisation, deren Hauptaufgabe die Verarbeitung von personenbezogenen Daten ist.

Klar geregelt werden auch die Zuständigkeiten der einzelnen Aufsichtsbehörden. In Deutschland besitzt jedes Bundesland eine zentrale Aufsichtsbehörde, die für die jeweiligen Länder zuständig sind. Einzige Ausnahme ist das Bundesland Bayern, welches zwei Aufsichtsbehörden besitzt, eine für öffentliche Stellen und eine für Nicht-Öffentliche Stellen. Auch im BDSG sind Strafen definiert, allerdings bei einer maximalen Höhe von 50.000 Euro und nur im Falle von bestimmten Fällen, in denen nur das BDSG eingesetzt werden darf. Andere Verstöße sind entsprechend der EU-DSGVO zu ahnden.

2.3 Gesetz über den Kirchlichen Datenschutz (KDG)

Im Rahmen der Gesetzgebungen steht es bestimmten Kirchen oder religiösen Vereinigungen frei, ihre eigenen Gesetze zu schreiben und diese entsprechend anzuwenden. So lässt auch die Europäische Datenschutzgrundverordnung diese Möglichkeit offen, und definiert sie in Art. 91 Abs. 1 EU-DSGVO wie folgt:

„*Wendet eine Kirche oder religiöse Vereinigung oder Gemeinschaft in einem Mitgliedsstaat zum Zeitpunkt des Inkrafttretens dieser Verordnung umfassende Regeln zum Schutz natürlicher Personen bei der Verarbeitung an, so dürfen diese Regeln weiter angewandt werden, sofern sie mit dieser Vereinbarung in Einklang gebracht werden.“*

Konkret bedeutet das, dass eine religiöse Vereinigung ihre eigenen Gesetze anwenden darf, sofern sie in Einklang mit der Europäischen Datenschutzgrundverordnung stehen. Von diesem Recht hat die Katholische Kirche in Deutschland Gebrauch gemacht. Am 20. November 2017 beschloss die Vollversammlung des Verbandes der Diözesen Deutschlands in einem einstimmigen Beschluss das „Gesetz über den Kirchlichen Datenschutz (KDG)“. Damit diese Regeln angewandt werden dürfen, musste das Gesetz vor der Europäischen Datenschutzgrundverordnung in Kraft treten, da diese Regeln „zum Zeitpunkt des Inkrafttretens“ angewandt werden mussten. Folglich, in § 58 Abs. 1 KDG geregelt, trat das KDG am 24.05.2018 in Kraft, also einen Tag vor dem Inkrafttreten der Europäischen Datenschutzgrundverordnung, welche nach Art. 99 Abs. 2 EU-DSGVO am 25.Mai 2018 in Kraft trat.

Anders als die Datenschutzgrundverordnung ist auch das KDG in Paragraphen eingestuft, da das Gesetz im jeweiligen Amtsblatt der einzelnen Diözesen veröffentlicht wurde.

Inhaltlich gliedert sich das KDG in neun Kapitel mit insgesamt 58 Paragraphen. Anhand der Anzahl der Paragraphen sieht man bereits, dass das KDG nicht den vollständigen Umfang der europäischen Datenschutzgrundverordnung besitzt. Zu erklären ist dies mit dem deutlich kleineren Anwendungsbereich, der beim KDG deutlich kleiner gefasst ist als bei der DSGVO, wobei der sachliche Anwendungsbereich identisch ist, wie § 2 Abs. 1 KDG zeigt, welche den exakt gleichen Wortlaut enthält wie Art. 2 Abs. 1 EU-DSGVO.

„Dieses Gesetz gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen."

Es ist im gesamten Gesetzestext nicht unüblich, dass Paragraphen des KDG mit den Artikeln der EU-DSGVO deckungsgleich sind. Um das KDG mit der DSGVO in Einklang zu bringen (vgl. Art. 91 Abs. 1 EU-DSGVO) wurden mehrere Artikel exakt übernommen, um diesen Einklang zu gewährleisten.

Der organisatorische Anwendungsbereich ist dafür allerdings deutlich konkreter gefasst. In § 3 Abs. 1 KDG sowie § Abs. 2 KDG werden konkret kirchliche Stellen benannt, welche unter das KDG fallen, darunter Diözesen, Kirchengemeinden, der deutsche Caritasverband, kirchliche Stiftungen und andere kirchliche Rechtsträger ohne Rücksicht auf ihre Rechtsform.

Auch anders als die EU-DSGVO und das BDSG n.F. fordert die Katholische Kirch in § 5 KDG eine Erklärung auf das Datengeheimnis für alle verarbeitenden Personen, was nach dem alten Bundesdatenschutz noch gefordert war aber mit Einführung des BDSG n.F. abgeschafft worden ist. Überwiegend ist das Gesetz aber deckungsgleich mit der Europäischen Datenschutzgrundverordnung. Einige signifikante Unterschiede werden in Kapitel 2.4 dargestellt.

Die durch die EU-DSGVO geforderte Aufsichtsbehörde ist ebenfalls aufgestellt worden. Insgesamt gibt es deutschlandweit fünf Aufsichtsbehörden, welche für die 27 Diözesen verantwortlich sind. Interessant ist hierbei, dass die Aufteilung der einzelnen Diözesen nicht nach den standesgemäßen sieben Kirchenprovinzen stattgefunden hat, sondern die Provinzen Paderborn und Bamberg aufgeteilt wurden und den übrigen Provinzen Hamburg, Berlin, München-Freising, Freiburg, Köln zugeteilt wurden.

Abbildung 1: Übersicht Katholische Datenschutzbehörden (34)

2.4 Synopse der Datenschutzgesetze

Prinzipiell unterscheiden sich die drei dargestellten Gesetze nicht in besonders großem Umfang. Durch ihre eingegrenzten Anwendungsbereiche ist klar definiert, in welchen Bereichen die einzelnen Gesetze angewendet werden müssen. Auch müssen sie alle in Einklang stehen, da dies gesetzlich von der Europäischen Datenschutzgrundverordnung gefordert ist, welche als internationales Gesetz vor Landesgesetz steht und somit vor dem BDSG steht. Das KDG gilt als Ersatzgesetz auf der gleichen Ebene wie die EU-DSGVO, hat aber durch den angegebenen Anwendungsbereich innerhalb von Deutschland Anwendung zu finden, genau wie das BDSG. Einzelne Unterschiede sollen im Folgenden aufgezeigt und verglichen werden.

Durch die Staffelung der einzelnen Gesetze, also dass das KDG prinzipiell auf der gleichen Ebene steht wie die EU-DSGVO, werden hier zur einfacheren Betrachtung die EU-DSGVO und das BDSG als eine Seite betrachtet, während das KDG dem gegenübersteht. Dies soll den einfacheren Vergleich zwischen kirchlicher Anwendung und nicht-kirchlicher Anwendung hervorheben.

Der bereits angesprochene Anwendungsbereich zeigt hierbei besonders klar die Abgrenzung der einzelnen Gültigkeiten der Gesetze. Die EU-DSGVO gilt dabei in der gesamten europäischen Union, unterscheidet aber nicht zwischen weiteren sachlichen

Anwendungsbereichen. Das BDSG unterscheidet zumindest zwischen öffentlichen und nicht-öffentlichen Stellen, und gilt entsprechend deutschlandweit. Das KDG gilt dagegen nur in den Diözesen der katholischen Kirche, nach der entsprechenden Veröffentlichung, und auch nur für kirchliche Stellen. Dieser so definierte Anwendungsbereich zeigt die Ebenen, auf denen sich die einzelnen Gesetze entsprechend bewegen, wobei das KDG auf einer Ebene mit der EU-DSGVO steht.

Weitere große Unterschiede zeigen sich in den Höchstmaßen der entsprechenden Strafen, die für den Verstoß gegen die entsprechenden Gesetze ausgesprochen werden können. Die EU-DSGVO sieht für Verstöße Bußgelder von bis zu zehn Millionen Euro oder zwei Prozent des Gesamtumsatzes eines Unternehmens vor, bei schweren Verstößen bis zu 20 Millionen Euro oder vier Prozent des Jahresumsatzes, ergänzend dazu noch die bis zu 50.000 Euro hohen Strafen aus dem BDSG für Verstöße, die rein auf das BDSG bezogen werden können. Das KDG sieht andere Werte vor und spricht Strafen in Höhe von bis zu 500.000 Euro aus. Dieser Unterschied lässt sich aber damit erklären, dass die EU-DSGVO darauf abzielt, auch größere Unternehmen auf die Einhaltung der Datenschutzgesetze zu verpflichten, und so auch das Höchstmaß für Strafen entsprechend angehoben hat, welche nach dem BSDG alt noch bei maximal 50.000 und 300.000 Euro lagen. Der Anwendungsbereich des KDG umfasst diese großen Unternehmen aber nicht, weshalb auch die Strafen entsprechend niedriger gefasst werden können, obwohl die katholische Kirche als der zweitgrößte Arbeitgeber Deutschlands einen geschätzten Gesamtumsatz von 82 Millionen Euro erwirtschaftet hat (4).

Auch räumt die Kirche sich zusätzlich weitere Rechte ein. So muss beispielsweise den Informationspflichten in bestimmten Bereichen nicht nachgekommen werden, sollte diese Pflicht der katholischen Kirche schaden können (vgl. § 16 Abs. 5 lat. A Nr. 2 KDG). Ebenso behält das KDG die in der EU-DSGVO und dem BDSG abgeschafften Verpflichtungserklärungen auf das Datengeheimnis in § 5 KDG bei, während EU-DSGVO und BDSG diese Pflicht abgeschafft haben.

Die durch das KDG und die EU-DSGVO geforderten Pflichten sind ebenfalls ähnlich. Gefordert werden unter anderem die Benennung eines Datenschutzbeauftragten, der der zuständigen Aufsichtsbehörde zu melden ist. Die Forderungen, ab wann ein Datenschutzbeauftragter zu bestellen ist, unterscheiden sich hierbei in den einzelnen Gesetzen nur in dem Punkt, der sich auf die Anzahl der Mitarbeiter bezieht. So fordern KDG und BDSG eine Bestellung bei mehr als 10 Personen, die regelmäßig mit der Verarbeitung personenbezogener Daten beschäftigt sind, während die EU-DSGVO keine Angaben zu Mitarbeitern bietet. Die anderen Voraussetzungen zur Bestellung eines Datenschutzbeauftragten, wie beispielsweise der Regelmäßigkeit der Verarbeitung, sind wiederum gleich. Weiterhin wird das Führen eines Verarbeitungsverzeichnisses in allen Gesetzen zu gleichen Voraussetzungen gefordert.

Alles in allem lässt sich also sagen, dass die drei ausgewählten Gesetzestexte durchaus einige parallelen Aufweisen und so durchaus vergleichbar sind. Die EU-DSGVO dient dabei

als Grundlage für die anderen beiden Gesetzestexte, weshalb die Texte überwiegend deckungsgleich sind. Zur weiteren Betrachtung der in dieser Arbeit angestellten Untersuchungen wird daher überwiegend auf die EU-DSGVO Bezug genommen, um die einzelnen Sachverhalte zu erläutern.

3 Auskunftspflichten als Informationsquelle

Durch die neugeschaffenen Gesetze im Bereich des Datenschutzes sind Verantwortliche an neue Informationspflichten gebunden. Hierbei sollen den Betroffenen mehr Rechte eingeräumt werden und ein Mindestmaß an Transparenz geschaffen werden, sodass der Betroffene sein Recht auf informationelle Selbstbestimmung besser wahren kann. Im Folgenden soll anhand eines Beispiels geprüft werden, wie die technische Umsetzung dieser Rechte ablaufen kann.

Dazu wurde ein praktischer Anwendungsfall geschaffen, in welchem personenbezogene Daten im Rahmen des Auskunftsrechts angefordert wurden und analysiert werden. Es soll überprüft werden, ob und in welchem Umfang diese Daten zustande kommen, wie schnell diese übermittelt werden können, und welche Möglichkeiten im Bereich der digitalen Forensik bestehen. Untersucht werden hier insbesondere die zur Verfügung gestellten Daten, die rechtlichen Grundlagen sowie der Nutzen, der entstehen könnte. Als praktisches Beispiel werden die Daten eines Nutzers des sozialen Netzwerks „Facebook“ angefordert und ausgewertet.

3.1 Rechtliche Grundlagen

Die Informationspflichten stützen sich in der Europäischen Datenschutzgrundverordnung auf das Kapitel 3 „Rechte der betroffenen Person“. Ziel dieses Abschnitts ist es, dem Betroffenen die Rechte zu gewähren, die ihn dabei unterstützen sollen, sein Recht auf informationelle Selbstbestimmung wahrzunehmen. Bereits Artikel 12 definiert, welche Informationen gemäß zur Verfügung gestellt werden müssen:

„Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln;[…]“ (Art. 12 EU-DSGVO)

Das Gesetz unterscheidet hierbei zwischen Informationen gemäß Artikel 13 und 14 und Mitteilungen, die in den Artikel 15 bis 22 sowie in Artikel 34 definiert sind. Mitteilungen sind überwiegend statische Informationen, beispielsweise welche Rechte er nach dem Gesetz der EU-DSGVO nun besitzt. In der Praxis variieren diese tatsächlich kaum, da nur auf die entsprechenden Artikel verwiesen wird und wie der Betroffene seine Rechte wahrnehmen

kann. In einer Übersicht werden hier die Mitteilungen gelistet, welche zur Verfügung gestellt werden müssen.

Artikel	***Mitteilungen***	***Inhalt***
Artikel 15 EU-DSGVO	Auskunftsrecht der Betroffenen Person	Der Betroffene hat das Recht auf Auskunft über die personenbezogenen Daten, welche vom Verantwortlichen verarbeitet werden
Artikel 16 EU-DSGVO	Recht auf Berichtigung	Der Betroffenen hat das Recht auf Berichtigung seiner personenbezogenen Daten, welche vom Verantwortlichen verarbeitet werden.
Artikel 17 EU-DSGVO	Recht auf Löschung/ „Recht auf Vergessenwerden“	Der Betroffene hat das Recht auf Löschung seiner personenbezogenen Daten
Artikel 18 EU-DSGVO	Recht auf Einschränkung der Verarbeitung	Der Betroffenen hat das Recht auf Einschränkung der Verarbeitung seiner personenbezogenen Daten
Artikel 19 EU-DSGVO	Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogenen Daten oder der Einschränkung der Verarbeitung	Der Verantwortliche teilt allen Empfängern der personenbezogenen Daten mit, sobald eine Berichtigung oder Löschung vorgenommen wurde
Artikel 20 EU-DSGVO	Recht auf Datenübertragbarkeit	Der Betroffene hat das Recht seine personenbezogenen Daten in einem gängigen und maschinenlesbaren Format zu erhalten
Artikel 21 EU-DSGVO	Widerspruchsrecht	Der Betroffene hat das Recht, jederzeit der Verarbeitung seiner personenbezogenen Daten zu widersprechen.
Artikel 22 EU-DSGVO	Automatisierte Entscheidungen im Einzelfall einschließlich Profiling	Der Betroffene hat das Recht, nicht einer ausschließlich automatisierten Entscheidung unterworfen zu werden
Artikel 34 EU-DSGVO	Benachrichtigung der von einer Verletzung des Schutzes personenbezogene Daten betroffenen Person	Der Verantwortliche muss den Betroffenen im Falle einer Verletzung des Schutzes seiner personenbezogenen Daten über diese informieren, sofern diese ein hohes Risiko für seine Rechte zur Folge hat.

Tabelle 1: DSGVO Art. mit Inhalten (2)

In den Mitteilungen sind also überwiegen nur Hinweise auf die einzelnen Rechte des Betroffenen einzugehen, und wie er diese wahrnehmen kann. Einige dieser Rechte stehen auch in direkter Kombination zueinander. Möchte ein Betroffenen sein Recht auf Löschung gemäß Artikel 17 EU-DSGVO einfordern, so stehen diesem oftmals gesetzliche

Aufbewahrungspflichten, beispielsweise durch das deutsche Handelsgesetz bedingt, entgegen, weswegen der Verantwortliche diese Daten nicht löschen darf. In der Praxis wird hier oftmals automatisch das Recht auf Einschränkung der Verarbeitung gemäß Artikel 18 EU-DSGVO geltend gemacht, wodurch die Verarbeitung weitestgehend eingeschränkt wird und nur auf ein Minimum reduziert wird.

Artikel 13 und 14 stehen hiervon gesondert, und enthalten in der Praxis keine statischen Informationen. Artikel 13 Absatz 1 EU-DSGVO, „Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person“, beschreibt, welche Informationen dem Betroffen bei der Erhebung mitzuteilen sind, während Artikel 13 Absatz 2 EU-DSGVO die Informationen festlegt, welche zusätzlich zur Verfügung zu stellen sind. Eine Gegenüberstellung dieser verschiedenen Klassen soll in der folgenden Tabelle vorgenommen werden.

Artikel 13 Abs. 1	***Artikel 13 Abs. 2***
Namen und Kontaktdaten des Verantwortlichen	Dauer, für die die personenbezogenen Daten gespeichert werden
Gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten	Bestehen des Rechts auf Auskunft, Widerspruch, Datenübertragbarkeit sowie Berichtigung oder Löschung oder Einschränkung der Daten
Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen sowie die entsprechende Rechtsgrundlage	Bestehen des Rechts auf Widerruf der Einwilligung
Die berechtigten Interessen des verantwortlichen, sollte die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f EU-DSGVO beruhen	Bestehen des Beschwerderechts bei einer Aufsichtsbehörde
Gegebenenfalls die Empfänger oder Kategorie von Empfänger der personenbezogenen Daten	Bestehen der Pflicht zur Angabe von Daten
Gegebenenfalls die Absicht, die personenbezogenen Daten an ein Drittland oder internationale Organisation zu übermitteln, sowie die entsprechenden geeigneten Garantien, welche die Übermittlung zulässig machen würde	Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling

Tabelle 2: Art. 13 und Art. 14 mit Inhalten (2)

In Artikel 14 wird beschrieben, welche Informationen der Verantwortliche dem Betroffenen mitteilen muss, sollten die Daten nicht vom Verantwortlichen selbst erhoben werden. Dies ist nahezu deckungsgleich mit den Informationen, welche laut Artikel 13 EU-DSGVO mitgeteilt werden müssen. Nur die Information aus welcher Quelle diese Daten stammen muss noch zusätzlich genannt werden.

Diese Informationen geben Aufschluss darüber, was der Verantwortliche mit den personenbezogenen Daten macht, und wie er sie verarbeitet. Hier muss entsprechend angegeben werden, wohin die Daten übermittelt werden und welche Daten generell zu welchem Zweck gesammelt werden.

3.2 Facebook

Facebook ist ein soziales Netzwerk, welches von der Facebook Inc. geführt wird. Gegründet wurde es im Jahr 2004 und startete mit Fokus auf Colleges und Universitäten in den Vereinigten Staaten. (5)

Facebook hat eine Useranzahl von mehr als 2 Milliarden Nutzern, die das Netzwerk mindestens einmal im Monat nutzen. Davon nutzen 1,4 Milliarden Nutzer das Netzwerk sogar täglich. Damit ist Facebook das größte soziale Netzwerk der Welt und ist mit 2,167 Millionen monatlichen Nutzern auch das größte Soziale Netzwerk in Deutschland. (6)

Auf der Plattform selbst können sich Nutzer mit anderen Menschen auf der ganzen Welt vernetzen. Es besteht die Möglichkeit, Freundschaften mit anderen Nutzern zu schließen, Mitglied in diversen Gruppen zu werden und Seiten zu abonnieren. Zusätzlich können jeder Nutzer und jede Seite eigene Beiträge erstellen. Diese können aus Texten, Bildern, Videos, Umfragen und Standortmitteilungen bestehen. Jeder Nutzer und jede Seite kann dann auf diese Beiträge entsprechend reagieren, in Form von Reaction-Buttons, einer Gefällt-Mir Angabe sowie das Verfassen von Kommentaren. Beiträge können auch geteilt werden, sodass die Reichweite eines Beitrags durchaus auch über die einzelne Freundesreichweite hinaus gehen kann und mehr Menschen erreichen kann. Die eigenen Profil-Informationen lassen sich individualisieren, sodass der Nutzer selbst bestimmt, welche Informationen das Netzwerk über ihn sammelt. So entsteht für jeden Nutzer ein individuelles Netz aus Informationen, welches für ihn einen eigenen Informationspool bereitstellt, damit das beste Nutzungsergebnis für den Nutzer bereitgestellt werden kann. (7)

Früher einst als Seite für Freunde und Bekannt gestartet, hat sich die Nutzerlandschaft in den letzten Jahren durchaus gewandelt. Viele Unternehmen und Persönlichkeiten nutzen die Plattform, um ihre Marketingstrategie voranzutreiben, da die beschriebene Netzstruktur eine gute Möglichkeit bietet, sich über die eigene Unternehmensreichweite hinaus zu

vermarkten. Ebenso lässt sich direktes Feedback zum Unternehmen geben, da die Nähe zum Nutzer deutlich kürzer ist und er so einfacher seine Meinung zum Produkt oder zum Unternehmen mitzuteilen. (7)

Facebook ist kostenlos nutzbar, doch Facebook schafft es Einnahmen von 13,2 Milliarden Dollar und ein Nettoeinkommen von über 5 Milliarden US-Dollar zu erwirtschaften. Facebook nutzt dafür die von den Usern angegebenen und generierten Daten. Jeder Nutzer gibt durch seine Likes und Posts entsprechend Informationen über seine persönlichen Interessen preis, also was sieht er eher gerne und welcher Freundeskreis sieht diese Interessen. Diese Daten verwendet Facebook, um für den Nutzer individuell Werbung zu schalten und durch diese Werbung entstehen so die Einnahmen von Facebook. Facebook nutzt dafür laut eigener Datenschutzrichtlinie drei Arten von Daten.

Die erste sind die von Nutzern bereitgestellten Informationen, dazu zählen insbesondere die Selbstangaben, die Netzwerke und Gruppenaktivitäten sowie alle weiteren Daten, die die Nutzung betreffen. Auch Daten über Transaktionen, die über Facebook abgewickelt werden, werden gespeichert, sowie Informationen, die andere Nutzer über den Nutzer bereitstellen. Als zweite Art sammelt das Netzwerk Geräteinformationen, um insbesondere die technische Nutzung des Netzwerks zu verbessern, aber auch um Werbeanzeigen besser anzeigen zu können. Insbesondere werden hier dann Daten zu Geräteinformationen gesammelt, darunter Hard- und Softwareversionen, Betriebssysteme, Identifikatoren (für andere Apps oder verknüpfte Produkte) sowie Standort- und Netzwerkdaten. Zuletzt erhält Facebook noch Informationen von Partnern. Diese stellen Facebook ihre eigenen Daten zur Verfügung, um auf der Plattform die Nutzer besser bewerben zu können. Übertragen werden die Daten unabhängig davon, ob der Nutzer ein Facebook-Konto hat. (9)

Facebook nutzt die Daten seiner Nutzer, um für diese personalisierte Werbung zu schalten. Dadurch bietet sich für Unternehmen die Möglichkeit, effektiver und umfangreicher Werbung zu schalten und dadurch generiert Facebook seine Umsätze und Einnahmen. Um diese Umsätze beizubehalten ist es für Facebook von immenser Bedeutung,die Nutzerzahlen beizubehalten und zu steigern, und dabei den Datenschutz seiner Nutzer zu gewährleisten, da aber diese Daten im direkten Verhältnis zum Umsatz des Unternehmens stehen, ist Facebook stets bemüht, möglichst viele Daten seiner Nutzer zu sammeln um die personalisierte Werbung beizubehalten.

Das Datensammeln von Facebook ist umstritten. Immer wieder wird das Unternehmen von Datenschützern kritisiert und zum Teil sogar angeklagt. Der aktuellste Skandal, der sich um Facebook zieht, ist in Kombination mit Cambridge Analytica öffentlich geworden. 2013 bezahlte ein Forscher der Cambridge-Universität 270.000 Facebook Nutzer um an einem Persönlichkeitstest in Form einer App teilzunehmen. Diese App durfte auf die Profilinformationen der Teilnehmer zugreifen, aber zusätzlich auch auf Informationen der Facebook-Freunde der Teilnehmer. Diese Daten von ca. 50 Millionen Facebook-Nutzern wurden für politische Werbung genutzt, ohne dass der Großteil dieser Nutzer davon in Kenntnis gesetzt

wurde. Facebook informierte weder die Nutzer, noch schränkte es diese Nutzung bis zum Jahr 2014 ein, und auch dann nicht im vollen Umfang. (10)

Durch die Größe des Unternehmens, seiner Art der Datenkollekte sowie seiner umstrittenen Vergangenheit in Bezug auf Datenschutz wurde Facebook als praktisches Beispiel herangezogen, um festzustellen, in wie weit es möglich ist, mithilfe der neuen Gesetze forensische Arbeit zu leisten und zu unterstützen. In Deutschland arbeiten aktiv das Bundeskriminalamt, die Bundespolizei und der Zollfahndungsdienst mit sozialen Netzwerken zusammen, um so ihre Ermittlungen voranzutreiben (11). Daher ist es nicht gerade unerheblich aufzuschlüsseln, welche Daten von Facebook gesammelt werden und in welchem Umfang diese bereitgestellt werden können.

3.3 Praktisches Beispiel: Facebook

In diesem Abschnitt soll überprüft werden, inwieweit die genannten theoretischen Gesetze praktisch umgesetzt werden. Dafür wird beim sozialen Netzwerk Facebook das Recht auf Auskunft durch einen Nutzer wahrgenommen, und die erhaltenen Daten werden dann analysiert und aufbereitet. Besonders hinsichtlich der Verwendung dieser Daten in Bezug auf forensische Untersuchungen werden diese dann bewertet und nach ihrer Relevanz beurteilt. Mögliche Probleme und Hindernisse werden erläutert und dargestellt.

Das Recht auf Auskunft wurde im praktischen Beispiel von einem langjährigen Nutzer wahrgenommen und die erhaltenen Daten wurden analysiert. Es wurde sich bewusst für einen bereits bestehenden, das soziale Netzwerk jahrelang nutzenden Nutzer entschieden und kein „künstlicher“ Nutzer extra für die Bearbeitung angelegt, um den realen Bezug besser integrieren zu können. Bei einem künstlichen Nutzer besteht die Gefahr, Daten anzulegen, die in der Praxis niemals zustande kommen. Durch die Analyse eines normalen Standardnutzers bietet sich die Möglichkeit, die durch tatsächliche und normale Nutzung entstehenden Daten zu erhalten. Es besteht auch die Möglichkeit, als Nicht-Nutzer die Daten von Facebook zu erhalten, allerding benötigt dies einen erweiterten Prozess mit einem Authentifizierungsnachweis.

Um an die Daten zu gelangen, muss sich der Nutzer bei Facebook einloggen, mit Nutzermail und Passwort, und sich über die Einstellungen zum Feld „Deine Facebook-Informationen“ navigieren. Dort kann er dann die Daten erhalten. Facebook stellt zwei Möglichkeiten zur Verfügung, mit der man seine personenbezogenen Daten anfordern kann. Zum einen ermöglicht es Facebook, online direkt seine Daten einzusehen. Zusätzlich stellt Facebook noch ein weiteres Tool zur Verfügung, mit dem man diese Daten herunterladen kann. Zur Datenerhebung wurde das Download-Tool verwendet, später wird im Abschnitt 3.3.2 auf die Unterschiede der zwei Werkzeuge eingegangen.

Um die Daten zu downloaden, muss man diese entsprechend auswählen, also welche Daten von Facebook konkret zum Download zur Verfügung gestellt werden, wie beispielswiese Beiträge, Suchverlauf etc. Die Daten können im HTML Format ausgewählt werden oder im JSONS-Format. Laut Facebook soll das HTML-Format zur Übersicht der Daten besser geeignet sein, während das JSONS-Format bei anderen Diensten besser implementiert werden kann. Ein Grund für diese zwei Formate ist das Recht auf Datenübertragbarkeit nach Artikel 20 EU-DSGVO, in dem festgelegt ist, dass ein Nutzer das Recht darauf hat, seine Daten in einem gängigen und maschinenlesbaren Format zu erhalten. Würde ein Facebook-Nutzer planen das soziale Netzwerk zu verlassen und sich bei einem anderen Netzwerk anzumelden, so könnte er seine Daten im JSONS-Format übertragen, damit der neue Anbieter seine alten Daten direkt übernehmen kann.

Im konkreten Beispiel wurde das HTML-Format gewählt, um die bessere Übersicht über die Daten zu erhalten. Es wurden alle Daten angefordert, die man anfordern konnte, sowie die Medien in hoher Qualität, welches Facebook ebenfalls als Option eingefügt hat, um gegebenenfalls die Datenmenge zu reduzieren, sollten es zu viele Daten zum einfachen Transfer werden. Per Mail und über Facebook selbst erfolgt dann die Benachrichtigung, dass die Daten nun heruntergeladen werden können, was direkt von der Facebook-Plattform aus erfolgen kann.

3.3.1 Beschreibung der erhaltenen Daten

Hier wird eine Übersicht über die erhaltenen Daten gegeben, und alles bezüglich der Daten, ohne Bewertung der Relevanz oder ähnlichem geführt.

Die Daten wurden von Facebook am 24. Juli 2018 um 14:06h angefordert, und standen innerhalb von 6 Minuten zur Verfügung. Die erhaltene ZIP-Datei war 14,0 MB groß (14.760.765 Bytes), entpackt waren es 29,7 MB (31.159.484 Bytes).

Enthalten sind 275 Ordner mit 344 Dateien. Man kann die einzelnen HTML-Dateien direkt aus dem Ordner öffnen, oder über die index.html Datei navigieren, welche automatisch die entsprechenden Dateien öffnet. Eine Bildschirmaufnahme dieser Navigationsansicht findet sich in den Anlagen (Anlage Teil I). Design-technisch lehnen sich die HTML-Seiten am Standard-Facebook Design an, welches stark dem Startbildschirm der Beiträge ähnelt. Es existieren 24 Stammordnern, in denen die weiteren HTML-Dateien und gegebenenfalls andere Dateien existieren. Eine Übersicht kann dem folgenden Bild entnommen werden.

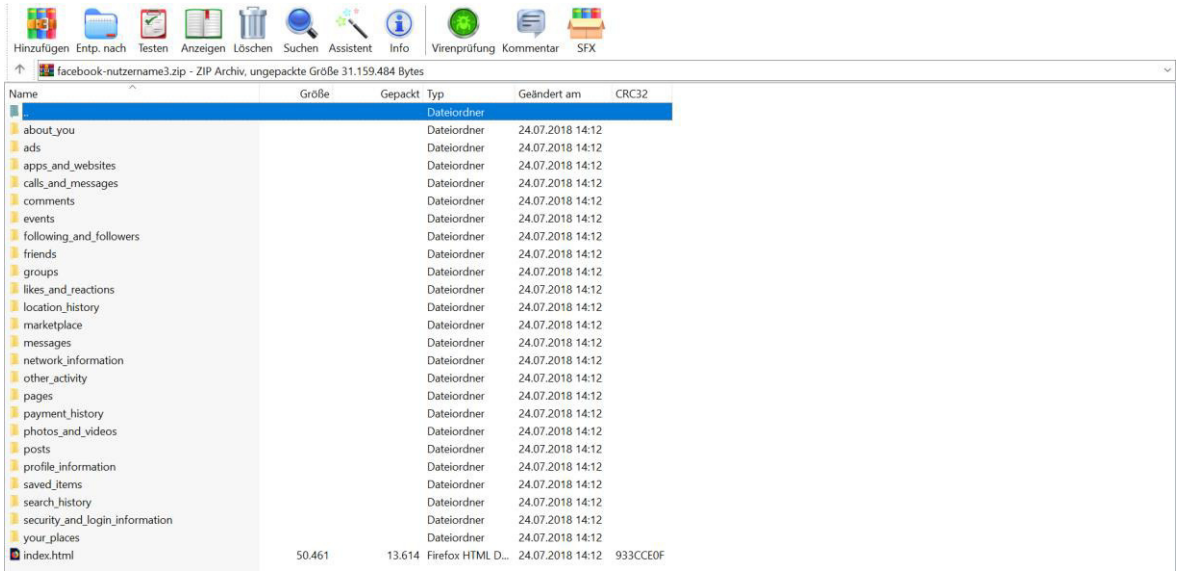


Abbildung 2: Inhaltsübersicht Stammordner

Innerhalb dieser Stammordner werden die einzelnen HTML-Dateien zu den einzelnen Informationen geführt. In Ordnern, in denen keine Daten geführt werden, ist eine .txt-Datei enthalten, in der folgender Text steht: „Du hast keine Daten in diesem Abschnitt“.

Im Folgenden werden die Stammordner jeweils einzeln betrachtet, da jeder einen eigenen Bereich abdecken soll. Die einzelnen Dateien und ihre Inhalte werden beschrieben, sofern sie im erhaltenen Datensatz enthalten sind.

Im Stammordner about_you findet sich nur eine HTML-Datei mit dem Namen friend_peer_group.html. In dieser wird die Peer-Group der Freunde des Betroffenen benannt. Facebook erstellt also aus der Freundesliste des Nutzers eine „Beschreibung des Lebensabschnitts deiner Freunde auf Facebook“, um so gezielter den User selbst verordnen zu können. Konkrete Bezeichnungen sind beispielsweise „Universität“, „Am Anfang des Erwachsenenlebens“ oder auch „Etabliertes Erwachsenenleben“. Facebook macht sich hier zu Nutze, dass Menschen in der Altersgruppe von 18-29 überwiegend Freunde suchen, die den gleichen Bildungsabschluss besitzen, sowie eher ältere Freunde als jüngere Freunde haben (28). Anhand dieser Einordnung können dann spezifischere Werbeinhalte geschaltet werden, sowie die Beiträge von Freunden hervorgehoben werden, die in einer ähnlichen Lebenssituation sind und so für den Nutzer interessanter sind.

Im nächsten Stammordnern werden die Daten über die „ads“, also die auf Facebook für den Nutzer geschaltete Werbung, präsentiert. Dies erfolgt in drei HTML-Dateien. In ads_interests.html werden die Interessen für Werbung gesammelt, basierend auf „Facebook-Tätigkeiten und anderen Handlungen, mit deren Hilfe wir dir relevante Werbung zeigen“ (35).

Die Interessen des Beispiel-Nutzers erstrecken sich über diverse Sportarten, verschiedene Musikrichtungen und Musikgruppen, welche konkret benannt werden, ebenso wie einzelne

Sportler, sowie politische Parteien. Nicht alles ist konkret benannt, es finden sich auch allgemeinere Begriffe wie „Staunen“, „Republik“, „Welt“ oder „Mediziner“.

Eine Übersicht über die Kategorien der einzelnen Werbebegriffe wird nicht bereitgestellt. Im folgenden Diagramm wurden den Begriffen Kategorien zugeordnet und dargestellt.

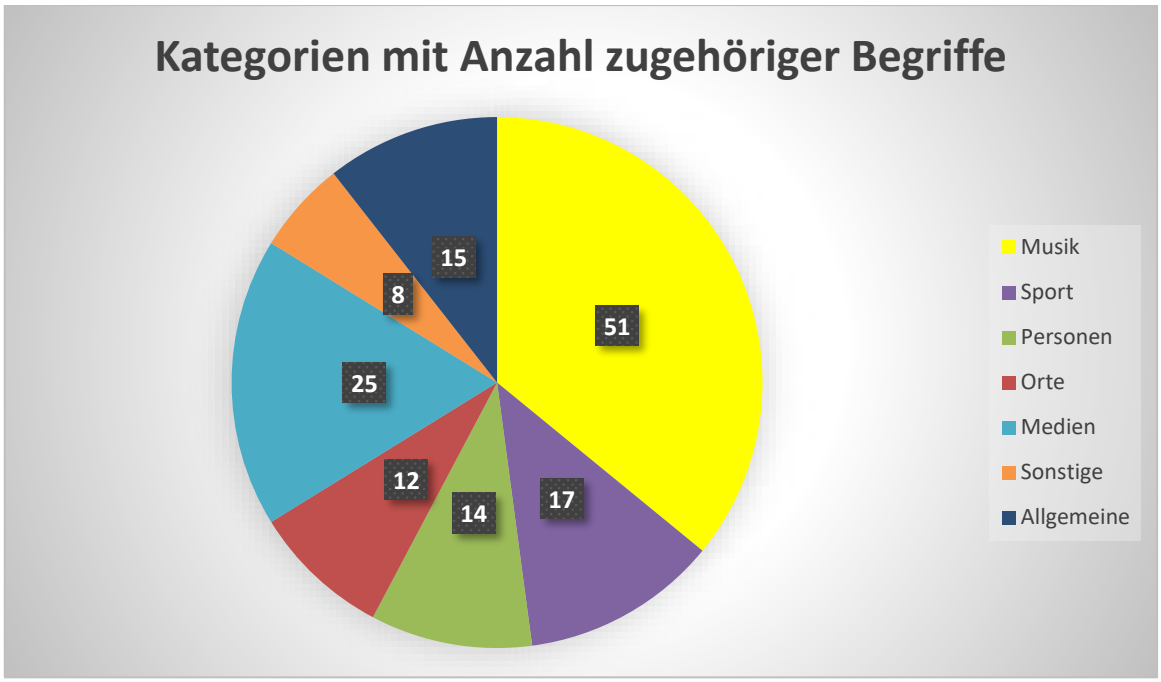


Abbildung 3: Werbekategorien Übersicht

Überwiegend treffen die Begriffe auf den Nutzer zu, die Begriffe die unter „Allgemeine“ abgelegt werden als Standard Werbebegriffe aufgefasst. Die übrigen Begriffe sind individuell zusammengesetzt, aus seinen „Gefällt Mir“-Angaben, seinen angegebenen Interessen sowie Assoziationen zwischen den einzelnen Begriffen. Dadurch ergibt sich ein klares Interessenbild des Nutzers, sodass Facebook mithilfe dieser personenbezogenen Daten gezielt Werbung für den einzelnen Nutzer schalten kann.

In den weiteren Dateien im Stammordner „ads“, „advertisers_you´ve_interacted_with.html“ sowie „advertisers_who_uploaded_a_contact_list_with_your_information.html“, werden die Werbeanzeigen aufgeführt, mit denen der Nutzer interagiert hat, sowie die Informationen über Werbetreibende, „die anhand einer hochgeladenen Kontaktliste mit Kontaktdaten, die du mit ihnen oder einem deren Datenpartner geteilt hast, Werbung schalten“. Insbesondere werden hier die Werbetreibenden genannt, die ihre Daten an Facebook weitergeben, um so effektiv eigene Nutzer auf der Plattform bewerben zu können. Erkennt Facebook eine gemeinsame Schnittstelle, beispielsweise die verwendete E-Mail-Adresse, so verknüpft Facebook diesen Nutzer mit dem Werbetreibenden. Es wird aber nur der Name des Werbetreibenden gespeichert, wann, woher und auf welcher Grundlage diese Verknüpfung zu Stande kommt wird nicht gespeichert.

Anders bei den Werbeanzeigen, mit denen der Nutzer interagiert hat. Hierbei speichert Facebook neben dem Namen der entsprechenden Werbeanzeige auch das Datum sowie die Uhrzeit, wann der Nutzer die Werbeanzeige angeklickt hat. Informationen zum Standort, dem Gerät oder dem Werbetreibenden werden nicht aufgeführt.

Die Werbeanzeigen sind chronologisch aufsteigend sortiert, der letzte Eintrag datiert vom 27. Mai 2018 um 21:05, insgesamt werden 14 Werbeanzeigen aufgeführt, mit denen der Nutzer interagiert hat.

Der dritte Stammordner „Apps_and_websites“ enthält nur die „posts_from_apps_and_websites.html“-Datei, in welcher die Beiträge von Apps und Websites gespeichert sind, die im Namen des Users posten dürfen. Hier lassen sich nicht nur die im eigenen Namen verfassten Posts einsehen, sondern auch die, die im Namen von Facebook-Freunden durch die App verfasst wurden. Gespeichert werden dabei der Zeitpunkt des Posts, der Name des Nutzers, in dessen Namen die Beiträge verfasst werden sowie der tatsächlich postenden App.

Der Stammordner „calls_and_messages“ enthält prinzipiell die „Protokolle deiner Anrufe und Nachrichten, die du in deinen Geräteeinstellungen zum Teilen freigegeben hast“. Also werden hier nur Daten erfasst, wenn der Nutzer diese ausdrücklich auf seinem mobilen Endgerät freigibt. Zu diesen Daten zählen insbesondere Namen, Telefonnummern und die Länge des Anrufs, auch Short-Message Service (SMS) Nachrichten, welche über die Nutzungsgeräte verschickt werden (27).

Die Kommentare, welcher der Nutzer auf Facebook unter den verschiedensten Beiträgen platziert, werden im Stammordner „comments“ und der darin enthaltenen „comments.html“-Datei gespeichert. Gespeichert werden der Inhalt der Kommentare, der Verfasser des Beitrags sowie Datum und Uhrzeit. Diese sind absteigend sortiert, der letzte Beitrag und damit erstmals verfasste Kommentar stammt aus dem November 2010, also kurz nach Erstellen des Accounts. Insgesamt werden mehr als 1000 Kommentare gespeichert.

Stammordner „events“ enthält wieder drei HTML-Dateien. In „event_invitations.html“ werden die eingegangenen Einladungen zu Veranstaltungen gespeichert. Hinterlegt sind der Name der Veranstaltung und der Zeitpunkt wann die Veranstaltung stattgefunden hat, allerdings nicht wer die Einladung versendet hat oder wann die Einladung erhalten wurde. Die älteste Veranstaltung, zu der der Nutzer eingeladen wurde datiert aus dem Jahr 2011.

In „your_events“ werden alle vom Nutzer erstellten Veranstaltungen gespeichert, inklusive Name, Ort, Zeitpunkt der Veranstaltung sowie der Zeitpunkt, an dem die Veranstaltung stattgefunden hat. In der dritten Datei, „your_events_responses.html“ sind die Veranstaltungen abgelegt, auf die der Nutzer konkret reagiert hat, also Zusagen, Absagen oder interessiert/ Vielleicht. Sortiert sind sie nach diesen Kategorien, absteigend von der neusten Veranstaltung bis zur letzten. Gespeichert werden jeweils der Name der Veranstaltung und das Datum, wann die Veranstaltung stattgefunden hat. Auch hier gehen die

Veranstaltungen bis 2011 zurück, was den Schluss nahelegt, dass Facebook bei den „Event-Daten“ eine längere Aufbewahrungsfrist nutzt als beispielsweise bei den Werbeanzeigen.

Im Ordner „following_and_followers“ findet sich eine HTML-Datei names “unfollowed_pages.html“, die Angaben über jene Seiten enthält, welche der Nutzer bewusst entfolgt hat. Seiten, die einst mit „Gefällt-Mir“ markiert waren und damit automatisch abonniert wurden, welche „entliked“ und automatisch de-abonniert wurden, werden allerdings nicht aufgeführt, sondern nur jene, bei denen bewusst der Abonniert-Status entfernt wurde. Aufgeführt wird der Name der Seite sowie das Datum, an dem der Seite nicht mehr gefolgt wurde, inklusive Uhrzeit.

Einer der größeren Stammordner ist der „friends“-Ordnern. Hier werden alle Informationen zu den Freunden, die der Facebook-Nutzer auf Facebook hat, angezeigt. In der „friends.html“-Datei werden die Freunde aufgeführt, mit Namen und Datum, wann die Freundschaft bestätigt wurde. Die Liste geht entsprechend bis 2010 zurück, ab dem Zeitpunkt, an dem die erste Freundschaft auf Facebook geschlossen wurde.

Wurde nur die Freundschaftsanfrage erhalten, aber weder bestätigt noch abgelehnt, so werden diese in der „received_friend_requests.html“-Datei abgelegt. Enthalten sind dort Name der Person sowie das Datum, an dem die Freundschafts-Einladung eingegangen ist. Abgelehnte Freundschaftsanfragen werden in der „rejected_friend_requests.html“ abgelegt, mit Namen der Person sowie einem Datum, wobei nicht eindeutig ist, ob es sich um das Datum des Eingangs der Freundschaftsanfrage oder dem Datum der Freundschafts-Ablehnung handelt. Da alle Daten aber nach demselben Schema abgespeichert sind, ist davon auszugehen, dass es sich um den Zeitpunkt der Freundschafts-Ablehnung handelt. In der letzten Datei, „removed_friends.html“ sind die gelöschten Freunde abgespeichert, mit Namen und dem Zeitpunkt, an dem der Freund aus der Freundesliste entfernt wurde.

Der „groups“-Ordner enthält die Daten bezüglich der Gruppenaktivitäten des Users. In der „your-groups.html“-Datei finden sich die Gruppen wieder, die der User als Administrator betreut und die von ihm gegründet wurden, abgelegt werden die Gruppen mit Namen und Datum der Erstellung. In der „your-posts_and_comments_in_groups.html“-Datei werden alle Beiträge und Kommentare, die der Nutzer in Gruppen, in denen er Mitglied ist, verfasst hat, angezeigt. Handelt es sich um direkte Beiträge so wird angezeigt, in welcher Gruppe er was gepostet hat und wann er es gepostet hat. Handelt es sich um Kommentare auf die Beiträge von anderen, so wird abgespeichert, um wessen Eintrag es sich handelt, in welcher Gruppe der Beitrag gepostet wurde, der Inhalt des Kommentars, sowie der Zeitpunkt der Verfassung. In der letzten Datei, „your-group_membership_activity.html“, werden die Daten zu Beitrittsanfragen protokolliert, also wann der Nutzer bei welcher Gruppe akzeptiert wurde, als Daten werden der Name der Gruppe, sowie das Datum und die Uhrzeit der Bestätigung abgespeichert. In allen drei Dateien fehlen aber Angaben zu den Gruppen, in denen der User Mitglied ist. Es werden nur die gelistet, welche seine Beitrittsanfrage bestätigt haben, aber nicht in welche er so hinzugefügt wurde ohne eine Beitrittsanfrage zu

versenden. Auch werden keine Angaben über die Gruppen geführt, in denen der Nutzer Mitglied gewesen ist und aus denen er ausgetreten ist.

Als nächsten Stammordner gibt es den „likes_and_reactions“ Ordner, welcher alle „Gefällt-Mir“-Angaben sowie sonstige weitere Reaktionen auf einzelne Beiträge enthält. In der „posts_and_comments.html“-Datei werden die Reaktionen auf die Beiträge gespeichert, mit Angabe zum entsprechenden Beitrag, um was für einen Beitrag es sich handelt (Foto, Beitrag/Video), von wem der Beitrag stammt, gegebenenfalls in welcher Gruppe der Beitrag veröffentlicht wurde, sowie der Zeitpunkt der Reaktion mit Datum und Uhrzeit. Die Reaktionen sind von der neusten bis zur ältesten sortiert und gehen bis ins Jahr 2010 zurück.

In der „pages_html“-Datei werden die „Gefällt-Mir“ Angaben zu Facebook-Seiten gespeichert, jeweils mit Datum und Zeitpunkt der Aktion sowie dem Namen der Seite. Auch hier werden die Aktionen absteigend nach Datum sortiert und gehen bis Anfang 2011 zurück.

Es fehlen Angaben zu Seiten, die der Nutzer einmal mit „Gefällt-Mir“ markiert hat und zu einem späteren Zeitpunkt wieder „entliked“, also die Gefällt-Mir-Markierung entfernt hat.

Im Ordner „location-history“ sollen Orte aufgeführt werden, an denen der Nutzer gewesen ist und sich mit dem sozialen Netzwerk verbunden hat. Dazu nutzt Facebook die Ortungsdienste des Gerätes und kann so den genauen Standort des Nutzers ermitteln und aufzeichnen.

Zusätzlich finden sich im nächsten Stammordner „marketplace“, welcher die Aktivitäten auf dem Facebook-eigenen Marketplace, auf dem Dinge zum Verkauf angeboten und gekauft werden können, aufzeichnet. Die einzelnen durchgeführten Transaktionen werden hier aufgelistet.

Der mit Abstand größte Ordner ist der „messages“-Ordner. Hier werden alle Konversationen, die der Nutzer über den Messenger-Dienst abschließt abgespeichert. Im Ordner selbst findet sich für jede Konversation ein weiterer Ordner. Der Name des Ordners setzt sich dabei aus dem Namen des Gesprächspartners oder, im Falle von Gruppenkonversationen, mit den Vornamen der beteiligten Personen, wobei bei Konversationen mit mehr als drei weiteren Teilnehmern nach den alphabetisch erstgenannten drei Teilnehmern mit „undXweiterenPersonen“ genannt wird, ohne weitere Teilnehmer zu nennen- Nutzer, welche nicht mehr im sozialen Netzwerk aktiv sind und ihren Account gelöscht haben werden als „facebooknutzer“ bezeichnet. Hinter dem Namen oder der Bezeichnung findet sich noch eine Zeichenkette, welche aus 10 Zeichen besteht und die aus den Zahlen von null bis neun sowie den Buchstaben A bis E (jeweils kleingeschrieben) bestehen kann.

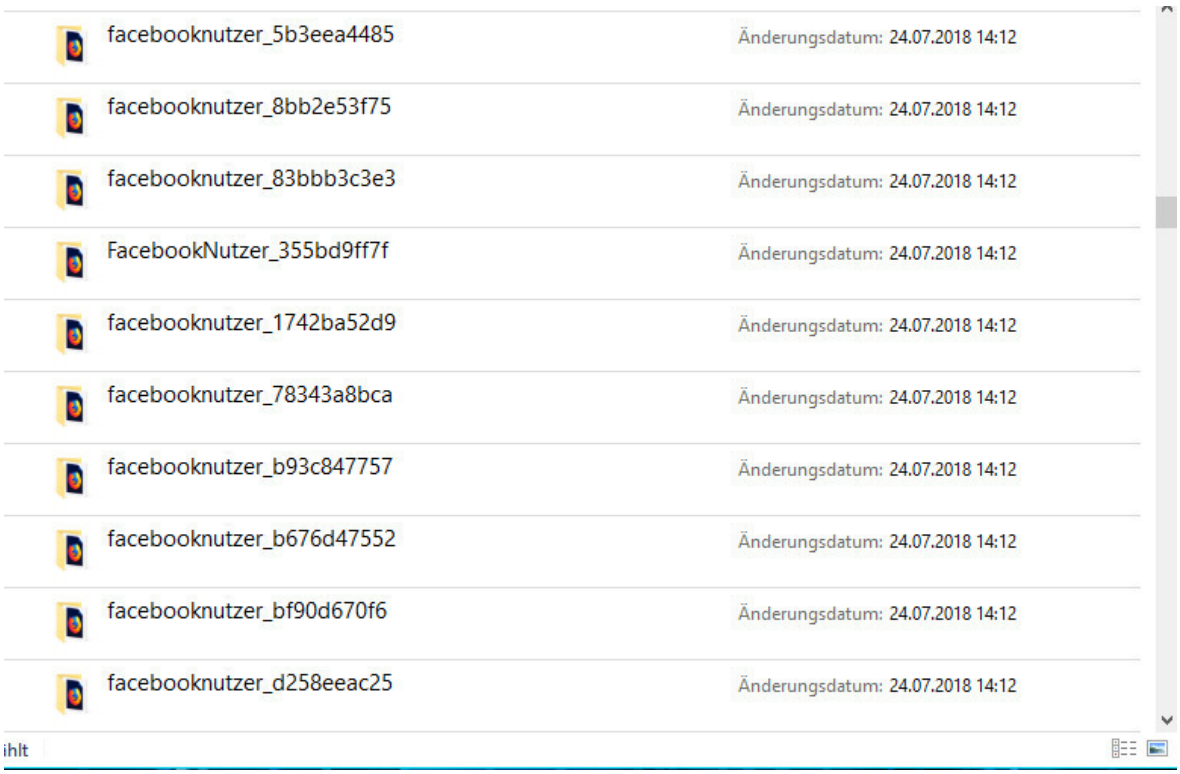


Abbildung 4: Ansicht "Messages Ordner"

Es ist nicht eindeutig, wie sich diese Zeichenkette zusammensetzt, noch was sie beschreibt. Prinzipiell könnte man annehmen, dass es sich um eine eindeutige Prüfsumme handelt, die im Hexadezimal-Code codiert ist und für jede Konversation eindeutig ist. Die lässt sich aber schnell wiederlegen.

Bei zehn Bytes steht eine maximale Spanne von möglichen 1.099.511.627.775 Trilliarden Nummern zur Verfügung (maximale hexadezimale Zahl FF FF FF FF FF). Facebook gibt selbst in seinem Jahresbericht 2017 ihres Dienstes „Messenger“ an, dass es im Durchschnitt am Tag zu 260 Millionen neuen Konversationen auf der Plattform kommt (30). Übertragen auf Facebook, von wo aus auf dieselben Konversationen zugegriffen wird, würde also die Menge an Prüfsummen theoretisch ausreichen, um ca. 4.229 Tage lang Konversationen mit einer eindeutigen Prüfsumme zu klassifizieren, umgerechnet ca. 11,75 Jahre. Das soziale Netzwerk existiert aber bereits seit 2004, also bereits 14 Jahre. Auch wenn in den ersten Jahren des Netzwerks nicht die Menge an Konversationen erstellt wurden wie es heute der Fall ist, so dürften sie doch mittlerweile an einer Kapazitätsgrenze angelangt sein, was die verbliebene Anzahl an individuellen Prüfsummen anbelangt. Einen Zeitstempel kann man auch ausschließen, da nahe gelegene neu angelegte Konversation deutlich unterschiedliche Zeichenketten haben und sich nicht in die üblichen Zeitstempel umwandeln lassen.

Mit einem anderen Datensatz abgeglichene Daten zeigen, dass die Nummer nicht individuell für die einzelne Konversation ist. Dazu wurden die Daten eines Facebook Nutzers angefordert, welcher mit dem Beispielnutzer eine Konversation hielt. Die abgeglichenen

Personen teilten einen gemeinsamen Konversationsverlauf, besaßen aber unterschiedliche Zeichenketten nach dem Namen des Konversationspartners. Eine übergreifende, konversationsspezifische und alleinstehende Prüfnummer lässt sich so ausschließen. Ein kryptographisches Verfahren oder eine Kombination aus Zeichenkette mit dem Nutzernamen können weiterhin denkbar sein, aber nicht eindeutig belegbar.

Im Ordner selbst befindet sich jeweils eine HTML-Datei „messages.html“ in welcher der komplette Nachrichtenverlauf seit Beginn der Konversation aufgelistet ist. Sollten in Laufe der Konversation Dateien ausgetauscht worden sein, so wird ein weiterer Ordner angelegt. Der Ordner enthält dann den Namen der ausgetauschten Datei wie beispielsweise „photos“ oder „files“. Die gesendeten Dateien werden entsprechend in diesen Ordnern abgelegt.

Im Stammordner „network_information“ sind Informationen zu den verwendeten Netzwerken zu finden.

Der Ordner „other_activity“ enthält die Aktivitäten, die dem Konto zugeordnet werden können, aber nicht in die anderen Bereiche eingeordnet werden können. Hierzu zählen Umfragen von öffentlichen Seiten, keine Gruppenumfragen oder Umfragen mit eingegrenztem Nutzerbereich, oder auch Aktivitäten der Facebook-Funktion „Anstupsen“. Mit dieser Funktion kann man einen anderen Nutzer anstupsen, das heißt dieser bekommt eine Benachrichtigung, dass der andere Nutzer ihn angestupst hat. Mehr beinhaltet dieses Feature nicht, es lassen sich also hiermit keine Nachrichten austauschen oder sonstige Aktivitäten nachweisen. Gespeichert wird in diesem Ordner dann für jede Aktivität eine eigene Datei, wie beispielsweise „polls_you_voted_on.html“. Im Detail werden bei Umfragen der Name des Nutzers, dem Ersteller der Umfrage, dem Datum der Aktivität sowie der gegebenen Antwortmöglichkeit.

Der Ordner „pages“ enthält Verweise auf die Seiten, bei denen der Nutzer als Administrator aktiv ist. Gespeichert werden hier die Namen dieser Seiten.

Sollte der Nutzer Zahlungen auf Facebook tätigen, so wird dieser Zahlungsverlauf im Ordner „payment_history“ gespeichert. Sind keine Zahlungen getätigt worden, so enthält der Ordner lediglich die Information zur bevorzugten Währung des Nutzers, in der Regel die Währung seines Heimatlandes.

Die Fotos und Videos, die der Nutzer auf Facebook hochlädt werden im Stammordner „photos_and_videos“ gespeichert. Unterteilt werden diese nach der Art wie sie hochgeladen wurden. Entsprechend enthält der Unterordner „your_posts“ die Fotos, welche der Nutzer als Post in einer Gruppe oder anderweitig als Kommentare gepostet wurden. Diese werden über die Navigationsübersicht der HTML-Seiten allerdings nicht im Ordner „Fotos und Videos“ angezeigt, sondern dort werden lediglich die Fotos/Videos angezeigt, die der Nutzer explizit geteilt hat. Im Ordner „stickers_used“ sind die Standard-Emoticons abgelegt, welche der Nutzer verwenden kann, um auf Beiträge zu reagieren. Der Ordner „album“ enthält eine HTML-Datei, die entsprechend für die erstellten Foto-Alben des Nutzers generiert wird

und alle Bilder enthält sowie einige Meta-Informationen. Diese enthalten das Format, die ursprüngliche Breite und Höhe, die ISO-Empfindlichkeit sowie die IP-Adresse, von der das Bild hochgeladen wurde. Zusätzlich werden die Profilbilder noch einmal zusätzlich in einem Ordner abgelegt, welcher den Namen „Profilbilder“ sowie eine Kennzahl enthält. Alte Bilder, die gelöscht worden sind, sind dort nicht zu finden.

Der Stammordner „posts“ enthält alle Informationen zu Postings, die der Nutzer erstellt hat oder die auf seiner Pinnwand von anderen Nutzern gepostet wurden. Aufgelistet werden diese in zwei Dateien, „your_posts.html“ für die eigenen Posts, „other_people´s_posts_to_your_timeline.html“ für nicht-eigene Posts. Sortiert werden diese wieder chronologisch absteigend, vom neusten Post bis zum letzten. Gespeichert werden alle Posts, sofern sie nicht gelöscht wurden, mit den Informationen zum Zeitpunkt des Posts, Datum und Uhrzeit, in welcher Gruppe oder an wessen Pinnwand der Beitrag gepostet wurde und bei fremden Posts wer den Beitrag verfasst hat.

Profilinformationen, die der Nutzer Facebook zur Verfügung stellt werden im Stammordner „profile_information“ gespeichert. Auch hier werden zwei Dateien angelegt, eine Datei, die die angegebenen Informationen enthält sowie eine die den Verlauf der Änderungen im Profil enthält. „profile_information.html“ speichert dabei alle selbst angegeben Daten. Hierzu zählen der gewählte Name, der Geburtstag, das Geschlecht, das Geschlecht, an dem der Nutzer interessiert ist, also seine sexuelle Neigung, Wohnort, Familienmitglieder, seine Ausbildung inklusive derer, die angegeben haben diese Ausbildung gemeinsam abgeschlossen zu haben, sowie seine Interessen in den Bereichen, die er persönlich angeben kann. Zusätzlich existiert hier eine Übersicht über die Gruppen, in denen der Nutzer aktiv ist, sowie sein Datum der Registrierung bei Facebook, seine angegebenen Mail-Adresse sowie die eigene Facebook-Mail-Adresse und ein Link zum eigenen Profil. Änderungen, die der Nutzer in diesen Kategorien vornimmt werden entsprechend werden in der Datei „profile_update_history.html“ abgespeichert, zusammen mit Änderungen des Profilbilds. Diese Änderungen werden bis zum Tag der Registrierung rückwirkend gespeichert, inklusive der Angabe wann diese Änderung vorgenommen wurde.

Facebook besitzt die Funktion, bestimmt Beiträge zu speichern. Diese gespeicherten Beiträge werden im Ordner „saved_items“ abgespeichert. In der enthaltenen HTML-Datei „your_saved_items.html“ werden allerdings nur das Datum der Speicherung, die Art des gespeicherten Beitrags (Beitrag, Foto, Video etc.) sowie eine Angabe zum Verantwortlichen, der den entsprechenden Beitrag veröffentlicht hat.

Suchanfragen auf Facebook werden im Ordner „search_history“ und der Datei „your_search_history.html“ gespeichert. Enthaltene Daten sind der Zeitpunkt der Suche sowie dem gesuchten Begriff.

Gespeichert wurden 79 Suchanfragen, die bis zum 14. Februar 2018 zurückreichen, diese Daten behält Facebook also nicht solange wie beispielsweise Profilinformationen oder Nachrichtenverläufe.

Ein weiterer umfangreicher Ordner ist der „security_and_login_information“ Ordner. Hier sind alle Informationen hinterlegt, die im Rahmen von Anmeldungen anfallen und gespeichert werden, aufgeteilt in sechs HTML-Dateien. In der ersten Datei „account_activity.html“ sind die Daten zu Kontoaktivitäten abgespeichert. Dazu zählen Logins, Session-Updates und beendete Web-Sessions. Die einzelnen Aktivitäten werden von der neusten Aktivität zur ältesten Aktivität abgespeichert, die älteste datiert aus dem August 2017. Erfasst werden konkret die Zeit der Aktivität, von welcher IP-Adresse und welchem Browser die Aktivität ausgeführt wurde sowie des dazugehörigen Cookies, der nach vier Zeichen anonymisiert ist. Für den Beispielnutzer wurden 855 Aktivitäten gespeichert.

Die Datei „administrative_records.html“ enthält weitergehende Informationen zu administrativen Aktionen auf dem Konto, wie beispielsweise Sicherheitsüberprüfungen, Passwort-Wechseln, Profil-Informationsänderungen (Profilfoto, Geschlecht, Name etc.) sowie Rechtevergaben für Gruppen. Hierbei wird zusätzlich zur Art der Aktion allerdings nur der Zeitpunkt mit Datum und Uhrzeit sowie die IP-Adresse gespeichert.

In der „login_protection_data.html“ werden „Daten zum Anmeldeschutz“ gespeichert. Sobald sich ein User bei Facebook anmeldet, erhält dieser einen Cookie, der sein Nutzungsverhalten erfasst und analysierbar macht. Diese Cookies werden in dieser Datei gespeichert, mit anonymisiertem Namen, Erstellungsdatum sowie dem letzten Aktualisierungszeitpunkt, erfasst werden genau 100 Cookies, der älteste aus dem September 2017. Nach der Auflistung der Cookies erfolgt in derselben Übersicht eine Auflistung der IP-Adressen, mit Erstellungs- sowie Aktualisierungsdatum. Es werden sowohl IPv4, als auch IPv6 Adresse abgespeichert. Bis zum Juni 2017, in dem der älteste Eintrag einer IP-Adresse erstellt worden ist, wurden 34 IP-Adressen erfasst.

Abschließend werden noch anhand der IP-Adressen ermittelte ungefähre Standorte verzeichnet. Dabei schwanken die bereitgestellten Informationen stark. Immer angegeben werden Längen- und Breitengrade sowie das Erstellungsdatum. Bei Aktualisierungen wird ebenfalls das Aktualisierungsdatum aufgeführt, aber nur in vier Fällen wird die tatsächlich verwendete IP-Adresse, anhand derer der Standort ermittelt wurde, genannt.

Auch wird nicht jede IP-Adresse aufgelistet, es werden nur 12 Standorte bis zum Juli 2017 aufgeführt, also ein ähnlicher Zeitraum, in dem Facebook 34 verschiedene IP-Adressen erfasst hat und also durchaus mehr Standorte hätte verzeichnen können.

„Logins_and_logouts.html“ enthalten die Daten zu den Anmeldungen und Abmeldungen im sozialen Netzwerk. Gespeichert wird hier, ob es sich um einen An- oder Abmeldevorgang handelt, die Zeit, die IP-Adresse sowie die Website oder die entsprechende Applikation, von der der Nutzer sich angemeldet hat. Die älteste Anmeldung datiert vom September 2017, gespeichert werden 199 An- und Abmeldevorgänge.

Die in der „login_protection_data.html“ erfassten 34 IP-Adressen werden in der „used_ip_adresses.html“ erneut aufgeführt, allerdings ohne das Erstellungsdatum, geschätzten Standort oder weitere Daten, sondern nur die reine IP-Adresse.

Die letzte Datei im Ordner „security_and_login_information“ ist die „where_you´re_logged_in.html“. Diese soll Zeitintervalle aufführen, in denen der Nutzer aktiv auf Facebook angemeldet war. Tatsächlich werden aber nur die Zeitdaten genannt, wann der Nutzer aktiv wurde, also das Event erstellt wurde, und gegebenenfalls wann dieses wieder aktiviert wurde, aber keine Angabe wann der Status des aktiven Anmeldens beendet wurde. Allerdings werden hier alle Informationen aus den vorherbeschriebenen Dateien zusammengeführt, zumindest ein Großteil dieser. Sortiert sind diese wie üblich, herabsteigend vom neusten bis zum letzten Event. Als Daten enthalten sind für jedes Event das Erstellungsdatum, der Ort, benannt mit Name sowie dem Land, der IP-Adresse, dem verwendeten Browser oder der verwendeten App, dem gesetzten anonymisierten Cookie, sowie einer Angabe über das Gerät welches verwendet wurde, allerdings nur mit prinzipieller Typ-Kennung. Ein Laptop wurde als „Windows-PC“ erkannt oder ein Smartphone als „Sony Xperia“, aber keine weitere eindeutige Seriennummer oder Gerätekennzeichnung. Aufgeführt werden 39 Events, zurückreichend bis zum Juli 2017.

Abbildung 5: Inhalt "where_you´re_logged_in.html" (anonymisiert)

Der letzte der Stammordner ist der „your_places“ Ordner, welcher die Orte enthalten soll, welche der Nutzer selbst erstellt hat. Diese Funktion wird durch die Nutzer dazu genutzt, Orte anzulegen, um so Veranstaltungen an konkreten Orten zu erstellen, aber auch, wenn ein Nutzer seinen Standort mitteilen möchte und dieser bei Facebook nicht hinterlegt ist.

Abschließend lässt sich festhalten, dass Facebook alle Daten nach gruppiert ablegt, es aber durchaus Verknüpfungen und Inhalte untereinander gibt, welche sich nicht direkt aus dem Zusammenhang ableiten lassen.

3.3.2 Nutzen der erhaltenen Daten

Nach der vorgenommenen Sichtung der Daten stellt sich nun die Frage, inwieweit sich diese erhaltenen Daten nutzen lassen. Können diese Daten es vereinfachen, mehr über einen Nutzer zu erfahren und können Sie sogar zur Aufklärung von Straftaten oder Ordnungswidrigkeiten genutzt werden? Dieser Frage soll im Folgendem beantwortet werden.

Die Struktur und Übersicht, in der die Dateien geliefert werden, machen es möglich, dass man schon nach einer kurzen Einarbeitungsphase damit vertraut ist, welche Daten in welchem Ordner liegen. Ebenfalls hilfreich ist die implementierte Navigation über den Browser selbst. Man muss nicht jedes Dokument einzeln händisch aus dem Ordner herausaufrufen, sondern kann durch die einzelnen Daten der HTML-Dokumente in einer Browser-Session durchnavigieren. Eine schnellere und übersichtlichere Navigation wird hierdurch geboten, allerdings lassen sich manche Inhalte nur aus der Ordner-Struktur heraus erkennen, was im Browser verborgen bleibt. Dazu gehören insbesondere gepostete Bilder, welche nicht auf dem eigenen Profil gepostet wurden sowie die eindeutige Nummer im Ordnernamen der Nachrichtenkonversationen.

Die bereitgestellten Daten werden gruppiert dargestellt, entsprechend der Kategorie, in welcher die Daten gespeichert werden. Dies hat den Vorteil, dass wenn man gezielt nach einer bestimmten Information sucht, diese sofort bekommt, vorausgesetzt eine der Kategorien ist von Facebook so eingesetzt worden. Für den normalen Informationsgebrauch für den einzelnen Nutzer ist dies ausreichend, bei tiefer gehenden Analysen bezüglich des Nutzers erschwert dies die Arbeit etwas.

Querverweise zwischen den einzelnen Daten sind ebenfalls nur sehr schwer einsehbar und oft mühsam zu erstellen. Durch die Kategorisierung und Aufteilung der einzelnen Informationen werden die Daten geteilt, und eventuell zusammenhängende Ereignisse sind schwerer nachzuvollziehen. Anhand des Beispieldatensatzes wird einmal ein konkretes Beispiel gegeben:

„Der Beispielnutzer hat sein Profilbild geändert. Zu diesem Ereignis sollen nun alle zu Verfügung stehenden Informationen gesammelt werden.“

Beginnend würde man über den Ordner „photos_and_videos“ auf den Ordner „Profilbilder“ zugreifen, in welchem sich nur das reine Profilbild als JPG-Datei befindet. Versteckt im Ordner „album“ findet sich die „0.html“ Datei, welche für die einzelnen Foto-Alben angelegt wird. Diese Datei geöffnet gibt einige Meta-Informationen bezüglich des Fotos wie Format, Breite, Höhe, ISO-Empfindlichkeit sowie die IP-Adresse, von welcher diese hochgeladen wurde. Ebenso das Datum an welchem die Datei hochgeladen wurde, inklusive örtlicher Zeitangabe, dem 15.November 2017 um 21:21. Diese Information findet sich ebenfalls im Ordner „profile_information“ und der „profile_update_history.html“, zusammen mit den Kommentaren des Bildes.

In dem „security_and_login_information“-Ordner in der „logins_and_logouts.html“-Datei finden sich am selben Tag Aufzeichnungen derselben IP-Adresse. Hierbei fehlt aber genau für die fragliche Zeit die Aufzeichnungen. Um 17:26 wurde für den Nutzer ein Logout verzeichnet, um 22:44 erst wieder ein Login. Er war also zum Zeitpunkt, an dem das Bild hochgeladen, zumindest den Aufzeichnungen nach, gar nicht auf der Plattform angemeldet. Aber die Anmeldungen, sowie die IP-Adresse sind alle im selben Zeitraum, woher sich leichte Unterschiede und Abweichungen erklären lassen. Die einzelnen Logins liegen auch noch einmal in der „account_activity.html“ Datei, allerdings hierbei noch zusätzlich hinterlegt der Browser, mit dem das Bild voraussichtlich hochgeladen wurde, sowie der anonymisierte Cookie. Die meisten Informationen lassen sich auch in der „where_you´re_logged_in.html“ Datei feststellen. Hieraus wird ersichtlich, dass der Nutzer vom 15.11.17 sich in der Facebook-App von einem Samsung Smartphone aus angemeldet hat, beziehungsweise der Eintrag für den Cookie sowie die IP erstellt worden ist. Dieser wurde um 22:47 an besagtem Tag aktualisiert, zur selben Zeit verzeichnet Facebook eine Abmeldung. In der Datei wird ebenfalls der Standort mitgeteilt, welcher für die IP ermittelt worden ist.

Zusammengefasst musst man für die Informationen bezüglich eines Ereignisses in vier HTML-Dateien suchen, um die folgenden Informationen zu erhalten: Zeit des Ereignisses, Ort, IP-Adresse, verwendete App, verwendetes Gerät, sowie bildtechnische Meta-Daten des Bildes. Dies zeigt deutlich, dass die bereitgestellten Daten teilweise sehr mühselig zusammenzusetzen sind, und eine gewisse Einarbeitungszeit benötigen, um die Informationen schnell und effektiv zu finden. Eine übersichtliche Aufbereitung bezüglich der einzelnen Ereignisse durch den Nutzer ist nicht vorhanden.

Eine zeitliche Aufbereitung gestaltet sich auch für die Nachrichtenverläufe als schwierig. Diese werden konversationsgebunden abgespeichert, ein Ordner entsprechend für eine Konversation. Sollte man nun nach den Nachrichten aus einem bestimmten Zeitintervall suchen, so erschwert dies die Suche erheblich. Die einfachste Lösung dieses Problems ist das Einloggen in den Facebook-Account, in welchem über die Nachrichten-Funktion direkt auf die letzten Nachrichten zugegriffen werden kann. Weiterhin kann dieses Problem mit einfachen Programmen und Algorithmen gelöst werden, beispielsweise besteht die Möglichkeit, ein Programm zu schreiben, welches durch alle Konversations-HTML-Dateien läuft und mithilfe eines Textparsers die gewünschten Informationen extrahieren kann. Am einfachsten lässt sich aber mithilfe der Suchfunktionen des Browsers nach den Zeitpunkten suchen, allerdings muss man dafür händisch in jeder Konversation nach den Zeitpunkten suchen.

Hinsichtlich der Nützlichkeit der Dateien lässt sich sagen, dass diese durchaus gegeben ist, je nachdem welche Informationen man hinsichtlich des Nutzers benötigt. Hierbei finden sich vor allem auch Informationen, welche durch den reinen Nutzen des Profils bei Facebook nicht direkt ersichtlich werden. Dazu zählen insbesondere die IP-Adressen sowie Reaktionen auf Werbeanzeigen und Werbeinteressen. Persönliche Gefällt-Mir-Angaben und die individuellen Werbeinteressen geben ein umfassendes Bild über den Nutzer ab, vorausgesetzt man bereitet diese hinreichend auf und interpretiert sie anschließend. Ebenso

Lebensumstände, wie beispielsweise die Peer-Group der Freunde des Nutzers, sind dem Nutzer oftmals nicht wirklich bewusst.

Der Anwendungsbereich, in dem diese Daten genutzt werden können, gestaltet sich daher als sehr weit. Hinsichtlich der Strafverfolgung ergeben sich neue und einfache Möglichkeiten, um gegen „Cybercrime“, also Straftaten oder Strafdelikte im digitalen Raum, vorzugehen. Die einzelnen gesammelten Informationen können ergänzend als Beweismaterial dienen, vorausgesetzt Facebook oder der Nutzer löscht diese nicht. Hierbei zählen überwiegend die technischen und faktischen Daten wie Zeitangaben, IP-Adressen oder Geräteangaben. Die persönlichen Informationen der Lebensumstände können aber auch durchaus von Nutzen sein, wie der Psychologe Dr. Michal Kosinski gezeigt hat.

Mithilfe von Facebook-Likes und einigen anderen Angaben ist es möglich, persönliche Angaben bezüglich einer Person zu treffen. Diese können Geschlecht, Alter, Sexualität sowie rassische Herkunft umfassen. Aber auch persönliche Eigenschaften wie Offenheit, emotionale Stabilität oder Intelligenz können teilweise vorhergesagt werden. Da diese Methode auf Ansätzen beruht, welche einen ausreichenden Testsatz an weiteren Informationen voraussetzt, lässt sich nicht jeder anhand seiner Facebook-Likes zu beschreiben. Allerdings können diese Informationen durchaus für psychologische Untersuchungen, Gutachten oder Profiling als weitere Informationsquellen dienen, um den Nutzer hinter dem Profil zu charakterisieren. (12)

Ein entscheidender Nachteil, welche nicht unerheblich zur Verwendung dieser Informationen ist, ist die Beschaffung dieser Informationen. Die Daten können nur von dem betreffenden Nutzer selbst angefordert werden. Selbst wenn die Daten von einem Dritten angefordert werden sollten, so müsste dieser Dritte zumindest über die E-Mail und das Passwort des Nutzers verfügen. Ebenso steht das Online-Angebot dieser Informationen zur Verfügung, das heißt man kann alle Daten, welche man herunterladen kann, ebenso gut online einsehen. Klarer Vorteil hier ist, dass der Zugriff erheblich einfacher und schneller geht, obwohl das Herunterladen ebenfalls nur wenige Minuten dauert. Problematisch dürften hier dann die forensische Sicherung und Nachweisbarkeit der Informationen, da diese dann nur flüchtig im Browser gespeichert werden. Mithilfe von Programmen zur Bildschirmaufnahme lassen sich hier trotzdem Sicherungen anfertigen, wobei die Option der heruntergeladenen Informationen deutlich besser ist. Die heruntergeladenen Dateien lassen sich mithilfe eines Hash-Verfahrens verifizieren, sodass eine nachträgliche Änderung und Fälschung direkt ausgeschlossen werden kann. Zu beachten ist hier auch der Übertragungsweg, da die Daten direkt über den Facebook-Browser heruntergeladen werden und so durchaus abgefangen werden können. Die erhaltene ZIP-Datei ist ebenfalls nicht verschlüsselt, sodass ein nachträglicher Verlust und eine damit eingehende Veränderung der Daten nicht auszuschließen sind.

3.3.3 Beurteilung der erhaltenen Daten

Bei der Informationsbeschaffung durch die neugeschaffenen Informationspflichten am praktischen Beispiel des Sozialen Netzwerks Facebook zeigt sich recht gut, welche neuen Methoden und Möglichkeiten der Informationsgewinnung nun bestehen.

Der Nutzer hat nun die Möglichkeit, bewusst seine Daten einzusehen, was zu deutlich mehr Transparenz führt. Zwar wird dies alles in den Allgemeinen Geschäftsbedingungen sowie den Datenschutzerklärungen und -bestimmungen geregelt, doch eine Studie des Deutschen Instituts für Vertrauen und Sicherheit im Internet zeigt, dass die meisten Internetnutzer AGBS und Datenschutzbestimmungen gar nicht lesen (23,25%), beziehungsweise nur grob überfliegen (45, 43%). Auch zeigt die Umfrage, dass über 80 Prozent der Nutzer eher glauben, dass man nicht überprüfen kann ob die AGB eingehalten werden. Dies zeigt ein sehr deutliches Misstrauen gegenüber solchen Bestimmungen. Auch empfinden, nach Ergebnissen der Umfrage, viele Nutzer das Zustimmen zu den AGB´s als lästig, und wollen sich nicht damit beschäftigen (>60 Prozent). (13)

Durch die neugeschaffenen Gesetze ist es nun für den Betroffenen möglich, schnell, einfach und effizient an seine Daten zu kommen, ohne sich mühsam durch die einzelnen Datenschutzbestimmungen und Geschäftsbedingungen lesen zu müssen. Er sollte, im Idealfall, eine einfache und übersichtliche Sammlung seiner Informationen erhalten können. Anschließend kann der Betroffene dann beurteilen, wie er mit diesen Daten umgehen möchte, beispielsweise ob er den Dienst weiter nutzen möchte oder ob er freiwillig preisgegebene Daten löschen möchte.

Facebook stellt für diesen Prozess eine sehr gute Lösung bereit. Mithilfe der Online-Möglichkeit kann der Nutzer seine Daten einsehen, ohne auf deren Bereitstellung zu warten oder sie abspeichern zu müssen. Verbraucherfreundlich ist dies ebenso, da die einzelnen Datensätze direkt bearbeitet werden können. Jede Angabe kann direkt gelöscht oder geändert werden. Die Alternative, das Herunterladen der Daten, bezieht sich hauptsächlich auf das Recht auf Datenportabilität (Art 20 EU-DSGVO), und ermöglicht es dem Nutzer, seine Daten in einem anderen sozialen Netzwerk weiterzuverwenden. Entsprechend wird hierbei auch das JSONS-Format angeboten, welches neben dem CSV und dem XML-Format als maschinenlesbares Format gilt. (14)

Allerdings besitzt diese Art der Informationsbeschaffung einige Probleme. Das bereits in Kapitel 3.3.2 genannte Problem des Zugriffs auf die Informationen und Daten ist hier das größte Problem. Ohne die Hilfe und Unterstützung des Nutzers können so Strafverfolgungsbehörden oder Staatsgewalten nur sehr erschwert Zugang zu diesen Daten haben. Allerdings können sie bei Facebook anfragen und die Herausgabe der Daten fordern, allerdings sind dann die entsprechenden Rechtsrahmen aus der Strafprozessordnung (STPO) sowie dem zuständigen Datenschutz-Gesetz zu prüfen. Einige Daten dürfen Ermittler nur auf Weisung eines Richters oder Staatsanwaltes unter Vorlage eines schriftlichen Beschlusses erhalten, während im Datenschutz immer ein konkreter Zweck hinter der Verarbeitung und

Weitergabe von Daten stehen muss. Durch den Prozess zur Umsetzung des Rechts auf Auskunft hat Facebook eine Methode geschaffen, mit der solche Auskunftsersuchen der Strafverfolgungsbehörden schnell und effizient beantwortet werden können, allerdings nur wenn die entsprechenden Rechtsbestimmungen eingehalten werden (29).

Prinzipiell kann eine Strafverfolgungsbehörde nur die Herausgabe von Daten fordern, sobald ein Richter die Genehmigung dazu schriftlich erteilt hat. Lägen die Daten auf einem Rechner in Deutschland, so könnte der Datensatz einfach beschlagnahmt werden, im Falle von Facebook liegen diese Daten aber nicht in Deutschland, sondern Facebook Ireland ist für die Daten zuständig. So muss dann ein ausländischer Staatsanwalt die Beschlagnahmung anordnen, was durchaus sechs Monate und länger dauern kann. (29)

Facebook selbst behält sich vor, die Daten an Dritte weiterzugeben, sowohl innerhalb ihres eigenen Unternehmens wie auch an Dritte, einschließlich Aufsichts- Strafverfolgungs- bzw. Vollstreckungsbehörden. Dies kann sowohl auf rechtliche Anfragen wie auch in eigenem gutem Glauben. Darunter fallen insbesondere Abwendung von Betrug, unrechtmäßiger Nutzung, Verstößen, sowie um Nutzer oder andere zu schützen. (29)

Das zweite Problem ist die Art, in welcher die Daten präsentiert werden. Ermittlungen oder Untersuchungen von Straftaten und Ordnungswidrigkeiten sind an ein konkretes Ereignis gebunden. Um diese Ereignisse aufzubereiten erfordert es aber Einarbeitung, da sich die erhaltenen Daten nicht nach Ereignissen gruppieren lassen beziehungsweise sie nicht danach gruppiert sind. Wie eine solche Untersuchung aussehen kann wurde in Kapitel 3.3.2 am Beispiel eines hochgeladenen Bildes beschrieben.

Alles in allem lässt sich festhalten, dass dieses Beispiel sehr gut zeigt, welche Möglichkeiten durch die neu geschaffenen Gesetze des Datenschutzes im Bereich von forensischer Arbeit eröffnet wurden. Alle Unternehmen, welche personenbezogene Daten verarbeiten sollten einen Prozess implementiert haben, welcher ermöglichen soll, dass das Recht auf Auskunft und Herausgabe der Daten möglichst schnell und vollständig ermöglicht wird. Besonders im Bereich der Strafverfolgung ist es oftmals wichtig, möglichst schnell an Informationen zu gelangen. Facebook hat mit seiner Umsetzung einen Prozess geschaffen, welcher dies sehr gut umsetzt. Innerhalb kürzester Zeit erhält man eine Vielzahl an personenbezogenen Daten, welche dann für Strafverfolgungszwecke genutzt werden können. Die Übersicht leidet darunter allerdings etwas, da besonders ereignisbezogene Daten schwerer zu ermitteln sind, beziehungsweise ein gewisser Aufwand besteht die einzelnen Daten zu vereinen. Die Nutzbarkeit ist auch zu beachten, da viele Daten auch gelöscht werden können, sodass Facebook diese ebenfalls löschen muss, sowie die Art der personenbezogenen Daten, da es sich hauptsächlich um die vom Nutzer selbst freigegebenen Daten handelt. Auch der Zugriff auf die Daten kann nur mit Unterstützung des Nutzers erfolgen, da hierfür die Login-Daten des Nutzers gefordert werden. Erhält man diese Daten allerdings auf Grundlage eines Beschlusses oder einer richterlichen Anordnung so kann man dieses Problem umgehen, vorausgesetzt Facebook gibt genau diese Daten weiter, was sich allerdings aus praktischer Sicht anbieten würde.

Das Beispiel sollte verdeutlichen, welche Schnittstellen zwischen Datenschutz, Datenschutzgesetzen und praktischer forensischer Arbeit existieren und wie diese zu bewerten sind. Sie sind nicht immer deckungsgleich, besonders in der Frage nach der Anwenderfreundlichkeit und dem Umfang der Daten, besitzen aber vermehrt doch mehr Gemeinsamkeiten. Auch wenn der Schutz von personenbezogenen Daten innerhalb der Datenschutzgesetze stets im Vordergrund steht, so gibt es doch Möglichkeiten auf Einschränkung und Eingriff in diesen Schutz. Ähnlich gestaltet sich dies in der forensischen Arbeit, in welcher ebenfalls stets auf Grundlage von Gesetzen in die Grundrechte und Freiheiten eingegriffen werden kann. Hierbei ist aber anzumerken, dass die Datenschutzgesetze selbst die Möglichkeiten zum Eingriff in die Rechte bieten, während, besonders im Bereich der Strafverfolgung, zusätzliche Gesetze geschaffen werden müssen.

4 Forensische Methoden und Tools zur Arbeit im Datenschutz

Die neuen Datenschutzgesetze fordern von den Verantwortlichen für die Datenverarbeitungen den nachweislichen Umsatz der Datenschutzbestimmungen. Dies wird als Rechenschaftspflicht bezeichnet. Gefordert ist dieses beispielsweise in Art. 5 Abs. 2 EU-DSGVO:

„Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftsplficht).“ (Art. 5 Abs. 2 EU-DSGVO)

Folglich muss nun dem Verantwortlichen nicht mehr bewiesen werden, dass er sich nicht datenschutzkonform verhält, sondern der Verantwortliche muss im Vorhinein beweisen, dass er die Datenschutzbestimmungen einhält und ausführt. Für den Schadensfall bezeichnet man dies als Beweislastumkehr. Übertragen auf ein Beispiel aus der Strafverfolgung bedeutet dies, dass einem Tatverdächtigen nicht mehr die Beteiligung an einer Tat durch die Strafverfolgungsbehörde bewiesen werden muss um als schuldig zu gelten, sondern der Tatverdächtige muss selbst beweisen können, dass er nicht an der Tat beteiligt war, andernfalls gilt er als schuldig. Die geforderte Rechenschaftspflicht zeigt sich als äußerst schwer umzusetzen, besonders da unterschiedliche Auffassungen existieren, wie sie umgesetzt werden sollte. Auch stellte sie sich als recht theoretisch heraus, was die Arbeit im praktischen unberührt lässt. Im Folgenden soll dieser theoretische Ansatz in die Praxis umgewandelt werden. Im Konkreten: welche praktischen Methoden, Hilfswerkzeuge oder Programme können eingesetzt werden, um eine nicht erfüllte Rechenschaftspflicht nachweisbar zu machen oder um die geforderte Rechenschaftspflicht erfüllen zu können. Der Fokus liegt hierbei auf den digitalen Möglichkeiten, betrachtet werden Umsetzung, Nutzen sowie Fehler innerhalb der Programme. Ebenso als Faktor werden der Nutzen für Unternehmen und deren Wirtschaftlichkeit stets beachtet.

4.1 Tools und Methoden zum Nachweis von Datenschutzverletzungen

Insbesondere für Datenschutzbehörden ist der Nachweis von Datenschutzverletzungen von immenser Bedeutung. Sie sind die Instanz, innerhalb von Deutschland, welche bei Unternehmen oder Vereinen nachweist, dass der entsprechende Verantwortliche nicht seiner Rechenschaftspflicht nachgekommen ist oder er sich nicht an die vorgeschriebenen Gesetze und Regelungen gehalten hat.

Wie bereits in den vorhergehenden Kapiteln thematisiert ist die forensische Arbeit natürlich von der Rechenschaftspflicht des Verantwortlichen abhängig. Ist sein System gut dokumentiert und einwandfrei nachzuhalten, so erleichtert es die forensische Arbeit, da sich so direkte Hinweise finden lassen, wo etwas nicht ausreichend dokumentiert oder umgesetzt wird. Ist die Rechenschaftspflicht nicht hinreichend ausgeführt, so wird die Arbeit erschwert, da diese Hinweise selbst gesucht werden müssen.

Aber auch bei einem vollständig dokumentierten System können Datenschutzverletzungen auftreten, da die Systeme oftmals einen „Soll-Zustand“ beschreiben, also wie das System zum Datenschutz funktionieren soll. Der tatsächliche „Ist-Zustand“, die konkrete praktische Anwendung innerhalb der Organisation oder des Verantwortlichen, weicht nicht selten stark davon ab. Faktoren dafür sind mannigfaltig, der größte Faktor ist hierbei der Mensch. Dieser kann durch Unachtsamkeit, mutwilligem Handeln oder nicht ausreichender Schulung und Kompetenz die aufgestellten Regelungen und Anweisungen missachten und so die gesamte Prozesskette zum datenschutzkonformen Arbeiten zunichtemachen. Nicht zuletzt fallen viele notwendigen Maßnahmen auch der Wirtschaftlichkeit der Organisation zum Opfer. Sollten bestimmte geforderte Regelungen sich negativ auf diese auswirken, so werden diese oftmals im Rahmen einer Risikoanalyse als Risiko getragen und akzeptiert. Insbesondere in kleineren Unternehmen ist dies nicht unüblich. Ein konkretes Beispiel wäre die Nutzung von Messenger Diensten, welche die Daten oftmals in Drittländer übertragen, was laut Art. 44 EU-DSGVO nur zulässig ist, solange der Empfänger sich an bestimmte Anforderungen hält, was in der Praxis selten umgesetzt wird.

Als praktisches Beispiel soll einmal der Fall herhalten, dass per Mail von einer Unternehmensadresse Kundendaten versendet worden sind, missbraucht worden sind und durch die Behörde ein Bußgeld ausgesprochen wurde. Hat das Unternehmen diese Art der Weitergabe nicht untersagt, so haftet es selbst und muss das Bußgeld selbst zahlen und auch den daraus resultierenden Image-Schaden tragen. Hat allerdings ein Mitarbeiter entgegen internen Richtlinien diese Daten versendet, so kann dieser mit in die Haftung einbezogen werden und auch arbeitsrechtliche Schritte nach sich ziehen. Um dies allerdings lückenlos nachweisen zu können kann ein forensisches Gutachten erstellt werden, in wessen Folge der unternehmenseigene Mailserver gesichert und analysiert wird. Im Zuge der Sicherung muss der Server aus dem Unternehmensnetz entfernt werden, was einen negativen Effekt auf die Wirtschaftlichkeit des Unternehmens hat, denn dieses ist für diese Zeit unter Umständen nicht arbeitsfähig. Daher sind Unternehmen, insbesondere bei solchen internen Untersuchungen daran interessiert, den Vorfall aufzuklären, aber auch die Wirtschaftlichkeit ihres Unternehmens nicht zu gefährden, zumal interne Untersuchungen nicht veröffentlicht werden, anders als von Behörden veranlasste Untersuchungen, welche veröffentlicht werden können.

Es zeigt sich also, dass nicht nur die Datenschutzaufsichtsbehörden ein Interesse daran haben, wie Datenschutzverletzungen nachzuweisen sind, sondern auch Verantwortliche im Sinne des Art. 4 Abs. 7 EU-DSGVO haben durchaus Interesse an diesen Nachweismöglichkeiten, da sie so überprüfen können, ob die Datenschutztechnischen Belange und

Regelungen innerhalb der Organisation auch umgesetzt werden, also ob ihr „Soll-Zustand“ ihrem „Ist-Zustand“ entspricht oder woher die Fehler in ihrem Datenschutz-Managementsystem stammen.

4.1.1 Private Internetnutzung

Um den vollen Umfang eines umfassenden Datenschutzkonzepts aufzubauen, gilt es auch, die Sicherheitsvorkehrungen innerhalb der Organisation zu gewährleisten. Ein großer Faktor spielt hierbei die Internetnutzung und das private Surfverhalten der Mitarbeiter am Arbeitsplatz, da die größte Gefahrenquelle für Computersicherheit weiterhin das Herunterladen von Schadsoftware darstellt. (15)

Daher ist es ratsam, die Anweisungen bezüglich des Datenschutzes auch auf diese Bereiche auszuweiten. Die einfachste Möglichkeit ist es, den Mitarbeitern die private Internetnutzung zu verbieten, allerdings lässt sich dies schwer überprüfen, da die Grenzen zwischen privatem Gebrauch und dienstlichem Gebrauch verschwimmen können. Im Verlauf lässt sich schwer zurückverfolgen, ob ein beispielsweise im Online-Shop bestelltes Buch für private oder dienstliche Zwecke benötigt wird.

Viele Unternehmen gestatten die private Internetnutzung im Rahmen der Pausenzeiten, aber auch hier können durchaus Sicherheitsrisiken zustanden kommen, beispielsweise durch das Öffnen einer infizierten Datei oder schadhaften Internetseite.

Um nachzuweisen oder zu überprüfen, ob ein Nutzer den Rechner privat benutzt oder eine schadhafte Seite besucht hat kommen Programme zum Einsatz, welche den Browserverlauf der einzelnen Internetbrowser aufzeigen können.

Eines dieser Programme ist der Browser history spy der Firma SecurityXploded. Erstmals 2012 veröffentlicht soll das Programm eine Übersicht über die Browserverläufe der einzelnen und verschiedenen Browser geben (16). Unter den zehn unterstützten Browser finden sich auch die am häufigsten verwendeten Chrome, Firefox und Internet Explorer. Das Programm bietet eine Graphisches User-Interface, welches einfachen Zugriff auf die entsprechenden Dateien der einzelnen Browser ermöglicht. Die Standard-Pfade der einzelnen Browser sind dabei direkt hinterlegt, eine manuelle Auswahl steht bei Firefox und Chrome ebenfalls zur Verfügung. So lassen sich auch Verläufe aus Datensicherungen in das Programm einspeisen und analysieren, in erster Linie dient es allerdings der Live-Analyse eines Systems im Betriebszustand.

Pro Eintrag zeichnet das System auf, welche URL besucht wurde, welchen Website Title die Seite hatte und wann der Zugriff erfolgte. Zusätzlich hinzu kommen dann spezifische Merkmale der einzelnen Browser. Während bei Firefox und Chrome zusätzlich noch die Anzahl der Besuche aufgezeichnet werden, enthält der Internet Explorer noch Angaben über den Login-Username sowie die Versionsnummer des Browsers. Die entsprechenden Einträge lassen sich auch direkt über das Programm löschen, sowie in HTML-, CSV- oder

XML-Dateien exportieren. Für den Internetexplorer gibt es sogar die Funktion, selbstständig Einträge hinzuzufügen.

Problematisch für das Tool ist allerdings die Einstellungen des jeweiligen Browsers. Dort kann man entsprechend festlegen, ob ein Verlauf angelegt werden soll oder nicht. Ist diese Funktion deaktiviert, so erscheint der entsprechende Eintrag auch nicht im Browser History Spy. Die Ergebnisse können also durchaus manipuliert werden, beispielsweise durch die Nutzung der „Incognito-Modi“ der Browser, in denen bewusst kein Verlauf angelegt wird. Aber um auch diese Anfragen aufzuzeichnen, kann der gesamte Netzwerkverkehr aufgezeichnet werden. Problematisch hierbei sind die aufgezeichneten Daten, da diese eine immense Größe haben, sowie das Herausfiltern der relevanten Einträge. Ebenso ist hier die Rechtslage zu beachten, denn das Aufzeichnen aller Netzwerksverkehrsdaten kann als unberechtigte Aufzeichnung gelten.

Das Tool zeigt also recht übersichtlich, welche Seiten zu welchem Zeitpunkt besucht wurden und zu welchem Zeitpunkt dies geschah. Eine private Internetnutzung lässt sich so schnell ermitteln und nachweisen, vorausgesetzt die Browser haben die nötigen Einstellungen zuvor erhalten. Mithilfe von Dienstanweisungen oder beschränkten Zugriffsrechten ist dies aber durchaus implementierbar und daher ist das Tool für interne Überprüfungen nützlicher als für forensische Analysen, wobei es auch für diese genutzt werden kann.

Alternativen für die Einsicht von Browserverläufen sind Browsing HistoryView von Nirsoft (25) sowie der History Viewer von Digital Forensics Studio (26).

4.1.2 Portscanner

Neben der Schaffung von neuen Risiken und Gefahrenpotenzialen geht es im Datenschutz auch um den Schutz vor unberechtigten Zugriff oder eine unberechtigte Weitergabe. Doch welche Daten wohin gehen ist für viele Endverbraucher nicht zu sehen, da die Anwendungsprogramme im OSI-Schichtenmodell in Layer sieben laufen, während die Datenübermittlung in Layer vier und drei stattfindet (36). Um sicherzustellen, wohin welche Daten übertragen werden können sogenannte Portscanner zum Einsatz kommen, welche Informationen über die verwendeten Ports geben.

Ports sind Teile der Netzwerkadresse, welche die Zuweisung der erhaltenen Pakete im Transmission Control Protocol (TCP) und dem User Datagram Protocol (UDP) zu einem bestimmten Programm oder einer Anwendung möglich machen. Dies dient dem Betriebssystem zur Zuweisung des Netzwerktraffics zu einem Programm. (17)

Da die Programme über diese Ports ihre Daten beziehen sind sie insbesondere für Cyberangriffe nützlich. Ein Angreifer kann über sie Schadsoftware einspielen und so das Zielsystem infizieren, teilweise sogar übernehmen. Um zu kontrollieren, dass die Ports stets geschlossen sind sowie keine falschen Ports verwendet werden, kommen die Portscanner zum Einsatz.

Ein Beispiel für einen Portscanner ist CurrPorts der Firma Nirsoft, welche eine der größten Anbieter für Open-Source Tools sind. CurrPorts erlaubt es, alle Ports eines laufenden Systems aufzuzeichnen und eine Vielzahl der Informationen zu geben. (18)

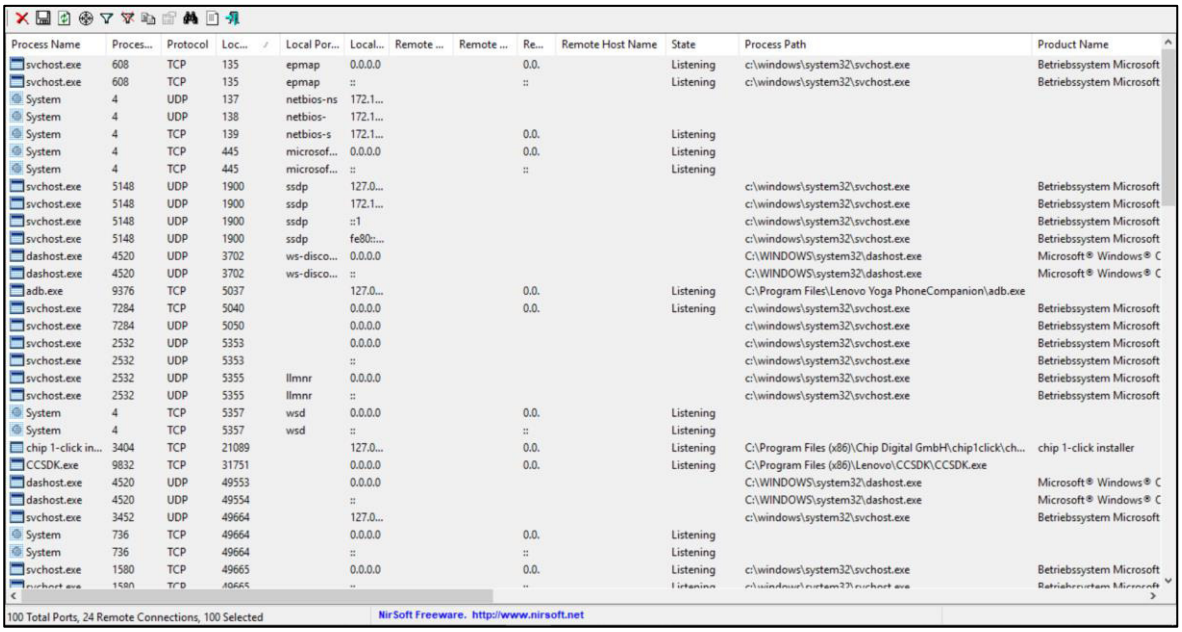


Abbildung 6: CurrPorts Programm

Darunter zählen insbesondere die verwendeten Ports, die Local und Remote Adressen sowie die Prozesse, welche gerade die Ports benutzen. Sollte ein Programm nun Ports nutzen, welche nicht zum Zweck des Programms genutzt werden sollen, so könnte man dies dieser Übersicht entnehmen.

Die verschiedensten Portscanner auf dem Markt wie beispielsweise NMAP oder ZMap arbeiten ähnlich wie CurrPorts. Die Variation geht häufig nur darüber hinaus, welche weiteren Funktionen implementiert sind, wie beispielsweise das Schließen der entsprechenden Prozesse oder eine Exportfunktion.

Auch diese Programme sind für den laufenden Betrieb der zu untersuchenden Systeme vorgesehen und eignen sich daher eher für interne Untersuchungen und systemadministrative Zwecke als für forensische Analysen, da das System durch das Ausführen dieser Programme verändert wird. Es hilft aber um festzustellen, ob die in der Organisation verwendeten Programme keine Sicherheitslücken lassen, durch die eine Datenschutzverletzung zu Stande kommen kann oder bereits existiert.

4.1.3 Windows spezifische Tools

Windows ist deutschlandweit das am häufigsten verwendete Betriebssystem. Während Entwickler Microsoft fortan Version Windows 10 nur noch weiter entwickeln möchte, sind auch weiterhin die veralteten Versionen von Windows wie beispielsweise Vista oder Windows 7 im Umlauf, weswegen der Abstand zum zweitplatzierten MacOS über 60 Prozent beträgt. (35)

Daher ist es durchaus interessant, die einzelnen Funktionsweisen von Windows für den Nachweis von Datenschutzverletzungen auszunutzen, und spezifische Programme zu betrachten, welche nur auf Windows Betriebssystemen funktionieren.

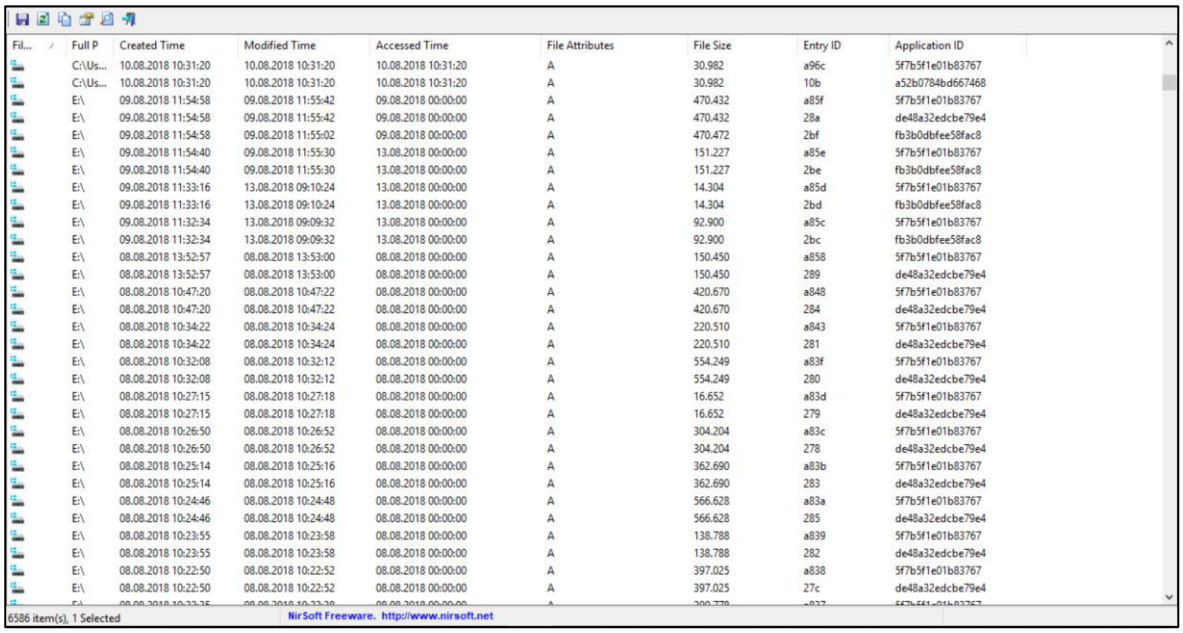
Zur praktischen Anwendung der folgenden Programme wird das forensische Tool-Kit DART (Digital Advanced Response Toolkit) verwendet. Dieses Open-Source Tool-Kit ist für die forensische Linux-Distribution DEFT (Digital Envidence & Forensic Toolkit) entwickelt worden und als Windows-Live-Umgebung implementiert (19). Sie simuliert also mithilfe des Emulators WINE (Wine is not an Emulator) ein Windows-Programm, aus dem sich die verschiedensten einzelnen Programme starten lassen (20).

Vorteil von DART ist die Anwendbarkeit auf nicht Windows-Systemen, aber auch die Übersichtlichkeit und der Umfang der Programme. Auch bietet es einen eigenen Pool für reine Windows-Programme, welche im Folgenden nun näher betrachtet werden sollen.

Eines der Tools ist das JumpListsView Programm von NirSoft. Dieses bietet die Möglichkeit, die in Windows angelegten Jump-Lists einzusehen und so nachvollziehen zu können, welche Dateien vom Nutzer angesehen oder geöffnet wurden. (21)

Die Windows JumpLists wurde mit der Version Windows 7 eingefügt und sollen dem Nutzer Links zu kürzlich verwendeten Dateien bereitstellen. Diese werden dann lokal abgelegt und können dann analysiert werden. (22)

JumpListsView greift auf die lokal abgelegten Programme zu und stellt sie übersichtlich dar.



Fil...	Full P	Created Time	Modified Time	Accessed Time	File Attributes	File Size	Entry ID	Application ID
	C:\Us...	10.08.2018 10:31:20	10.08.2018 10:31:20	10.08.2018 10:31:20	A	30.982	a96c	5f7b5f1e01b83767
	C:\Us...	10.08.2018 10:31:20	10.08.2018 10:31:20	10.08.2018 10:31:20	A	30.982	10b	a52b0784bd667468
	E:\	09.08.2018 11:54:58	09.08.2018 11:55:42	09.08.2018 00:00:00	A	470.432	a85f	5f7b5f1e01b83767
	E:\	09.08.2018 11:54:58	09.08.2018 11:55:42	09.08.2018 00:00:00	A	470.432	28a	de48a32edcbe79e4
	E:\	09.08.2018 11:54:58	09.08.2018 11:55:02	09.08.2018 00:00:00	A	470.472	2bf	fb3b0dbfee58fac8
	E:\	09.08.2018 11:54:40	09.08.2018 11:55:30	13.08.2018 00:00:00	A	151.227	a85e	5f7b5f1e01b83767
	E:\	09.08.2018 11:54:40	09.08.2018 11:55:30	13.08.2018 00:00:00	A	151.227	2be	fb3b0dbfee58fac8
	E:\	09.08.2018 11:33:16	13.08.2018 09:10:24	13.08.2018 00:00:00	A	14.304	a85d	5f7b5f1e01b83767
	E:\	09.08.2018 11:33:16	13.08.2018 09:10:24	13.08.2018 00:00:00	A	14.304	2bd	fb3b0dbfee58fac8
	E:\	09.08.2018 11:32:34	13.08.2018 09:09:32	13.08.2018 00:00:00	A	92.900	a85c	5f7b5f1e01b83767
	E:\	09.08.2018 11:32:34	13.08.2018 09:09:32	13.08.2018 00:00:00	A	92.900	2bc	fb3b0dbfee58fac8
	E:\	08.08.2018 13:52:57	08.08.2018 13:53:00	08.08.2018 00:00:00	A	150.450	a858	5f7b5f1e01b83767
	E:\	08.08.2018 13:52:57	08.08.2018 13:53:00	08.08.2018 00:00:00	A	150.450	289	de48a32edcbe79e4
	E:\	08.08.2018 10:47:20	08.08.2018 10:47:22	08.08.2018 00:00:00	A	420.670	a848	5f7b5f1e01b83767
	E:\	08.08.2018 10:47:20	08.08.2018 10:47:22	08.08.2018 00:00:00	A	420.670	284	de48a32edcbe79e4
	E:\	08.08.2018 10:34:22	08.08.2018 10:34:24	08.08.2018 00:00:00	A	220.510	a843	5f7b5f1e01b83767
	E:\	08.08.2018 10:34:22	08.08.2018 10:34:24	08.08.2018 00:00:00	A	220.510	281	de48a32edcbe79e4
	E:\	08.08.2018 10:32:08	08.08.2018 10:32:12	08.08.2018 00:00:00	A	554.249	a83f	5f7b5f1e01b83767
	E:\	08.08.2018 10:32:08	08.08.2018 10:32:12	08.08.2018 00:00:00	A	554.249	280	de48a32edcbe79e4
	E:\	08.08.2018 10:27:15	08.08.2018 10:27:18	08.08.2018 00:00:00	A	16.652	a83d	5f7b5f1e01b83767
	E:\	08.08.2018 10:27:15	08.08.2018 10:27:18	08.08.2018 00:00:00	A	16.652	279	de48a32edcbe79e4
	E:\	08.08.2018 10:26:50	08.08.2018 10:26:52	08.08.2018 00:00:00	A	304.204	a83c	5f7b5f1e01b83767
	E:\	08.08.2018 10:26:50	08.08.2018 10:26:52	08.08.2018 00:00:00	A	304.204	278	de48a32edcbe79e4
	E:\	08.08.2018 10:25:14	08.08.2018 10:25:16	08.08.2018 00:00:00	A	362.690	a83b	5f7b5f1e01b83767
	E:\	08.08.2018 10:25:14	08.08.2018 10:25:16	08.08.2018 00:00:00	A	362.690	283	de48a32edcbe79e4
	E:\	08.08.2018 10:24:46	08.08.2018 10:24:48	08.08.2018 00:00:00	A	566.628	a83a	5f7b5f1e01b83767
	E:\	08.08.2018 10:24:46	08.08.2018 10:24:48	08.08.2018 00:00:00	A	566.628	285	de48a32edcbe79e4
	E:\	08.08.2018 10:23:55	08.08.2018 10:23:58	08.08.2018 00:00:00	A	138.788	a839	5f7b5f1e01b83767
	E:\	08.08.2018 10:23:55	08.08.2018 10:23:58	08.08.2018 00:00:00	A	138.788	282	de48a32edcbe79e4
	E:\	08.08.2018 10:22:50	08.08.2018 10:22:52	08.08.2018 00:00:00	A	397.025	a838	5f7b5f1e01b83767
	E:\	08.08.2018 10:22:50	08.08.2018 10:22:52	08.08.2018 00:00:00	A	397.025	27c	de48a32edcbe79e4

6586 item(s), 1 Selected NirSoft Freeware. http://www.nirsoft.net

Abbildung 7: JumpListsView

Es speichert zu jedem Eintrag, also einer bestimmten geöffneten Datei oder den Pfad der Datei, den Namen, die Erstellungszeit, die Zeit der Modifikation sowie die Zeit des Zugriffs, und die Größe der Datei in Bytes. Zusätzlich erhält jeder Eintrag eine ID ebenso wie die Anwendung, mit der auf die Datei zugegriffen worden ist.

Das Programm ist also auch auf eine Anwendung im laufenden Betrieb des Systems ausgelegt. Um die Jump-Lists von forensisch gesicherten Systemen auswerten zu können bieten sich Alternativen, beispielsweise erlaubt die forensische Analyse-Suite X-Ways eine Auswertung von Windows Jump-Lists von Datensicherungen. Nützlich ist dies für den Datenschutz und dem Nachweis von Datenschutzverletzungen in beiden Fällen, da sich so Zugriffe auf Dateien nachweisen lassen. Die Anforderungen an die Zugriffskontrolle sind explizit in § 64 Abs. 3 Satz 1 Nr. 7 BDSG n.F. geregelt:

„Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassenden personenbezogenen Daten Zugang haben“

Sollte also ein Nutzer Zugriff auf eine Datei haben, auf die er keinen Zugriff haben sollte so lässt sich dies mithilfe der Jump-Lists nachweisen. Um spezifischer zu erkennen, was ein Nutzer getan hat und ob er Dateien geändert hat, bietet sich ein weiteres Programm von NirSoft an, LastActivityView. Das Betriebssystem speichert an mehreren Orten diverse Informationen zu Aktivitäten des Nutzers, wie beispielsweise den Log-Dateien, den Prefatch-Dateien oder der eigenen Registry-Datenbank. Mithilfe von LastActivityView lassen sich eine Vielzahl dieser Ereignisse in einer Anzeige zusammenbringen. (23)

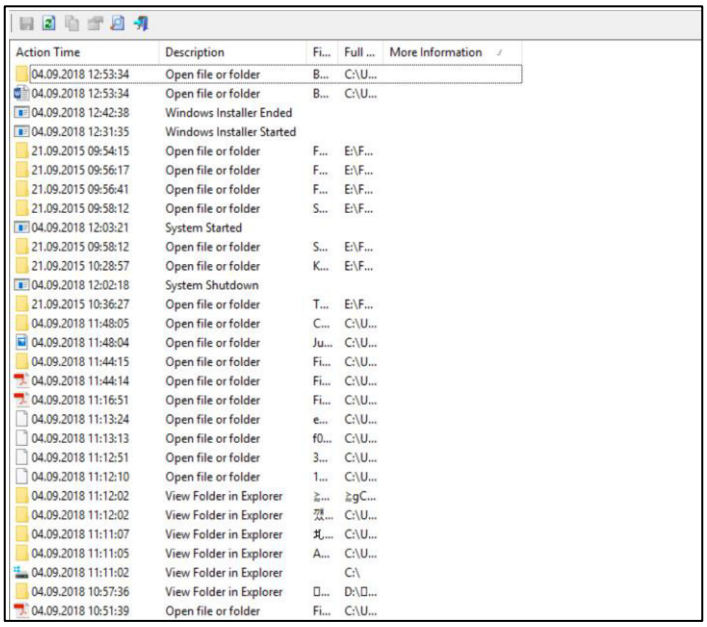


Abbildung 8: LastActivityView

Es stellt die Zeit des Ereignisses, die Art des Ereignisses, die Datei inklusive vollständigem Pfad dar sowie eine Spalte mit zusätzlichen Informationen, beispielsweise dem verwendeten Programm oder welche Nutzergruppe die Rechte für diese Aktion verliehen hat. Eine Übersicht der Ereignisarten findet sich entsprechend in der folgenden Tabelle.

Bezeichnung des Ereignisses	***Beschreibung des Ereignisses***
Run .EXE file:	: .EXE file run directly by the user, or by another software/service running in the background.
Select file in open/save dialog-box	The user selected the specified filename from the standard Save/Open dialog-box of Windows.
Open file or Folder	The user opened the specified filename from Windows Explorer or from another software.
View Folder in Explorer	The user viewed the specified folder in Windows Explorer.
Software Installation	The specified software has been installed or updated.
System Started	The computer has been started.
System Shutdown	The system has been shut down, directly by the user, or by a software that initiated a reboot.
Sleep	The computer has been placed into sleep mode.
Resumed from sleep	The computer has been resumed from sleep mode.
Network Connected	Network connected, after previously disconnected.
Network Disconnected	Network has been disconnected
Software Crash	The specified software has been crashed.
Software stopped responding	The specified software stopped responding.
Blue Screen	Blue screen event has been occurred on the system.
User Logon	The user logged on to the system.
User Logoff	The user logged off from the system. This even might caused by a software that initiated a reboot.
Restore Point Created	Restore point has been created by Windows operating system.

Bezeichnung des Ereignisses	***Beschreibung des Ereignisses***
Installer Ended	Windows Installer has ended his process
Windows Installer Started	Windows Installer has been started
Wireless Network Connected	Windows connected to a wireless network, the connection information is displayed in the 'More Information' column.
Wireless Network Disconnected	Windows disconnected from a wireless network, the connection information is displayed in the 'More Information' column.

Tabelle 3: Ereignisse in LastActivityView (23)

Durch diese Vielzahl an möglichen dokumentierten Ereignissen ist es möglich, die Aktivitäten eines Nutzers zurückzuverfolgen. Die Aktivitäten können dabei je nach Einstellung und Aktivität des Nutzers mehrere Jahre zurückgehen. Problematisch bei der Auswertung der Aktivitäten ist die Herkunft. Die Ereignisse sind zwar übersichtlich dargestellt, doch man kann den Ursprungsort nicht feststellen, der Eintrag könnte also aus allen möglichen Informationsquellen des Nutzers stammen. Zur forensischen Nachweisbarkeit eignet sich dieses Tool daher weniger, denn um den eindeutigen Beweis eines Ereignisses darlegen zu können muss die Originalquelle gefunden und ausgewertet werden. Zudem läuft das Programm nur in einer Live-Umgebung und beeinträchtigt so die Unveränderlichkeit des Systems. Für das Arbeiten auf Datensicherungen empfiehlt sich daher auf andere Programme zuzugreifen und die Auswertung der Registry oder der Ereignisanzeige beispielsweise mit der Forensik-Suite X-Ways durchzuführen. Für interne Untersuchungen bezüglich des Datenschutzes ist dieses Programm aber eher geeignet, da es direkt Aufschlüsse über mögliche Verletzungen oder Fehlverhalten geben kann.

Zusätzlich zu den Aktivitäten kann man noch weitere Programme heranziehen, welche die sogenannten Events aus den verschiedenen Log-Dateien des Windows-Betriebssystems betrachten. Ein Beispiel wäre MyEventViewer, ebenfalls von NirSoft, welches es ermöglicht, alle Events in einer übersichtlichen Anzeige zu erhalten. Es dient also als alternative zu der bereits von Windows implementierten Ereignisanzeige, fasst aber darüber hinaus noch weitere Events zusammen sowie erspart das mehrfache Suchen, da alle Ereignisse in einer Liste angezeigt werden. Bei der Windows Ereignisanzeige werden die Events nach ihrer Art sortiert und somit vorgefiltert. MyEventViewer gibt daher sofortigen Ausschluss, sollte man zu einem bestimmten Ereignis oder Datum etwas suchen. Alle relevanten Log-Einträge werden dann aufgelistet. (24)

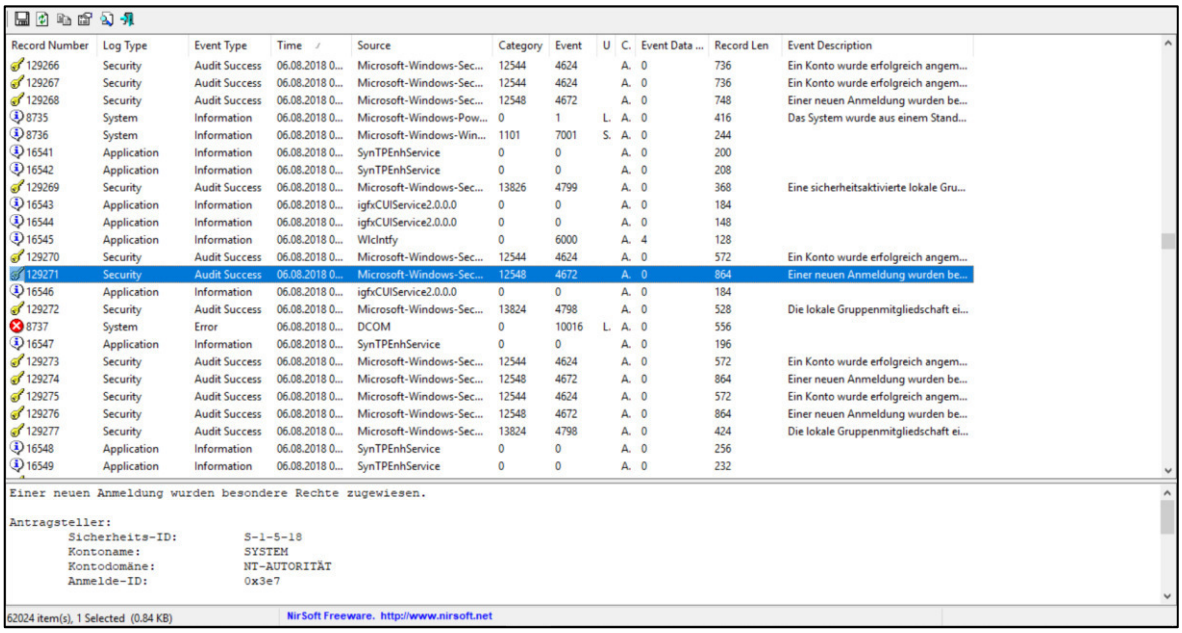


Abbildung 9: MyEventViewer

Wie in der Abbildung dargestellt erhält man schnell die nötigen Informationen bezüglich der Art des Eintrags, der Zeit, der Quelle, sowie den einzelnen Details zur Beschreibung des Events wie Länge des Eintrags, Kategorie oder User-Name. Auch hier zeigt sich wieder das Problem der forensischen Anwendbarkeit, denn das Programm ist als Live-Action Programm im laufenden Betrieb konzipiert, und verändert damit das entsprechende System. Für die interne Untersuchung sollte dieses Programm aber als Hilfsmittel durchaus interessant sein, da es die Arbeit erspart, die verschiedenen Log-Dateien einzeln zusammenzustellen und zu analysieren.

5 Fazit und Ausblick

Sind der Datenschutz und die digitale Forensik in praktischer Arbeit kombinierbar? Wo unterstützen sich die beiden Bereiche und wo stehen sie konträr gegenüber oder stellen Hindernisse für den anderen dar, aber auch wo entstehen Chancen durch diese Verknüpfung? Im letzten Kapitel sollen die Ergebnisse dieser Arbeit noch einmal dargestellt und aufgezeigt werden. Die Ergebnisse werden bewertet und sollen die anfangs gestellte Frage beantworten. Herangezogen werden persönliche Aspekte aus der praktischen Arbeit als Fachkraft für Datenschutz sowie die eben erörterten Ergebnisse dieser Arbeit.

5.1 Zusammenfassung

Die Einteilung dieser Arbeit teilte sich im Wesentlichen in zwei Teile: wie können durch den Datenschutz geschaffene Möglichkeiten die forensische Arbeit erleichtern und wie können durch die digitale Forensik geschaffene Möglichkeiten die Arbeit im Bereich des Datenschutzes erleichtern.

Zunächst sollte geprüft werden, welche Möglichkeiten der Datenschutz schafft. Durch die neu eingeführte Europäische Datenschutzgrundverordnung werden dem Betroffenen neue Rechte ermöglicht. Diese Rechte gelten für die gesamte Europäische Union sowie darüber hinaus, sobald der Verarbeiter nach dem Marktortprinzip sich ebenfalls an die Regelungen der EU-DSGVO zu halten hat. Der Betroffene hat nun die Möglichkeit seine Daten löschen oder einschränken zu lassen, aber auch seine Daten herausgeben zu lassen und sie in einem gängigen Format zu erhalten. Dadurch besteht die Möglichkeit, eine Anzahl an Daten zu erhalten, welche nicht unbedingt ersichtlich sind.

Diese Möglichkeit stellt einen großen Schritt für die digitale Forensik dar, wie das praktische Beispiel zeigen soll. Die von Facebook angeforderten Daten gehen weit über das hinaus, was auf einem Nutzerprofil dargestellt wird. So werden alle Interaktionen mit anderen Nutzern aufgezeichnet, sofern der Nutzer diese nicht gelöscht hat. Doch um zu verifizieren, wer diese Interaktionen durchführt oder welche natürlich identifizierbare Person hinter dem Nutzerprofil steht, reichen diese Informationen nicht aus, sofern der Inhalt der Interaktionen keine Informationen bereithält. Um dies ermitteln zu können reichen die veröffentlichten Inhalte nicht aus, denn einen Kommentar oder ein Bild kann jeder hochladen. Facebook speichert aber auch technische Daten, die für die Nutzung der Plattform interessant sind und benötigt werden. Darunter fallen dann insbesondere Gerätedetails, welche eine Identifikation des Gerätes ermöglichen, von welchem aus diese Aktivität getätigt werden. Über mehrere Speicherorte verstreut liegen einzelne Informationen, welche zusammengesetzt ein klares und strukturiertes Gesamtbild ergeben können. So werden Geräteversionen, Anmeldungen, IP-Adressen und anhand dieser sogar Standorte des Gerätes aufgezeichnet,

und so lassen sich Informationen zu den einzelnen Aktionen im sozialen Netzwerk feststellen und kombinieren.

In den letzten Jahren ist die Anzahl der im Internet begangenen Straftaten deutlich gestiegen, allein von 2015 auf 2016 um 80,5 Prozent. Auch das Tatmittel Internet wird immer beliebter, um Tatverwirklichungen umzusetzen. Insbesondere für die Verteilung von Botnetzen oder Schadsoftware eignen sich soziale Netzwerke, denn durch die Netzstruktur ist eine einfache und großflächige Verbreitung möglich, oftmals über versendete Nachrichten mit infizierten Anhängen. (33)

Doch rein an einer Nachricht lässt sich nicht sagen, ob ein Nutzer diese Nachricht eigenständig versendet hat oder ob möglicherweise ein Dritter involviert ist. Hier kommt dann die digitale Forensik zum Einsatz und soll die digitalen Spuren auswerten und analysieren. Die von Facebook im Rahmen der Informationspflichten mitgeteilten Daten können hier von entscheidendem Vorteil sein. Mithilfe der technischen Daten, die so nicht auf dem Nutzerprofil einsehbar sind, kann dann verifiziert werden, von welchem Gerät aus diese Nachrichten verteilt worden sind und wer tatsächlich hinter den kriminellen Aktivitäten steht. Die Daten können durchaus auch als Indizien für weitere Ermittlungen bereitstellen.

Ebenso können diese Daten für das genutzt werden, wofür Facebook sie einsetzt: Profiling. Anhand der gesammelten Daten, sowohl den bereitgestellten, technischen und erhaltenen Daten kategorisiert Facebook den Nutzer, um so gezielt für ihn Werbung zu schalten. Anhand seines Nutzerverhaltens lassen sich Rückschlüsse auf seine Persönlichkeit zeigen. Eine Vielzahl an Eigenschaften, wie beispielsweise politischer Gesinnung, sexueller Orientierung oder sogar Intelligenz lassen sich mit diesen Daten ermitteln und können für strafrechtliche Ermittlungen, insbesondere in operativer Fallanalyse zur Erstellung von Täterprofilen, relevant sein und so auch Erkenntnisse über einen Nutzer geben.

Problematisch ist allerdings die Beschaffung dieser Daten, denn um an diese zu gelangen benötigt der Ermittler sowohl die E-Mail-Adresse des Nutzers als auch sein Passwort. Hierbei ist in der Regel die Mitarbeit des Nutzers hilfreich und würde zu einer Aufwands- und Zeitersparnis führen. Aber die Daten lassen sich auch weiterhin auf einem offiziellen, anderen Weg beschaffen. So kann ein Richter oder ein Staatsanwalt die Herausgabe der Daten direkt bei Facebook anfordern, um diese anschließend zu analysieren (29). Dauerte dieser Prozess in der Regel sechs Monate und mehr, so könnte sich dieser Prozess durch die neuen Datenschutzbestimmungen beschleunigen, denn nur ist es Facebook möglich, innerhalb von wenigen Minuten die gesamten Daten eines Nutzers bereitzustellen, die das Unternehmen über ihn sammelt. Hierbei ist aber zu berücksichtigen, dass das Misstrauen gegenüber Facebook stetig wächst und die jüngsten Skandale gezeigt haben, dass das Unternehmen nicht unumstritten ist, weshalb es durchaus berechtigt ist zu fragen, ob die bereitgestellten Daten tatsächlich alle Daten umfassen, die das Unternehmen über den Nutzer besitzt.

Dieses Fallbeispiel soll zeigen, wie der Datenschutz Möglichkeiten für digital forensische Arbeit schafft und wie diese aussehen kann. Im zweiten Teil der Arbeit wurde die Ausgangslage umgekehrt und es wurde ermittelt, welche forensischen Möglichkeiten für den Datenschutz von Vorteil sein können.

Hier stand der praktische Nutzen im Vordergrund, denn die technische Umsetzung des Datenschutzes ist weiterhin ein großes Problem in der freien Wirtschaft. Auch wie man mögliche Verletzungen des Datenschutzes nachweisen soll ist noch ein neu zu erforschendes Feld.

Forensische Untersuchungen sind in der freien Wirtschaft nicht gerne gesehen, denn die Forensik beachtet die Wirtschaftlichkeit nur in Bezug auf die eigene Arbeit, also welche Methoden sind wirtschaftlich und mit den verfügbaren Ressourcen umsetzbar, um eine bestimmte Spur zu finden und zu sichern. Welche wirtschaftlichen Folgen diese Sicherung hat werden nicht beachten. Auch die aus den Ergebnissen resultierenden Folgen spielen für die Forensik keine Rolle, denn diese ist nur an einer gewissenhaften Aufklärung interessiert. Für Unternehmen sind dies aber Faktoren, die alles ausmachen können. So sind die Bußgelder, die für Datenschutzverletzungen ausgesprochen werden können, mit bis zu 20 Millionen Euro oder vier Prozent des weltweiten Jahresumsatzes durchaus ein enormes Risiko für ein Unternehmen. Sollte es aber zu einer Datenschutzverletzung kommen so ist von Unternehmensseite aus zu prüfen, ob diese Verletzung durch ein fehlerhaftes Managementsystem entstanden ist oder ob eine Verletzung dieses Managementsystems vorlag, denn dadurch kann sich dann entscheiden ob der Verantwortliche das Bußgeld alleine zahlen muss oder ob er einen weiteren beteiligten miteinbeziehen kann. Dafür eignen sich eigene interne Untersuchungen eher also offizielle forensische Gutachten, welche neben einem Einbruch der Wirtschaftlichkeit eines Unternehmens auch Image-Schäden zur Folge haben können.

Daher wurden einige Tools, die in der Forensik Anwendung finden, dargestellt, welche zum Nachweis von Datenschutzverletzungen eingesetzt werden können und die aber auch einen wirtschaftlichen Faktor für die Unternehmen beachten, da sie alle Open-Source Lösungen sind sowie im laufenden System eingesetzt werden können. Dadurch wird zwar nicht die 100 prozentige Unberührbarkeit des Systems gewährleistet, kann aber ebenso gute Erkenntnisse liefern. Diese können dann als Grundlage für weitere Untersuchungen dienen und mithilfe anderer Ergebnisse kombiniert und verifiziert werden.

Vorgestellt wurden insgesamt fünf Tools, die jeweils einen Bereich abdecken sollen, in dem Datenschutzverletzungen entstehen und nachgewiesen werden können. Die private Nutzung von Internet stellt an sich in der Regel keine Datenschutzverletzung dar, stellt aber ein Sicherheitsrisiko dar, welches die Datensicherheit gefährden kann. Sobald der Arbeitgeber die private Nutzung gestattet so wird er nach Telemediengesetz zum Diensteanbieter, und damit unterliegen die durch die private Nutzung entstehenden Daten dem Fernmeldegeheimnis und der Arbeitgeber darf diese nicht mehr nutzen oder einsehen. Per schriftlichem Verzicht auf sein Fernmeldegeheimnis besteht allerdings die Möglichkeit, die private

Nutzung des Internets und die Einsicht der Daten zu gewährleisten, verlangt aber noch weitere Vorkehrungen bezüglich der privaten Nutzung, wie beispielsweise einer getrennten Speicherung von privaten und beruflichen Daten. Ein Verstoß gegen solche Bestimmungen stellt eine arbeitsrechtliche Pflichtverletzung dar und kann zur Kündigung für den Mitarbeiter führen. Daher besteht durchaus das Interesse von Arbeitgebern, sicher zu prüfen, ob seine Mitarbeiter sich an diese Bestimmungen halten oder nicht. Der vorgestellte History Spy zeigt hierbei nur eine Möglichkeit auf, wie die private Nutzung nachgewiesen werden kann.

Um unberechtigte Weitergaben oder Sicherheitslücken im System zu finden lohnt sich der Einsatz von sogenannten Portscannern. Diese zeigen alle anwendungsspezifischen Ports des Gerätes an und die Nutzung dieser. Sollte ein offener und ungeschützter Port zu finden sein, so stellt dies ein erhebliches Sicherheitsrisiko dar, da ein potentieller Angreifer über diesen Zugang zum System erlangen kann. Auch die Weitergabe von Daten durch Programme kann so erkannt werden, denn geben diese über unsichere Ports Daten weiter so kann dies mithilfe der Portscanner erkannt werden.

Spezifische Tools, die eigens für bestimmte Betriebssystem entwickelt wurden, können ebenfalls zum Nachweis von Verletzungen der Datensicherheit eingesetzt werden. Ausgewählt wurden mehrere Tools für Windows-Betriebssysteme, da dieses das am weitesten verbreiteten Betriebssystem ist und durch eigene Features die forensische Nachweisbarkeit erleichtert. Eines dieser Features sind die sogenannten Jump-Lists, in welchen Einträge der zuletzt geöffneten Dateien angelegt wurden. Private Nutzung oder unberechtigter Zugriff kann somit nachgewiesen werden. Eine erweiterte Übersicht über die Aktivitäten des Nutzers bieten der LastActivityViewer, der aus diversen Quellen eine Übersicht erstellt, in der die Aktivitäten zu sehen sind. Hierbei geht es über die Jumplists hinaus und zieht Daten aus den Log-Dateien, Prefatch-Dateien und der Registry-Datenbank heran. Erweitert dazu kann dann der MyEventViewer verwendet werden, der eine alternative zum windowseigenen Eventviewer darstellt, die Übersicht aber vor allem bei der Erstellung von Zeitachsen besser gewährleistet.

5.2 Fazit

Die Forensik wird oftmals als Querschnittswissenschaft bezeichnet, also als eine „interdisziplinäre, mehrere Einzelwissenschaften übergreifende Wissenschaft“ (31). Die Grenzen zwischen den einzelnen Bereichen sind oftmals offen und leicht zu kreuzen. So benötigt man für die Rekonstruktion eines abgegebenen Pistolenschusses mit Folge einer körperlichen Verletzung einer Person Kenntnisse in Physik, Biologie, Kriminalistik und auch der digitalen Forensik, beispielsweise bei der digitalen Rekonstruktion. Allein dieses Beispiel zeigt deutlich, wie umfangreich die Forensik sein kann und worauf alles zu achten ist, um gewissenhafte und fehlerlose forensische Arbeit zu leisten. Insbesondere die digitale

Forensik sticht hier heraus, da sie mit ihren eigenen Methoden oftmals dafür genutzt wird, die anderen forensischen Bereiche zu unterstützen und die Arbeit in diesen zu vereinfachen.

Der Datenschutz ist hingegen als der „Schutz personenbezogener Daten“ (32) definiert, also nicht als eine Wissenschaft. Doch hinter diesem formal definierten Ziel verbirgt sich doch durchaus mehr. Denn um diesen Schutz zu gewährleisten müssen, ähnlich wie bei der Forensik, mehrere Teilgebiete beachtet werden. Zum ersten sind hier ganz klar die gesetzlichen Grundlagen zu nennen. Durch (mittlerweile) umfangreiche Datenschutzgesetze soll gewährleistet werden, dass die Daten von natürlich lebenden Personen weltweit geschützt werden sollen. Ein weltweit gesamteinheitliches Bild existiert hierfür allerdings nicht, obwohl Ansätze geschaffen wurden. Des Weiteren gilt es, stets die am besten geeigneten technischen und organisatorischen Maßnahmen zu treffen, um die Sicherheit der Daten zu gewährleisten. Kenntnisse aus dem Risikomanagement sind ebenfalls von Vorteil, denn die Entscheidung für eine Maßnahme kann nur nach einer vernünftigen Risikoanalyse erfolgen.

Der Datenschutz zeigt sich also auch als genauso vielschichtig wie die digitale Forensik. Die Schnittmenge aus beiden stell sich als vielseitig dar, denn so kann nicht nur der Datenschutz für die Forensik unterstützend agieren, sondern auch umgekehrt. Ein umgesetztes Datenschutzkonzept kann für einen Forensiker von immensem Vorteil sein, um schnell und effizient bestimmte Sachverhalte zu untersuchen. Fehlt diese Dokumentation so fehlt oftmals der Kontext zu den gewonnenen Erkenntnissen und es wird schwerer die einzelnen Puzzlestücke zusammenzusetzen. Auch durch die neu geschaffenen Gesetze können Forensiker bei Untersuchungen ganz andere Informationen zur Verfügung stehen, deren Verwendung von der Erstellung von Profilen bis einer Time-Line-Analysis, dem Erstellen und Analysieren von Geschehnissen in einem bestimmten Zeitraum, reichen können. Das Erlangen von Datensätzen aus externen Quellen ist somit vereinfacht worden, allerdings fehlt es hier noch an einer klaren Rechtsprechung, die einen noch effektiveren Weg zum Erlangen dieser Daten für Strafermittlungsbehörden bereitstellt. In naher Zukunft ist eine Verbesserung dieses Problems aber absehbar.

Umgekehrt bietet die Forensik das Potential, die umgesetzten Maßnahmen zu prüfen sowie deren Einhaltung zu verifizieren. Es besteht sogar die Möglichkeit, diese Maßnahmen, im Sinne eines Verantwortlichen, im Sinne der Wirtschaftlichkeit zu verbessern und so kosten- und aufwandeffizient wie möglich zu halten, allerdings in der Regel auf Kosten der forensischen Unveränderlichkeit der Spuren. Eine komplette forensische Untersuchung eignet sich daher überwiegend bei schweren Verstößen oder schweren Straftatbeständen, für intern angelegte Untersuchungen würden sie den Rahmen sprengen und die Wirtschaftlichkeit des Unternehmens zu sehr beeinträchtigen.

Es bleibt also festzuhalten, dass die Querschnittswissenschaft der Forensik zusammen mit dem vielseitigen Ziel des Datenschutzes sehr gut kombinierbar ist, und nicht nur theoretische und rechtliche Grundlagen füreinander schafft, sondern auch in der Praxis durchaus Anwendung finden kann und die beiden Themengebiete sich ergänzen können.

Index

Literatur

(1) Intersoft cinsulting Services AG, „Begriff und Geschichte des Datenschutz“, 28. Mai. 2014, https://www.datenschutzbeauftragter-info.de/begriff-und-geschichte-des-datenschutzes/, zuletzt aufgerufen am 13.09.2018 um 14:09

(2) Die Bundesbeauftragte für den Datenschutz und die Informationssicherheit, „Datenschutz-Grundverordnung, BfDI – Info 6“, Bonn, Die Bundesbeauftragte für den Datenschutz und die Informationssicherheit, 5. Auflage, September 2017

(3) Siller, Prof. (FH) Mag. Dr. Helmut, „Forensik - Definition“, 19.02.2018, https://wirtschaftslexikon.gabler.de/definition/forensik-53390/version-276483, zuletzt aufgerufen am 13.09.2018 um 14:18

(4) Joho, Katja, „Großkonzern Kirche“, Wirtschaftswoche, 25.11.2011, https://www.wiwo.de/unternehmen/dienstleister/finanz-riese-gross-konzern-kirche/5220262.html, zuletzt aufgerufen am 13.09.2018 um 14:37

(5) Dwyer, Catherine; Hiltz, Starr Roxanne; and Passerini, Katia, “Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and Myspace”, 2007, AMCIS 2007 Proceedings 339

(6) Statista.com, “Ranking der größten sozialen Netzwerke und Messenger nach der Anzahl der monatlich aktiven Nutzer (MAU) im Januar 2018 (in Miilionen)“, 2018, https://de.statista.com/statistik/daten/studie/181086/umfrage/die-weltweit-groessten-social-networks-nach-anzahl-der-user/, zuletzt aufgerufen am 12.09.2018 11:23

(7) Wölwer, Felix, „Facebook – was ist das? Einfach erklärt“, 12.06.2015, Chip.de, https://praxistipps.chip.de/facebook-was-ist-das-einfach-erklaert_41486, zuletzt aufgerufen am 14.09.2018 um 14:53

(8) Facebook Inc, „Facebook Reports Second Quarter 2018 Results “, 25. Juli 2018, Menlo Park, Calif

(9) Facebook Inc., “Datenrichtlinie”, letzte Überarbeitung am 19. April 2018, https://de-de.facebook.com/policy.php, zuletzt aufgerufen am 14.09.2018 um 14:58

(10) Landau, Susan, „What went wrong? Facebook and Sharing Data with Cambridge Analytica”, 28.03.2018, ACM-0001-0782/18/6

(11) Deutscher Bundestag, “Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Jan Korte, Dr. Petra Sitte, weiterer Abgeordneter und der Fraktion DIE LINKE. Drucksache 17/6100 – Nutzung sozialer Netzwerke zu Fahndungszwecken“, 14.07.2011, Drucksache 17/6587 Bundesanzeiger Verlagsgesellschaft mbH

(12) Kosinski, Michal; Stillwell, David; and Graepel, Thore, „Private traits and attributes are predictable from digital records of human behavior“, Proceedings of the National Academy of Sciences (PNAS), 2013.

(13) Deutsches Institut für Vertrauen und Sicherheit im Internet, „Allgemeine Geschäftsbedingungen (AGB) von Kommunikationsdienstleistern“, 2015, DIVSI Deutsches Institut für Vertrauen und Sicherheit im Internet Hamburg

(14) Staatsbetrieb Sächsische Informatikdienste, „Anlage des Handlungsleitfadens zur Umsetzung de SächsEGovG für staatliche Behörden“, Dezember 2014, https://www.opendata.sachsen.de/HLF/8_Maschinenlesbare_Dateiformate.pdf, zuletzt aufgerufen am 13.09.2018 um 15:28

(15) AVTest GmbH, „Security Report 2015/16“, 2016, Magdeburg

(16) SecurityXploded, “Browser History Spy”, https://securityxploded.com/browser-history-spy.php, zuletzt aufgerufen am 13.09.2018 um 15:36

(17) Touch, Joe, „Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry“, August 2015, Marine del Rey, USA

(18) Sofer, Nir, “CurrPorts v2.51 - Monitoring Opened TCP/IP network ports / connections“, https://www.nirsoft.net/utils/cports.html, zuletzt aufgerufen am 13.09.2018 um 15:50

(19) DEFT Association, http://www.deftlinux.net/about/, zuletzt aufgerufen am 14:09.2018 um 14:33

(20) WINEHQ, https://www.winehq.org/about, zuletzt aufgerufen am 14.09.2018 um 14:35

(21) Sofer, Nir, “JumpListsView v1.16 – View jump lists information stored by Windows 7” , https://www.nirsoft.net/utils/jump_lists_view.html, zuletzt aufgerufen am 14.09.2018 um 14:37

(22) Kolar, Sebastian, “Windows-Jumplists: Programme mit praktischem Kontextmenü”, 01.07.2018 16:00, COMPUTER BILD, http://www.computerbild.de/artikel/cb-Tipps-Software-Windows-Jumplist-Programme-21835847.html, zuletzt aufgerufen am 14.09.2018 um 14:42

(23) Sofer, Nir, “LastActivityView v1.32”, https://www.nirsoft.net/utils/computer_activity_view.html, zuletzt aufgerufen am 14.09.2018 um 14:43

(24) Sofer, Nir, “MyEventViewer v2.25 – Alternative to the standard event viewer of Windows”, http://www.nirsoft.net/utils/my_event_viewer.html, zuletzt aufgerufen am 14.09.2018 um 14:46

(25) Sofer, Nir, „BrowsingHistoryView v2.17 – View browsing history of your Web browsers“, https://www.nirsoft.net/utils/browsing_history_view.html, zuletzt aufgerufen am 14.09.2018 um 15:12

(26) Digital Forensics Studio, „History Viewer – a free digital forensics software to view history data“, http://www.historyviewer.net/, zuletzt aufgerufen am 14.09.2018 um 15:13

(27) Brien, Jörn, „Daten protokolliert: Facebook weiß, mit wem du telefoniert hast“, 25.03.2018, yeebase media GmbH, https://t3n.de/news/daten-protokolliert-facebook-998868/, zuletzt aufgerufen am 19.09.2018 um 13:13

(28) Institut für Demoskopie Allensbach, „Jacobs Studie 2014 – Freunde fürs Leben“, 2014

(29) Banse, Philip, „Wie die Polizei bei Facebook, Twitter etc. ermittelt“, Wordpress, 2012

(30) Facebook Inc, „Messenger´s 2017 Year in Review”, 2017

(31) ”Querschnittswissenschaft" beim Online-Wörterbuch Wortbedeutung.info (21.9.2018), https://www.wortbedeutung.info/Querschnittswissenschaft/, zuletzt aufgerufen am 25.09.2018 um 13:33

(32) "Datenschutz" beim Online-Wörterbuch Wortbedeutung.info (21.9.2018), https://www.wortbedeutung.info/Datenschutz/, zuletzt aufgerufen am 25.09.2018 um 13:34

(33) Bundeskriminalamt, „Cybercrime – Bundeslagebild 2016“, Bundeskriminalamt, 2016

(34) Katholisches Datenschutzzentrum, „AB-Deutschlandkarte-DS-Aufsichten.jpg“, 2018 , https://www.katholisches-datenschutzzentrum.de/wir-ueber-uns/konferenz-der-dioezesandatenschutzbeauftragten/,

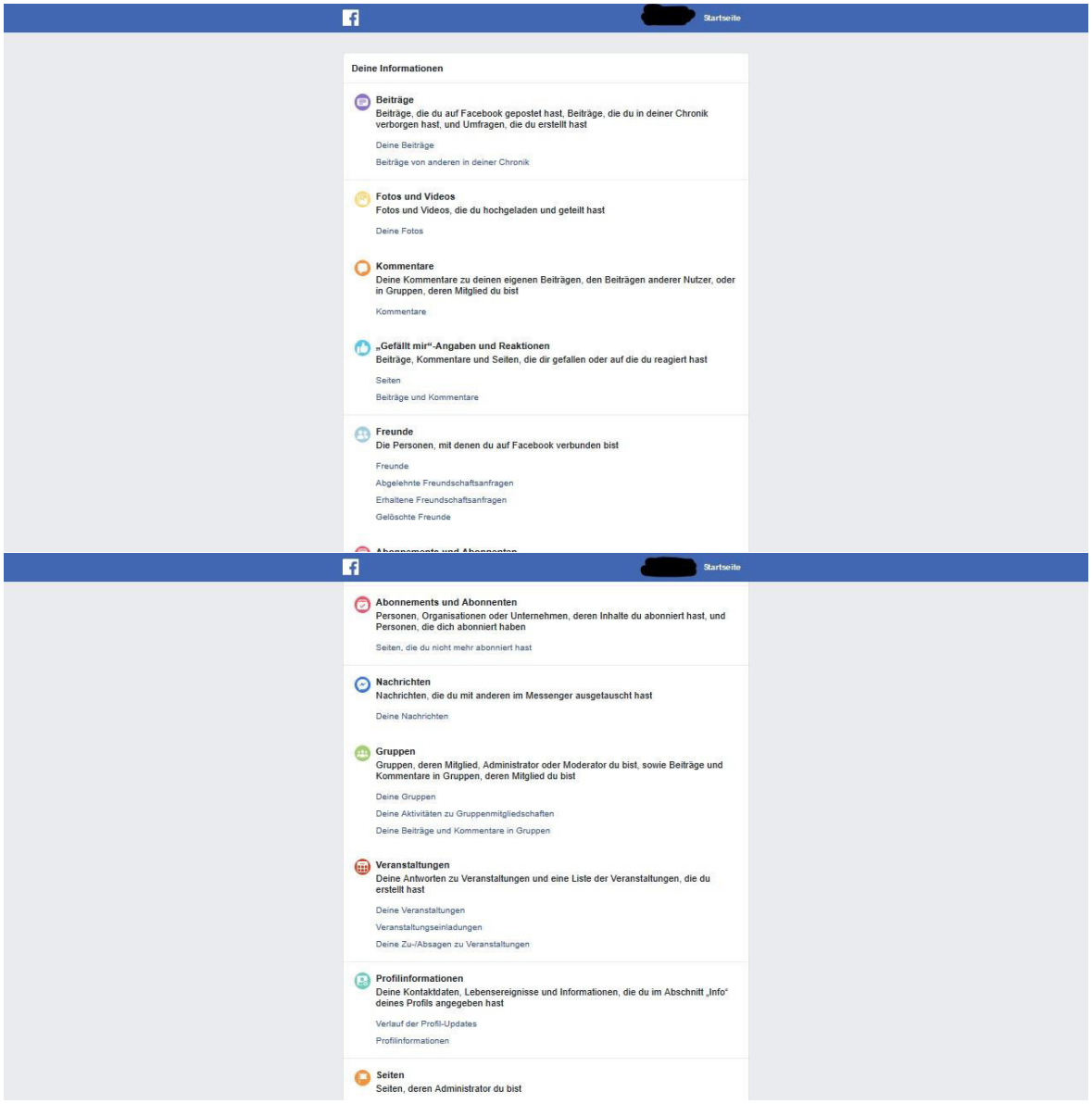
(35) Statista.com, „Marktanteile der führenden Betriebssysteme in Deutschalnd von Januar 2009 bis Mai 2018“, 2018,

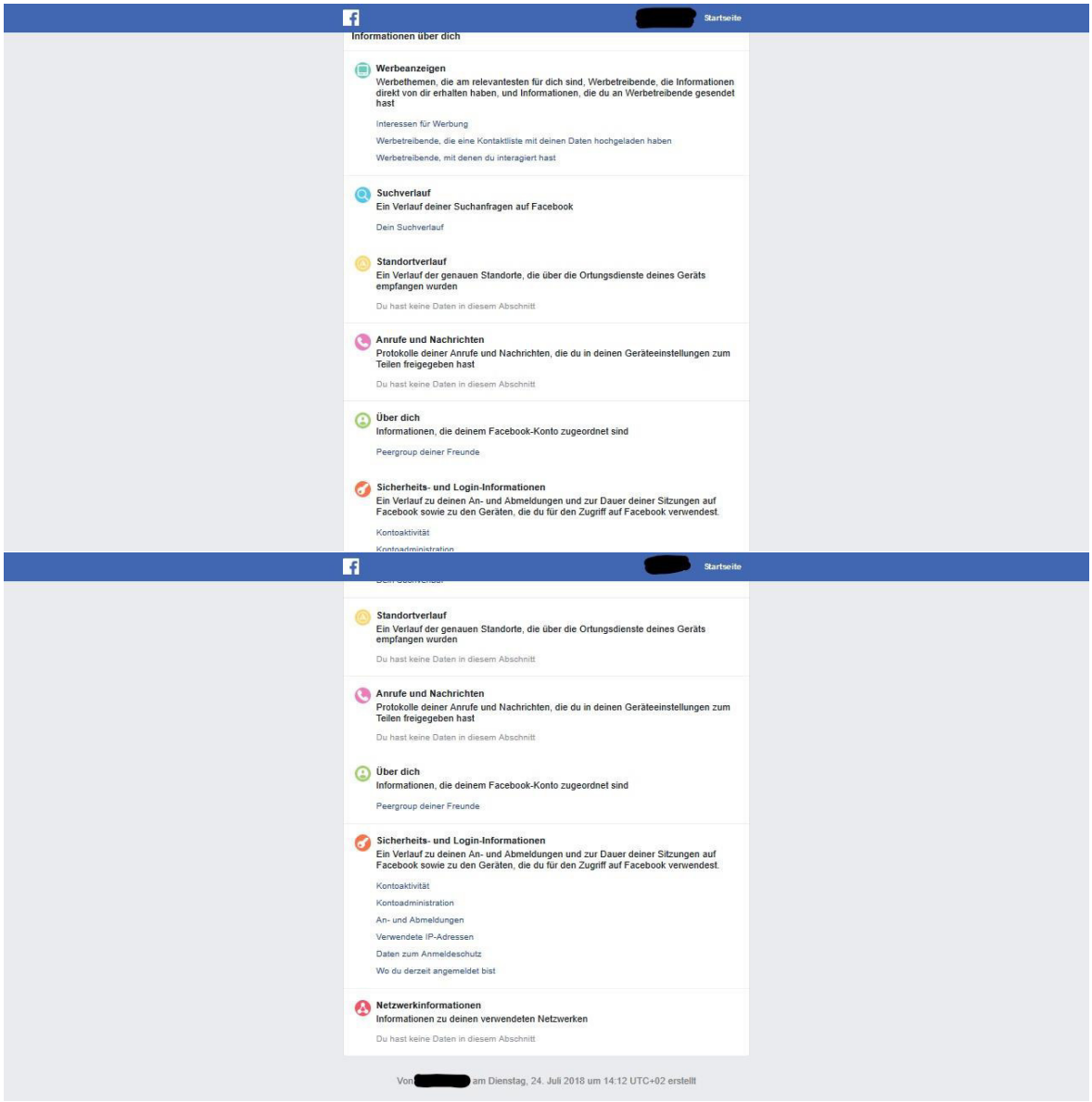
(36) Facchi, Christian. „Methodik zur formalen Spezifikation des ISO-OSI-Schichtenmodells“. Herbert Utz Verlag, 1995.

Anlagen

Anlagen, Teil 1

Navigationsansicht der HTML-Übersicht der erhaltenen Facebook-Daten (anonymisiert)




[redacted] Startseite
Informationen über dich
Werbeanzeigen
Werbethemen, die am relevantesten für dich sind, Werbetreibende, die Informationen direkt von dir erhalten haben, und Informationen, die du an Werbetreibende gesendet hast
Interessen für Werbung
Werbetreibende, die eine Kontaktliste mit deinen Daten hochgeladen haben
Werbetreibende, mit denen du interagiert hast
Suchverlauf
Ein Verlauf deiner Suchanfragen auf Facebook
Dein Suchverlauf
Standortverlauf
Ein Verlauf der genauen Standorte, die über die Ortungsdienste deines Geräts empfangen wurden
Du hast keine Daten in diesem Abschnitt
Anrufe und Nachrichten
Protokolle deiner Anrufe und Nachrichten, die du in deinen Geräteeinstellungen zum Teilen freigegeben hast
Du hast keine Daten in diesem Abschnitt
Über dich
Informationen, die deinem Facebook-Konto zugeordnet sind
Peergroup deiner Freunde
Sicherheits- und Login-Informationen
Ein Verlauf zu deinen An- und Abmeldungen und zur Dauer deiner Sitzungen auf Facebook sowie zu den Geräten, die du für den Zugriff auf Facebook verwendest.
Kontoaktivität
Kontoadministration
[redacted] Startseite
Standortverlauf
Ein Verlauf der genauen Standorte, die über die Ortungsdienste deines Geräts empfangen wurden
Du hast keine Daten in diesem Abschnitt
Anrufe und Nachrichten
Protokolle deiner Anrufe und Nachrichten, die du in deinen Geräteeinstellungen zum Teilen freigegeben hast
Du hast keine Daten in diesem Abschnitt
Über dich
Informationen, die deinem Facebook-Konto zugeordnet sind
Peergroup deiner Freunde
Sicherheits- und Login-Informationen
Ein Verlauf zu deinen An- und Abmeldungen und zur Dauer deiner Sitzungen auf Facebook sowie zu den Geräten, die du für den Zugriff auf Facebook verwendest.
Kontoaktivität
Kontoadministration
An- und Abmeldungen
Verwendete IP-Adressen
Daten zum Anmeldeschutz
Wo du derzeit angemeldet bist
Netzwerkinformationen
Informationen zu deinen verwendeten Netzwerken
Du hast keine Daten in diesem Abschnitt
Von [redacted] am Dienstag, 24. Juli 2018 um 14:12 UTC+02 erstellt

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Simmerath, den 30.09.2018

_____

Andreas Thomas Kayser