Hochschule Wismar
Fakultät für Ingenieurwissenschaften
Bereich Elektrotechnik und Informatik

Master-Thesis

Ist ganzheitliche Informationssicherheit für Bürger in Deutschland möglich?

von: M.G.

Das Internet ist ein Überwachungsstaat. Ob wir es uns eingestehen oder nicht, und ob wir es wollen oder nicht, wir werden ständig verfolgt.

Bruce Schneier, 25.03.2013

Aufgabenstellung

Der Bürger[1] als tragende Säule der Gesellschaft wird im Bereich der Informationssicherheit aus meiner Sicht viel zu kurz bzw. ‚stiefmütterlich' behandelt. Einerseits bspw. durch den Umgang der Firma Microsoft ggü. privaten Kunden, was die Abschaltung von Telemetrie Daten angeht, die nur bei Firmenkunden dagegen vollumfänglich möglich sind s. [1]. Andererseits beispielsweise durch die Politik, die den Bürger nicht vor der Massen-Spionage durch einen anderen Staat, hier durch die National Security Agency (NSA) der Vereinigten Staaten von Amerika, schützt s. [2]. Daher kam die Frage auf, wie es zu dieser Entwicklung kommen konnte und die Ursachen hierfür sind nicht eindeutig auszumachen. Das liegt zum einen der Tatsache geschuldet, dass Informationstechnik einerseits ein Querschnittsthema ist und somit viele Bereiche des alltäglichen Lebens berührt. Andererseits wird Informationstechnik aus verschiedenen Blickwinkeln sehr unterschiedlich betrachtet, so dass es schwierig ist, sich eine eindeutige Meinung zu bilden. Mit Blickwinkeln ist hier insbesondere der Blick des Bürgers einschließlich der Psychologie gemeint. Die Psychologie spielt deswegen hier eine Rolle, da es beispielsweise eine kognitive Dissonanz zum Thema Massenüberwachung bei der Mehrheit der Bürger gibt s. [3, p. 42] . Durch Edward Snowden ist die Massenüberwachung durch die NSA einer breiten Öffentlichkeit bekannt geworden. Dennoch wurden Schutzmechanismen wie bspw. E-Mailverschlüsselung von der Mehrheit der Bevölkerung nicht in Anspruch genommen, obwohl „[d]rei Viertel der deutschen Internetnutzer … es wichtig [finden], E-Mails … [zu] verschlüsseln." [4]. Daneben kommt der jeweilige Blickwinkel der Hersteller, der Dienstleister - die Services (z.B. Apps) zur Verfügung stellen -, der Regierung einschließlich der öffentlichen Verwaltung, der Geheimdienste sowie der Politik einschließlich der Geostrategie. Daher ist das Ziel meiner Masterthesis sich einen Gesamtüberblick darüber zu verschaffen, welche Faktoren auf die Informationssicherheit des Bürgers einwirken bzw. voneinander abhängig sind und ob dieser in der Lage ist, überhaupt - auch langfristig - Informationssicherheit zu realisieren. Die Informationssicherheit bringt auch seinen Anteil für die Demokratie in Deutschland bei, denn eine „verdeckte Einflussnahme auf politische Wahlen" durch andere Staaten ist bspw. eine Gefahr für die unbeeinflusste Ausübung des Wahlrechts durch den Bürger s. [5]. Daher zählt auch die Prüfung der gegenwärtigen rechtlichen und technischen Rahmenbedingungen, ob der Bürger es so einfach wie möglich ausüben kann. Dies schließt auch die Option, wie man Informationssicherheit langfristig realisieren kann, mit ein. Aus meiner Sicht reichen daher die bisherigen klassischen Schutzziele „Vertraulichkeit, Verfügbarkeit und Integrität" bei weitem nicht mehr aus. Aus diesem Grund wird entweder der bisherige Begriff „Informationssicherheit" um weitere Aspekte erweitert oder es wird ein neuer Begriff geschaffen, der eine ganzheitliche Sichtweise ermöglicht. Anschließend wird ein ganzheitliches Sicherheitskonzept für den Bürger erstellt, der all die o.g. Schutzziele berücksichtigt.

[1] In dieser Masterarbeit sind bei Bürgern bzw. Nutzern stets Personen jedweden Geschlechts gemeint.

Kurzreferat

Ziel dieser Masterarbeit ist es, den Begriff der Informationssicherheit einer kritischen Analyse zu unterziehen und im Hinblick auf neuere Entwicklungen bzw. Erkenntnisse weiter zu entwickeln. Der Fokus werden nicht - wie sonst üblich - nur die sog. technische bzw. organisatorische Aspekte sein, sondern es werden weitere Faktoren, die auf den Bürger bei der Informationssicherheit einwirken, betrachtet. Die bisherige und getrennte Betrachtungsweise nur auf den technischen Aspekt bzw. auf den organisatorischen oder rechtlichen Aspekt lässt andere Aspekte wie Dark Pattern, Big Data usw. außen vor und ermöglicht damit keinen ganzheitlichen Blick auf die Informationssicherheit. Ein Beispiel: Eine technische Forderung der Informationssicherheit ist es, die Zwei-Faktor-Authentisierung (2FA) zu nutzen, um u.a. die Authentifizierung zu gewährleisten. Im Zusammenhang mit Facebook ist diese Forderung kontraproduktiv, wenn der Facebook-Nutzer bislang darauf geachtet hat, keine Handynummer im Profil von Facebook zu hinterlegen. Durch die Umsetzung auf die 2FA hat Facebook rechtswidrig die Handynummer zu Werbezwecken missbraucht s. [6]. Die o.g. Faktoren bilden einen Rahmen ab. Hier wird geprüft werden, ob die Rahmenbedingungen nicht nur einzeln, sondern auch insgesamt zu Lasten oder zu Gunsten des Bürgers gehen können. Sobald diese identifiziert und erarbeitet worden sind, ist das Ziel daraus ableitend ein ganzheitliches Sicherheitskonzept zu entwickeln, um einen adäquaten Schutz für den Bürger zu ermöglichen. Dazu wurde anschließend Prof. Dr. Hannes Federrath, Präsident der Gesellschaft für Informatik, befragt, ob aus seiner jeweiligen Sicht eine ganzheitliche Informationssicherheit für Bürger möglich ist. In diesem Zusammenhang wird geprüft, welche technischen (Schutz-)Tools hierfür in Frage kommen würden. Diese Arbeit soll auch als Ausgangspunkt für Forscher dazu dienen, tiefergehend die herausgearbeiteten Faktoren zu behandeln und ggf. weitergehende Fragen zu stellen, wie Informationssicherheit langfristig für alle Bürger gewährleistet werden kann. Es kann aufgrund der Komplexität des Themas Informationssicherheit schwerpunktmäßig nur diejenigen Faktoren ausgearbeitet werden, die wesentlich auf den Bürger einwirken. Zum einen wird dadurch sichergestellt, dass die Masterarbeit im angemessenen Rahmen bleibt und zum anderen muss es für die Zielgruppe - hier der Bürger - handhabbar sein. Was die Auswahl der möglichen technischen (Schutz-)Tools angeht, so werden diese nicht der technischen Analyse unterzogen.

Abstract

The aim of this master's thesis is to subject the concept of information security to a critical analysis and to develop it further with regard to more recent developments or findings. The focus will not - as is usually the case - be only on the so-called technical or organizational aspects, but will look at other factors that affect the citizen in information security. The previous and separate approach of focusing only on the technical aspect or on the organizational or legal aspect leaves out other aspects such as Dark Pattern, Big Data, etc. and thus does not allow for a holistic view of information security. For example, one technical requirement of information security is to use two-factor authentication (2FA) to ensure authentication, among other things. In the context of Facebook, this requirement is counterproductive if the Facebook user has so far been careful not to store a cell phone number in the Facebook profile. By switching to 2FA, Facebook has unlawfully misused the cell phone number for advertising purposes s. [6]. The above factors provide a framework. Here, it will be examined whether the framework can be harmful or beneficial to the citizen, not only individually, but also as a whole. As soon as these have been identified and worked out, the aim is to develop a holistic security concept to provide adequate protection for the citizen. Prof. Dr. Hannes Federrath, President of the German Informatics Society, was asked from his point of view, if holistic information security for citizens is possible. In this context, it will be examined which technical (protection-) tools could be considered for this purpose. This work should also serve as a starting point for researchers to go deeper into the factors identified and, if necessary, to ask further questions about how information security can be ensured for all citizens in the long term. Due to the complexity of the topic of information security, the focus can only be on those factors that have a significant impact on citizens. On the one hand, this ensures that the master thesis remains within the appropriate scope and, on the other hand, it must be manageable for the audience group - here the citizen. As for the selection of possible technical (protection) tools, these will not be subjected to technical analysis.

Hinweis:
Für die Veröffentlichung der Masterarbeit wurden Anpassungen vorgenommen (u.a. Kürzungen im Anhang).

Inhalt

1. Einleitung

1.1 Einführung

Das Ziel dieser Masterarbeit ist die Erarbeitung von Faktoren, die wesentlich auf die Informationssicherheit des Bürgers einwirken. Nachdem diese identifiziert worden sind, wurde daraus folgend ein ganzheitliches Schutzkonzept entwickelt, um einen adäquaten Schutz für den Bürger - idealerweise - langfristig zu ermöglichen. Hierzu wurde Prof. Dr. Hannes Federrath befragt. Zweck der Befragung ist die Eruierung von Handlungsoptionen für den Bürger, um eine ganzheitliche Informationssicherheit realisieren zu können. In diesem Zusammenhang wurde geprüft, welche technischen (Schutz-)Tools hierfür in Frage kommen würden.

1.2 Problemstellung

Der Fokus der Informationssicherheit auf die drei klassischen Schutzziele - hier Vertraulichkeit, Integrität und Verfügbarkeit - reichen angesichts der zunehmenden Vernetzung von immer mehr internetfähigen IT-Systemen sowie der Weiterentwicklung von Analysemöglichkeiten, angefangen von Targeting, über Dark Pattern bis hin zu Big Data Mechanismen nicht mehr aus, um einen ganzheitlichen Schutz für den Bürger zu gewährleisten. Daher ist die bisherige Betrachtung rein auf technische, organisatorische bzw. personelle Schutzmaßnahmen zu kurz, da es weitere Faktoren gibt, die auf die Informationssicherheit der Bürger einwirken. Mit dieser Masterarbeit sollen diese (Schlüssel-)Faktoren identifiziert werden, um eine ganzheitliche Sichtweise zur Informationssicherheit zu ermöglichen. Daraus ableitend besteht die Herausforderung, die wesentlichen Schutzmaßnahmen zu identifizieren, um einen adäquaten Schutz zu gewährleisten.

1.3 Zielsetzung der Arbeit und Abgrenzung

Es kann aufgrund der Komplexität des Themas Informationssicherheit schwerpunktmäßig nur diejenigen Faktoren ausgearbeitet werden, die wesentlich auf den Bürger einwirken. Zum einen soll dadurch sichergestellt werden, dass die Arbeit im angemessenen Rahmen bleibt und zum anderen muss es für die Zielgruppe - hier der Bürger - handhabbar sein. Was die Auswahl der möglichen technischen (Schutz-)Tools angeht, so werden diese nicht der technischen Analyse unterzogen.

1.4 Stand der Forschung

In den einleitenden Worten zum Buch „IT-Sicherheit“ von Prof. Dr. Claudia Eckert steht wie folgt: „Informations- und Kommunikationstechnologie ist heute in nahezu allen Bereichen von zentraler Bedeutung. Eingebettete Systeme, Machine-to-Machine (M2M), Kommunikation, Vernetzung, aber auch on-demand beziehbare Mehrwertdienste aus der Cloud sind zentrale Wachstumstreiber … Der IT-Sicherheit kommt hierbei eine Schlüsselrolle zu“ [7, p. 1]. Die Grundaussage im letzten Satz ist eindeutig zu bejahen, denn die Digitalisierung nimmt immer weiter zu und der nachhaltige Erfolg hängt mit der Anwendung der Informationssicherheit zusammen. Umgekehrt bedeutet das, dass der heutige Alltag von immer mehr vernetzen IT-Systemen durchdrungen ist und damit verbunden auch die Grenzen zwischen der privaten und beruflichen Nutzung nicht mehr eindeutig sind. Das IT-System ist wie folgt definiert: „Ein IT-System ist ein geschlossenes oder offenes, dynamisches System mit der Fähigkeit zur Speicherung und Verarbeitung von Informationen.“ [7, p. 3].

In diesem Zusammenhang reicht es heute aufgrund der zunehmenden Digitalisierung und der damit verbundenen Vernetzung der IT-Systeme nicht mehr aus, in bislang getrennten Kategorien wie „Informationssicherheit“ bzw. „Cyber-Sicherheit“, „Datensicherheit“, sowie „Datenschutz“ zu klassifizieren. Der Begriff „Informationssicherheit“, der seit kurzem auch „Cyber-Sicherheit“ genannt wird, ist wie folgt definiert: „Cyber-Sicherheit befasst sich mit allen Aspekten der IT-Sicherheit, wobei das Aktionsfeld auf den gesamten Cyber-Raum ausgeweitet wird. Cyber-Raum umfasst in dieser Definition sämtliche mit dem globalen Internet verbundene IT und IT-Infrastrukturen sowie deren Kommunikation, Anwendungen, Prozesse mit Daten, Informationen und Intelligenzen.“ [8, p. 3]. Der Begriff Datensicherheit wird wie folgt definiert: „Die Datensicherheit ist die Eigenschaft eines funktionssicheren Systems, nur solche Systemstände anzunehmen, die zu keinem unautorisierten Zugriff auf Systemressourcen und insbesondere auf Daten führen. [Dies] umfasst … auch Maßnahmen zur Datensicherung.“ [7, p. 6]. Beim Begriff Datenschutz „versteht man die Fähigkeit einer natürlichen Person, die Weitergabe von Informationen, die sie persönlich betreffen, zu kontrollieren.“ [7, p. 6].

Daher ist eine ganzheitliche Sichtweise unumgänglich, um Informationssicherheit in allen Aspekten, die bislang getrennt betrachtet wurden, umfassend zu gewährleisten. Eine andere Herangehensweise hat Ross Anderson vorgenommen, in dem er ein (IT)-System mit der damit verbundenen Herausforderung, zwischen den einzelnen Punkten Klarheit zu schaffen, wie folgt beschreibt:

1. „ein Produkt oder Komponente, wie zum Beispiel ein kryptografisches Protokoll, eine Smartcard, oder die Hardware von einem Telefon, einem Laptop oder Server;

2. einer oder mehrere der oben genannten plus ein Betriebssystem, Kommunikation und andere Infrastruktur;

3. die oben genannten plus eine oder mehrere Anwendungen (Bank-App, Gesundheits-App, Medienspielgerät, Browser, Accounts / Gehaltspakete, und so weiter - einschließlich sowohl Client als auch Cloud Komponenten);

4. einen oder alle der oben genannten Punkte plus IT-Personal;

5. einen oder alle der oben genannten Punkte plus interne Nutzer und Management;

6. einen oder alle der oben genannten Punkte plus Konsumenten und andere externe Nutzer.“ [9, p. 12].

Bei der oben genannten Auflistung nimmt die Komplexität und die damit verbundene Abhängigkeit, die in der Informationssicherheit betrachtet werden muss, immer weiter zu. Parallel nehmen die Angriffsflächen bzw. die Risiken mit jedem aufsteigenden Punkt weiter zu.

Unter Information ist ein Abstraktum zu verstehen, „das in Form von Daten bzw. Datenobjekten repräsentiert wird.“ [7, p. 4], s. [7, p. 4]. Eine Unterscheidung erfolgt „zwischen passiven Objekten (z.B. Datei, Datenbankeintrag) mit der Fähigkeit, Informationen zu speichern, und aktiven Objekten (z.B. Prozesse) mit der Fähigkeit, sowohl Informationen zu speichern als auch zu verarbeiten. Informationen und Objekte, die sie repräsentieren, sind schützenswerte Güter (engl. asset) eines Systems.“ [7, p. 4]. In diesem Zusammenhang sind auch Informationskanäle wichtig. Hier wird zwischen legitimen und verdeckten Kanälen sowie Speicherkanälen unterschieden s. [7, p. 5]. „Die legitimen Kanäle sind diejenigen, die ein Subjekt in der Regel für den Informationsaustausch nutzt“ [7, p. 5]. Hingegen sind verdeckte Kanäle nicht für einen Informationstransfer vorgesehen, die dennoch missbraucht werden können s. [7, p. 5]. Speicherkanäle sind Objekte, die von Subjekten gemeinsam benutzt werden können s. [7, p. 5].

Die klassischen Schutzziele der Informationssicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit s. [10, p. 8]. Der Begriff Vertraulichkeit ist wie folgt definiert: „Das System [gewährleistet] die Informationsvertraulichkeit …, wenn es keine unautorisierte Informationsgewinnung ermöglicht.“ [7, p. 10]. Integrität bedeutet, wenn „das System die Datenintegrität gewährleistet, wenn es Subjekten nicht möglich ist, die zu schützenden Daten unautorisiert und unbemerkt zu manipulieren.“ [7, p. 9]. Verfügbarkeit ist wie folgt definiert: „[D]ie Verfügbarkeit [ist] gewährleistet, wenn authentifizierte und autorisierte Subjekte in der Wahrnehmung ihrer Berechtigungen nicht unautorisiert beeinträchtigt werden können.“ [7, p. 12].

1.5 Schadsoftware

Angriffe erfolgen meist mit Hilfe von Schadsoftware. Schadsoftware - auch Malware genannt - ist eine „Software, die bei Ausführung auf dem Zielrechner schädliche Operationen ausführt“ [11, p. 13], wobei nach folgenden Klassen unterschieden wird s. [11, p. 13]. In der Regel „besteht moderne Schadsoftware vielfach aus einer Kombination verschiedener Funktionalitäten, … [welches] modular aufgebaut und durch Nachladen weiterer

Schadcodes dynamisch veränderbar“ [11, p. 13] ist. Die „Entwicklung und [der] Vertrieb von Schadsoftware werden zunehmend professionalisiert, wobei die Angreifer mit Webseiten, Support oder Hosting Verfahren der normalen Software-Entwicklung adaptieren“ [11, p. 13], was als „Malware-as-a-Service” [11, p. 13] bezeichnet wird.

Viren

Viren sind eine „[k]lassische Form von Schadsoftware, die sich selbst verbreitet und unterschiedliches Schadpotenzial in sich tragen kann“ [11, p. 13]. Dabei treten „Viren … in Kombination mit einem Wirt auf“ [11, p. 13].

Trojanische Pferde

Trojanische Pferde sind eine „Schadsoftware, die sich in scheinbar nützlichen oder interessanten Dokumenten oder Programmen versteckt.“ [11, p. 13], wobei es „heimlich ausgeführt“ [11, p. 13] wird. Hier wird häufig versucht, „gezielt Informationen zu sammeln (Dateien, Tasteneingaben, Bildschirmfotos) und nach außen zu übertragen - ohne dabei entdeckt zu werden - oder Hintertüren zu öffnen, um Folgeangriffe zu ermöglichen.“ [11, p. 13].

Bots

„Ein Bot ist eine Schadsoftware, die einen Steuerkanal zum Angreifer aufbaut und ihm darüber die Kontrolle über das infizierte System erlaubt“ [11, p. 13] und wenn „ein Angreifer mehrere Bots unter seiner Kontrolle [hat], … [ist] von einem Botnetz“ [11, p. 13] zu sprechen. Botnetze werden meist bspw. „zur Versendung von Spam-Nachrichten, zur Durchführung von DDoS-Angriffen oder auch zur Weiterverbreitung und Vergrößerung des Botnetzes“ [11, p. 13] genutzt.

Würmer

„Ein Wurm ist eine Schadsoftware, die sich selbstständig über ein Netzwerk ausbreiten kann.“ [11, p. 13]. Dadurch „kommt es häufig zur Überlastung und zum Ausfall von Systemen und/oder Netzen“ [11, p. 13]. Zusätzliche Schadfunktionen sind bei dieser Schadsoftware auch möglich s. [11, p. 13].

Rootkits

Als Rootkit ist eine Schadsoftware, „die sich möglichst tief im angegriffenen System … versteck[t], um eine Erkennung durch ein Virenschutzprogramm zu verhindern.“ [11, p. 13]. Dabei können „[a]ndere Schadsoftware, wie z. B. Trojanische Pferde, können ebenfalls Rootkit-Funktionen enthalten.“ [11, p. 13].

Scareware

„Scareware ist eine Form von Schadsoftware, die der Nutzer selbst auf seinem System installiert." [11, p. 13]. Hier wird dem Nutzer vorgegaukelt, „dass ein Problem mit seinem Computer" [11, p. 13] vorhanden sei, was aber nicht der Fall ist.

Ransomware

„Ransomware (von engl. ransom - Lösegeld) ist eine Schadsoftware, die die Verfügbarkeit des Systems oder von Daten durch Verschlüsselung, Löschung oder Aussperrung stört und ein Lösegeld vom Opfer für den Zugang zu seinen Daten fordert." [11, p. 13].

Spyware

Spyware ist eine „Spionagesoftware, die … das Verhalten des Nutzers aufzeichnet." [11, p. 13].

Backdoors

„Backdoors sind Hintertüren, über die ein System vom Nutzer unbemerkt durch Dritte kontrolliert werden kann." [11, p. 13].

Von den o.g. Schadsoftwarearten sind Rootkits und Backdoors die gefährlichsten Varianten, da hierbei fast keine Möglichkeit besteht, diese zu entdecken bzw. im Nachhinein durch (System-)Protokollierung überhaupt bemerken zu können. Das gilt auch für Zero-Day-Schadprogramme, die noch nicht von den Herstellern von Sicherheitsprodukten als Schadprogramm klassifiziert worden sind.

1.6 Methodisches Vorgehen

Das methodische Vorgehen besteht hauptsächlich aus Recherchearbeiten sowie einer Befragung eines Informationssicherheitsexperten, hier Prof. Dr. Hannes Federrath.

2. Phasen eines Cyber-Angriffs

Um einen Cyber-Angriff schematisch einordnen zu können, ist ein Verständnis über den regulären Verlauf eines Cyber-Angriffs notwendig. In der Regel durchläuft ein Cyber-Angriff schematisch in drei Phasen ab. Die erste ist die Initiierungsphase, die Zweite die Vorbereitungsphase und die dritte und entscheidende Phase, die Durchführungsphase, wie es im folgenden Schaubild ersichtlich ist:

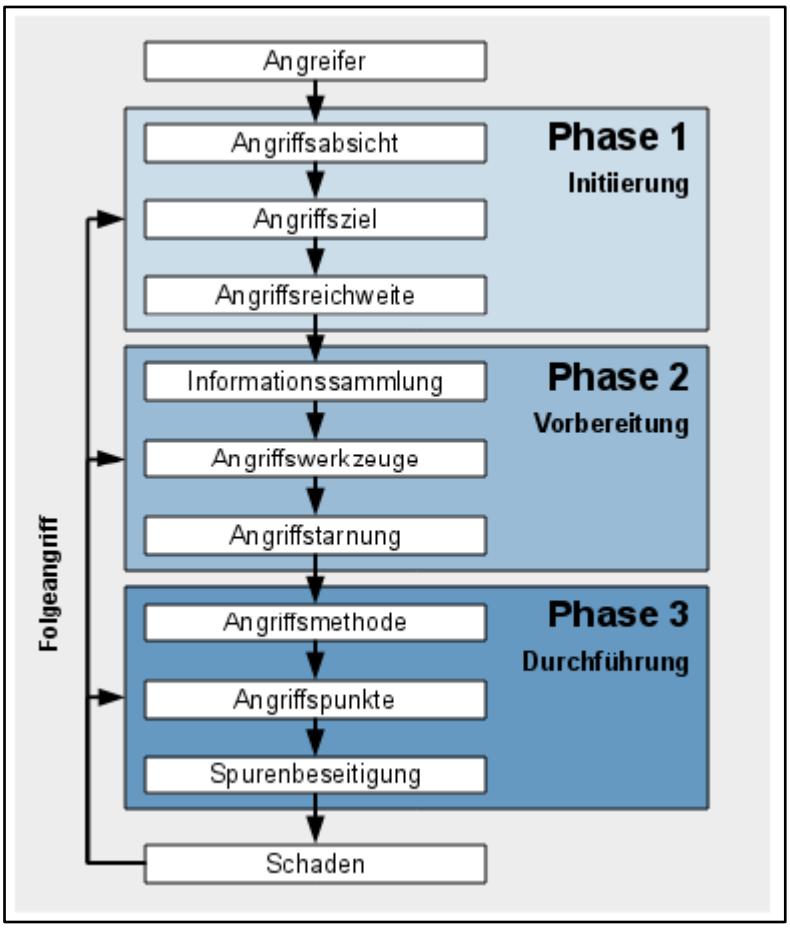


Bild 1: Phasen eines Cyber-Angriffes [11, p. 2]

Bevor ein tatsächlicher Cyber-Angriff gestartet wird, steht fest, dass der Angreifer hier einerseits vorsätzlich vorgeht und andererseits unerlaubt mit einer bestimmten Absicht - hier Cyberangriff - handelt. Dies gilt nicht für sog. White-Hacker bzw. Penetrationstester, die im Auftrag einer Organisation agieren, um Schwachstellen aufzudecken. Zunächst wird - je nach Motivation - in der Initiierungsphase das Angriffsziel gewählt und „in diesem Zusammenhang auch die Angriffsreichweite“ [11, p. 2] festgelegt s. [11, p. 2]. Bei letzterem ist das Spektrum vom einzelnen System bis hin zu wenigen Zielen oder zu Flächenangriffen, in dem möglichst viele Systeme betroffen sind s. [11, p. 2]. In der nächsten - zweiten - Phase der Vorbereitung steht die Informationssammlung an, um möglichst viel über das Ziel zu erfahren. Danach wird - je nach Kapazität und Zeitaufwand - über die Art von Angriffswerkzeugen entschieden, wobei dasjenige Angriffswerkzeug gewählt

wird, welches die größten Chancen zum Angriff ermöglicht s. [11, p. 2]. Anschließend wird in diesem Zusammenhang nach Methoden gesucht, um den Angriff weitestgehend verschleiern zu können s. [11, p. 2]. In der letzten Phase steht die Durchführung an. Bei Erfolg des Angriffs wird zugleich versucht, die digitalen Einbruchsspuren zu minimieren bzw. zu beseitigen. Bei Fehlschlag wird nach neuen Wegen gesucht, um einen erfolgreichen Cyberangriff erreichen zu können s. [11, p. 2] .

Motivation von Angreifern

Die Motivation der Angreifer bleibt trotz der Vielzahl an unterschiedlichen Angriffszielen und - methoden meist auf fünf folgende Themen beschränkt:

1.„Finanzielle Interessen,
2. Informationsbeschaffung,
3. Sabotage,
4. Einflussnahme sowie
5. Durchsetzung politischer Interessen.“ [11, p. 4].

2.1 Rahmenbedingungen für Internetkriminalität

Die Rahmenbedingungen sind für Angreifer im digitalen Raum aus folgenden Gründen - auch zukünftig - vorteilhaft:

1. „Die Vernetzung von Informationstechnik macht Angriffe aus der Distanz von nahezu jedem Ort der Welt und zu jedem Zeitpunkt möglich. …
2. Das heutige offen gestaltete Internet bietet für Angreifer vielfältige Tarnungsmöglichkeiten, die das Entdeckungsrisiko minimieren.
3. Nicht abgesicherte Informationstechnik und speziell zugeschnittene Werkzeuge ermöglichen es, eine Vielzahl unterschiedlicher Ziele parallel anzugreifen.
4. Angriffswerkzeuge und -methoden sind einfach und kostengünstig verfügbar und beschaffbar. Neueste Erkenntnisse über Schwachstellen und Angriffsverfahren werden bereits nach kurzer Zeit für Cyber-Angriffe angewendet.
5. Erfolgreiche Angriffe auf den elektronischen Geschäftsverkehr ermöglichen große finanzielle Gewinne für Angreifer.
6. Der intensive Informationsaustausch über das Internet erleichtert den Zugriff auf schützenswerte Informationen.
7. Die Komplexität der Technik und/oder fehlendes Sicherheitsbewusstsein erhöhen in vielen Fällen die Erfolgsaussichten für Cyber-Angriffe.“ [11, p. 4].

2.2 Angreifer Typen

Es gibt verschiedene Arten von Angreifer Typen, die - alphabetisch geordnet - wie folgt beschrieben werden:

Cyber-Aktivisten: „Angreifer, die durch einen Cyber-Angriff auf einen politischen, gesellschaftlichen, sozialen, wirtschaftlichen oder technischen Missstand aufmerksam machen oder eine diesbezügliche Forderung durchsetzen wollen („Hacktivismus“). Die Motivation hinter dem Angriff ist Einflussnahme. Der durch einen Cyber-Angriff entstandene Schaden wird in Kauf genommen bzw. forciert, um eine höhere Aufmerksamkeit zu erlangen.“ [11, p. 4].
Ein Beispiel ist hier der Angriff der Gruppe „Anonleaks“ gegen eine Privatperson, hier Attila Hildmann s. [12]. Hier wurde der Hoster von Herrn Hildmann angegriffen und dabei wurde im Zuge des Angriffs festgestellt, dass offenbar Mindestmaßnahmen zur Informationssicherheit seitens des Hosters nicht eingehalten wurden, wie bspw. veraltete Joomla-Version, so dass die Angreifer daraus resultierend vollen Root-Zugriff auf alle IT-Systeme hatten s. [12].

Cyber-Kriminelle: „Die Motivation von Cyber-Kriminellen ist es, mithilfe der Informationstechnik auf illegalen Wegen Geld zu verdienen. Die Bandbreite reicht von organisierter Cyber-Kriminalität bis hin zu einfacher Kriminalität mit geringen Schäden“ [11, p. 4], wobei es zwei verschiedene Unterarten gibt:

1. Organisierte Cyber-Kriminalität: Diese „reicht vom Identitätsdiebstahl mit Warenbetrug über den Diebstahl von Geld durch Missbrauch von Bankdaten bis hin zur Erpressung. Organisierte Cyber-Kriminelle nutzen die genannten Vorteile von Cyber-Angriffen bei ihren Aktivitäten mit hoher Professionalität aus.“ [11, p. 4].
2. Einfache Cyber-Kriminelle: Es sind „meist Einzelpersonen oder kleine Gruppen, die sich durch geringere Professionalität in ihrem Handeln auszeichnen. Dementsprechend ist auch die Auswahl der Angriffsziele eingeschränkt und der verursachte Schaden typischerweise geringer.“ [11, p. 4].

Konkurrenzausspähung/Industriespionage im Cyberraum: „Durch die Vorteile des Internets ergeben sich für die Ausforschung eines Unternehmens durch Wettbewerber oder private Akteure neue Möglichkeiten. Konkurrenzausspähung dient finanziellen Interessen. Interne Informationen über Mitbewerber und deren Produkte bieten geldwerte Vorteile im globalen Wettbewerb.“ [11, p. 5].

Staatliche Nachrichtendienste im Cyber-Raum: „Cyber-Angriffe durch staatliche Nachrichtendienste sowie staatlich gelenkte Wirtschaftsspionage dienen … primär der Informationsbeschaffung und der Einflussnahme, auch um den eigenen nationalen Wirtschaftsunternehmen Vorteile auf den internationalen Märkten zu verschaffen.“ [11, p. 5].

Staatliche Akteure im Cyber-War: „Im militärischen Sektor wird der Cyber-Raum … als weitere wichtige Domäne neben den klassischen militärischen Domänen Land, See, Luft und Weltraum angesehen.“ [11, p. 5].

Cyber-Terroristen: „Terroristen können Cyber-Angriffe … nutzen, um unterschiedliche Ziele anzugreifen und somit ihre Ideologie zu verbreiten und ihren Einfluss auszuweiten.“ [11, p. 5].

Hobbyisten/Skript-Kiddies: „Die Gruppe der Hobbyisten und Skript-Kiddies führt Cyber-Angriffe aus Neugier durch, um ihre Fähigkeiten und ihr Wissen in der Praxis zu testen“ [11, p. 5] und „verfolgt keine finanziellen Interessen. Die Auswahl der Angriffsziele ist unspezifisch und vielfach allein vom Grad der Absicherung abhängig.“ [11, p. 5].

Innentäter: „Cyber-Angriffe durch Innentäter haben größere Aussicht auf Erfolg als Angriffe von außen, da der Angreifer bereits Zugang zu internen Ressourcen einer Organisation hat und so Schutzmaßnahmen und Schwachstellen über einen langen Zeitraum analysieren kann. Zusätzliche Vorteile genießen Innentäter durch das ihnen entgegengebrachte Vertrauen einer Organisation. Externe Dienstleister, die durch ihre Tätigkeit Einfluss oder direkten Zugang zur Organisation haben, werden hier ebenfalls zu den Innentätern gezählt.“ [11, p. 5]. Daher gehören Innentäter zu den gefährlichsten Angreifer Typen, da diese über einen längeren Zeitraum fast unbemerkt agieren können.

IT-Sicherheitsforscher: „IT-Sicherheitsforscher haben ein primär akademisches Interesse an der Aufdeckung von Risiken und der Durchführung von Cyber-Angriffen. Die unkoordinierte Veröffentlichung ihrer Ergebnisse („Full Disclosure”) kann reale Attacken anderer Angreifer zur Folge haben.“ [11, p. 5].

Für den Bürger zählen staatliche Angriffe - einschließlich Geheimdienste - sowie Angriffe von Innentätern von Organisationen - bei denen die Daten von Bürgern vorliegen - zu den gefährlichsten Angreifer Typen, da hier in der Regel so gut wie keine Schutzmaßnahmen - sei es technischer, personeller oder organisatorischer Art - wirken können. Denn bei diesen Angreifer Typen werden gezielt Schutzmaßnahmen umgangen, deren Angriff in der Regel vom Bürger selbst nicht festgestellt werden kann. Ursache hierfür, liegt u.a. daran, dass der Bürger einerseits in der Regel nicht über das Fachwissen verfügt und andererseits nicht über Kontrollmöglichkeiten in Form von Protokollierungen verfügt, da es sich meist außerhalb von dessen Einflussbereiches befindet, hier bspw. Netzprovider oder Serviceanbieter. Dies gilt auch für Angriffe am Endgerät - hier Smartphone -, wenn das Bundeskriminalamt (BKA) bspw. den modifizierten Staatstrojaner der israelischen Firma NSO einsetzt s. [13]. Bei den restlichen Angreifer-Typen können bereits ergriffene Schutzmaßnahmen die Erfolgswahrscheinlichkeit eines Angriffes minimieren.

2.2.1 Formen der Angriffsinitiierung

Je nach Angriffsziel werden dabei immer mindestens eines der drei Schutzwerte der Informationssicherheit verletzt, diese sind Vertraulichkeit, Integrität und/oder Verfügbarkeit. Folgende Absichten stehen hinter einem Angriff, die nach den Grundwerten zugeordnet sind.

Bei „Angriffe auf die Vertraulichkeit“ [11, p. 5] ist „z.B. das Ausspionieren vertraulicher Informationen“ [11, p. 5] mit folgenden Methoden möglich:

- „durch direktes Abhören (z. B. Kabel, Funk, Netze)
- durch Direktzugriff (z. B. Hotel, Zoll)
- durch Diebstahl
- durch Abfangen kompromittierender Abstrahlung
- durch Ausspähen/Passive Reconnaissance
- durch Wiederherstellung gelöschter Informationen
- durch Profiling/Überwachung“ [11, p. 6].

Bei „Angriffe auf die Integrität“ [11, p. 6] ist „z.B. die Manipulation“ [11, p. 6] möglich:

- „von Informationen
- von Speichermedien
- von IT-Diensten
- von Software
- von Kommunikationskanälen
- von Schnittstellen oder Zugängen
- von zentralen/dezentralen/externen Komponenten
- von Internet-Strukturen
- von Spezial-IT
- von Sicherheitskomponenten“ [11, p. 6].

Bei „Angriffe auf die Verfügbarkeit“ [11, p. 6] ist „z.B. das Sabotieren von Informationen oder IT-Diensten“ [11, p. 6] ist mit folgenden Methoden möglich:

- „durch Denial of Service-Angriffe
- durch physikalische Zerstörung
- durch Diebstahl“ [11, p. 6].

Dazu gehört auch je nach Angriffsziel die (Ruf-)Schädigung von Personen oder Institutionen sowie „als Spezialfall auch Angriffe auf die Authentizität, beispielsweise das Vortäuschen eines falschen Absenders“ [11, p. 6] wie es beispielsweise bei Phishing-Angriffen bei professionellen Angreifern der Fall ist s. [11, p. 6].

Dabei sind folgende Angriffsziele betroffen:

1. „Informationen
2. IT-Dienste
3. IT-Systeme“ [11, p. 6].

Zu Punkt 1. Informationen:

Informationen sind „ein vorrangiges Ziel von Cyber-Angriffen“ [11, p. 7]. Daher können sie „sowohl das eigentliche Ziel eines Angriffs darstellen, aber auch als Hilfsmittel zur Durchführung von weiteren Cyber-Angriffen genutzt werden.“ [11, p. 7]. Informationen im Sinne der IT-Technik sind immaterieller Natur, dennoch sind diese von hohem Wert und sind daher schützenswert s. [11, p. 7]. Die Bandbreite der Informationen ist wie folgt aufgeführt:

- „… Finanzdaten
- Bankdaten und Zahlungsinformationen
- Kunden- und Rechnungsdaten
- Dokumente
- Transaktionen
- Geistiges Eigentum
- Konfigurationsdaten
- Kommunikationsdaten
- Protokollierungsdaten
- Identitätsmerkmale/Credentials
- Kryptodaten/Schlüssel/Zertifikate
- Personenbezogene/biometrische Daten
- Verhaltens- und Standortdaten
- Metadaten
- …
- Informationen über IT-Infrastruktur und -Architektur“ [11, p. 7].

Informationen sind auf Datenspeicher enthalten, die es in unterschiedlicher Ausprägung und Form gibt [11, p. 7]. Daher sind diese auch Ziel von Cyber-Angriffen s. [11, p. 7]. Die Bandbreite von Datenspeichern ist wie folgt aufgeführt:

- „Datenbanken
- Dateien
- Stationäre Datenträger
- Mobile Datenträger
- Externe Datenspeicher/Cloud-Storage
- Hauptspeicher
- Zwischenspeicher (Caches)
- Cookies/Local Shared Objects
- Ausweise/Karten
- Verzeichnisse/Listen“ [11, p. 7].

Zu Punkt 2 IT-Dienste:

Ohne IT-Dienste würde das Internet nicht den gewohnten Leistungsumfang anbieten können wie beispielsweise den Domain Name Service (DNS) oder E-Shopping s. [11, p. 7]. Daher sind „Dienste ein exponiertes Angriffsziel“ [11, p. 7] und damit „auf vielfältige Weise und mit unterschiedlicher Motivation angreifbar.“ [11, p. 7]. Folgende IT-Dienste gibt es u.a.:

- „Elektronischer Geschäftsverkehr
- E-Government
- Web-Präsenzen/-Portale
- Web-Services
- Kommunikationsdienste
- Benutzerkonten
- Datei- und Verzeichnisdienste
- Synchronisationsdienste
- Infrastrukturdienste (z. B. DNS)
- Sicherheitsdienste (z. B. PKI)
- Authentisierungsdienste
- Administrationsdienste
- Protokollierungsdienste“ [11, p. 8].

Software

Die Software weist in der Regel Schwachstellen auf, daher sind diese bei Angreifern beliebt s. [11, p. 8]. Ziel des Angriffs auf Software sind entweder Störungen auszulösen oder das „System zu infiltrieren, um anschließend z.B. Informationen auszuspähen.“ [11, p. 8]. Der Einsatz von Software ist nahezu unbegrenzt, wie es die folgende Auflistung zeigt:

- „Lokale Anwendungen
- Benutzerschnittstellen/Browser/Plug-ins
- Client-Server-Anwendungen
- Internet-Anwendungen
- Mobile Anwendungen/Apps
- Aktive Inhalte
- Betriebssysteme
- Laufzeitumgebungen
- Software/Update Repositories
- Download-Plattformen/App-Stores
- Versionskontrollsysteme
- Quellcode
- Firmware
- Sicherheitssoftware“ [11, p. 8].

Kommunikationskanäle

Eine weitere Angriffsmöglichkeit sind Kommunikationskanäle. Darüber kann abgehört, manipuliert oder eine Störung ausgelöst werden, um „an die übertragenden Informationen zu gelangen oder die darüber abgewickelten Geschäftsprozesse zu beeinträchtigen.“ [11, p. 8], [11, p. 8]. Folgende Kommunikationskanäle gibt es:

- „E-Mail
- Instant Messaging
- Web-basierte Kommunikation
- (Mobile) Telefonie (auch VoIP)
- Kurzmitteilungen
- Videokonferenzen/Webmeetings
- …
- Soziale Netze und Foren“ [11, p. 8].

Schnittstellen und Zugänge

Des Weiteren gibt es Schnittstellen und Zugänge, die als „Einfallstor für Cyberangriffe“ [11, p. 9] dienen können s. [11, p. 9]. Ein Angriffsziel kann „die Verfügbarkeit der Zugänge“ [11, p. 9] sein, was zu einem Ausfall der Kommunikationsfähigkeit führen kann s. [11, p. 9]. Folgende Schnittstellen und Zugänge gibt es beispielsweise:

- „Provider-Anbindungen und Backbones
- Extranet-Anbindungen[2]
- Virtual Private Network-Anbindungen (VPN) und -Knoten
- Kunden-/Partner-/Dienstleister-Schnittstellen
- Fernzugänge
- Drahtlose Zugänge
- Kabel
- Übertragungsprotokolle
- Infrastrukturprotokolle
- Enterprise Service Bus
- Mobilfunk-Basisstationen“ [11, p. 9].

[2] Unter Extranet ist zu verstehen, dass es sich um eine „Erweiterung des Intranets einer Organisation, … um die gemeinsame Nutzung von Ressourcen zwischen der Organisation und anderen Organisationen und Personen, mit denen sie zu tun hat, einen begrenzten Zugang zu ihrem Intranet gewährt wird“ aus [389], Punkt 3.10.

Zentrale interne Komponenten

Sofern Schnittstellen und Zugänge überwunden sind, sind zentrale interne Komponenten einer Institution häufig Ziele eines Angriffs s. [11, p. 9]. Denn interne Komponenten „enthalten Daten oder stellen Dienste, die für die Funktionsfähigkeit … oft entscheidend sind.“ [11, p. 9]. Zu den zentralen internen Komponenten zählen beispielsweise:

- „Server
- Speichersysteme/Speichernetze
- Virtualisierungskomponenten
- Private Cloud-Komponenten
- Netzwerkkomponenten
- Sicherheitskomponenten
- Administrationskomponenten
- DMZ-Komponenten
- Proxies/Load Balancer
- Mobile Backend/Management“ [11, p. 9].

Dezentrale Komponenten

Bei Angriffen sind auch dezentrale Komponenten beliebt, da diese im Gegensatz zu den zentralen Komponenten in der Regel nicht das gleiche Schutzniveau vorweisen können s. [11, p. 9]. Hier ist die Manipulationsgefahr vor allem bei leicht zugänglichen Räumen am größten s. [11, p. 9]. Zu den dezentralen Komponenten gehören beispielsweise:

- „Stationäre Clients/Endgeräte
- Mobile Clients/Endgeräte, wie Smartphones oder Tablet-PCs
- Kiosk-Systeme
- Eingabegeräte (z. B. Maus, Tastatur, Lage- und Ortssensoren)
- Ausgabegeräte (z. B. Bildschirm, Drucker)“ [11, p. 9].

Externe Komponenten

Ein sehr hohes Risiko ist die Nutzung von externen Komponenten durch Auslagerung eigener Geschäftsprozesse an Drittparteien, da diese die Dienstleistung günstiger anbieten oder wenn das jeweilige Geschäftsprozess nicht selbst durch die Institution erbracht werden kann s. [11, p. 10]. Hier entstehen dadurch weitere Schnittstellen in Form von Einbindung von fremden Systemen an das eigene Netzwerk „oder dass Daten zur weiteren Verarbeitung das eigene Netzwerk verlassen.“ [11, p. 10]. Zu den externen Komponenten zählen u.a.:

- „IT von Partnern/Kunden/Dienstleistern
- Cloud Computing
- Private IT
- Gebäude und Räume

- Versorgungsnetze (insbesondere Energie)
- Klimatisierung
- Dienstleister (nicht IT-spezifisch)“ [11, p. 10].

Zu der o.g. Aufzählung ist auch die Schatten-IT zu zählen, die an das Netzwerk der jeweiligen Organisation eingebunden ist, ohne dass die entsprechende IT-Abteilung davon Kenntnis hat. Hierdurch kann es u.a. zu unbeabsichtigten Datenabflüssen kommen.

Internet-Strukturen

Eine der wichtigsten Ressourcen stellt das Internet mit seinen Basisdiensten dar, daher ist eine funktionsfähige Infrastruktur des Internets essenziell s. [11, p. 10]. Durch die zunehmende Vernetzung ist eine höhere Abhängigkeit gegeben, so dass durch Angriffe auf die Komponenten des Internets mit „massiven Auswirkungen“ [11, p. 10] zu rechnen ist s. [11, p. 10]. Folgende Internet Strukturen sind angreifbar:

- „Internet-Dienstleister
- Hosting-Provider
- Content Delivery Networks
- Internet-Kerninfrastruktur
- Routing-Strukturen
- Namensauflösung (DNS)
- Domain Registries
- TLS/SSL-Zertifizierungsstellen
- Suchmaschinen
- Zentrale Blacklists
- Soziale Netzwerke
- Cloud-Dienstleistungen
- Anonymisierungsdienste
- Öffentliche Internet-Zugänge“ [11, p. 10].

Spezial-IT

Zur Spezial-IT gehören alle Systeme, die nicht zur klassischen Büro-IT gehören s. [11, p. 10]. Diese haben in der Vergangenheit in der Regel Anforderungen der Informationssicherheit gar nicht oder kaum berücksichtigt, was durch die zunehmende Vernetzung mit dem Internet bzw. großen Netzen ein großer Vorteil für Angreifer ist s. [11, p. 10]. Zur Spezial-IT gehören u.a.:

- „Zutrittskontrollsysteme
- Videoüberwachungssysteme
- Prozesssteuerung, -automatisierung, -leittechnik
- Digitale Mess-/Steuerungs-/Regelsysteme
- Medizin-IT
- Automobil-IT

- Smart Grid/Smart Metering
- Positionierungsdienste
- Geldautomaten/Zahlungsterminals“ [11, p. 11].

Angriffsreichweite

Cyber-Angriffe lassen sich in Bezug auf ihre Reichweite unterscheiden:

- „Gezielte Angriffe auf ein Ziel oder wenige ausgesuchte Ziele
- Großflächiger Angriff auf möglichst viele beliebige Ziele gleichzeitig“ [11, p. 11].

Dabei steht „[d]ie Reichweite … in engem Zusammenhang mit Motiv, Absicht und Ziel des Angriffs“ [11, p. 11], wobei die Größe der Reichweite jeweils spezifische Vor- und Nachteile beinhaltet s. [11, p. 11]. Bspw. ist bei einem großflächigen Angriff die Erfolgswahrscheinlichkeit höher, andererseits fällt dieser Angriff eher auf s. [11, p. 11]. Darüber hinaus können „Schäden auch bei unbeteiligten Dritten entstehen, die durch Fehler oder Fehlfunktionen unbeabsichtigt Opfer eines Cyber-Angriffs werden (Begleitschaden)“ [11, p. 11].

2.2.2 Angriffsvorbereitung

Informationssammlung über Angriffsziele

Vor einem Angriff werden Informationen über das Ziel eingeholt, um die Erfolgswahrscheinlichkeit zu erhöhen s. [11, p. 12]. Typische Informationen zur Angriffsvorbereitung sind wie folgt:

- Identifikation möglicher Angriffspunkte
  - „Art der IT-Systeme und IT-Architektur
  - Netzwerk-Architektur und Schnittstellen
  - Betriebssysteme, Anwendungen und Patchlevel
  - IT-Sicherheitsmaßnahmen und eingesetzte IT-Sicherheitsprodukte
- Informationen über das Angriffsziel
  - „Informationen über Personen
  - Informationen über den organisatorischen Aufbau
  - Informationen über die Geschäftstätigkeit
- Abschätzung der Risiken eines Angriffs und Strategien zur Tarnung
- Abschätzung der Folgen eines Angriffs“ [11, p. 12].

Die folgenden Informationen werden über verschiedene Wege eingeholt, bspw.:

-Social Engineering
  - „Vortäuschen einer falschen Identität
  - Ausnutzen von Hilfsbereitschaft, Vertrauen oder Neugier
  - Ausnutzen von Angst, Autorität oder technischem Unverständnis

- Sammlung und Auswertung frei verfügbarer Informationen über das Ziel
  - „in Veröffentlichungen
  - über Web-Inhalte
  - in Sozialen Netzen
  - im Altpapier, Restmüll und anderen Abfällen einer Organisation
- Sammlung und Auswertung von Informationen über Systeme und Zugänge des Angriffsziels
  - „durch Network Mapping
  - durch Fingerprinting/Probing
  - Identifikation von Angriffspunkten“ [11, p. 12].

Gezielte Angriffe sind nur aufgrund der gesammelten Informationen möglich, was bei großflächigen Angriffen nicht der Fall ist, da „eher statistische Informationen im Vordergrund [stehen], beispielsweise über den Verbreitungsgrad einer bestimmten Software“ [11, p. 12], s. [11, p. 12].

Angriffswerkzeuge

Für Cyber-Angriffe stehen ein großes Spektrum an Hilfsmitteln und Werkzeugen zur Verfügung s. [11, p. 12]. Es „werden unterschiedliche Typen von Schadsoftware oder Exploits zur Ausnutzung von Software-Schwachstellen genutzt, um Zugriff auf ein System zu erlangen.“ [11, p. 12]. Dabei kann „nach Art des Angriffs … auch spezielle Hardware zum Einsatz kommen“ [11, p. 12]. Zu den einzelnen Schadsoftwarearten wird auf Kapitel 1.5 verwiesen.

Datenträger und Kanäle

Datenträger sowie Kommunikationskanäle können zu einem Angriffswerkswerkzeug umfunktioniert werden, sobald diese manipuliert worden sind oder Angriffstools enthalten s. [11, p. 14]. Folgende Komponenten eignen sich dafür:

- „Mobile Datenträger
- Mobile Endgeräte
- Private Endgeräte in der Organisation („Bring Your Own Device“)
- Webseiten (infiziert oder manipuliert/gefälscht)
- E-Mails (infiziert oder manipuliert/gefälscht)
- Chats, Kurzmitteilungen, Benachrichtigungen
- Datei- und Verzeichnisfreigaben
- Netzwerkprotokolle
- Unverschlüsselte Netzwerkverbindungen“ [11, p. 14].

Nach heutigem Stand können auch verschlüsselte Netzwerkverbindungen zum Angriff eignen, sofern diese Schwachstellen aufweisen, wie es zuletzt bei Heartbleed[3] der Fall war.

Software

Folgende Möglichkeiten zum Angriff mithilfe von Softwarefunktionalitäten sind möglich:

- „Aktive Inhalte
  Die Manipulation gegebener Aktiver Inhalte, wie beispielsweise JavaScript-Code, sind häufig Ausgangsbasis für Cross-Site-Scripting oder SQL-Injection-Angriffe.
- Administrationswerkzeuge
  Schlecht abgesicherte Administrationswerkzeuge, z. B. zur Fernwartung, erlauben Angreifern u. U. einen einfachen Zugriff auf Systeme.
- Sicherheits-/Hacking-Tools
  …
- Internet-Client-Software
  Browser oder andere Internet-Clients sind nicht nur Ziel von Cyber-Angriffen, sondern werden auch bei der Durchführung von Angriffen benutzt.
- Exploit
  Als Exploit bezeichnet man eine Methode oder einen Programmcode, mit dem über eine Schwachstelle in Hard- oder Software-Komponenten nicht vorgesehene Befehle oder Funktionen ausgeführt werden können.“ [11, p. 14].

Internet-Strukturen

Die Internet-Struktur spielt für Angriffe eine große Rolle. Daneben gibt es spezielle Internet-Dienste, die explizit nur „für die Durchführung von Cyber-Angriffen entwickelt worden“ [11, pp. 14-15] sind s. [11, pp. 14-15]. Folgende Komponenten können dafür genutzt werden:

- „Cloud-Dienstleistungen“ werden genutzt bspw. um Phishing-Seiten zu hosten oder DDoS-Angriffe durchzuführen.
- „Bulletproof-Hoster“ stellen „Webspace, IP-Adressen oder andere Ressourcen im Internet bereit“.
- Botnetze „werden für DDoS-Angriffe oder den Versand von Spam-Nachrichten verwendet“ sowie u.a. als Dropzone benutzt.
- Command & Control-Server
- Dropzones „sind Speicher im Internet, an die von Schadsoftware aufgezeichnete Daten automatisch übermittelt werden.“

[3] Heartbleed war eine Schwachstelle in der kryptografischen Software Bibliothek von OpenSSL gewesen, welches es jedem Angreifer ermöglichte, den Speicher vom System auszulesen, so dass unbefugt Daten ausgelesen werden konnten [388].

- Internet-Basisdienste werden genutzt bspw. „für DNS oder Routing“ [11, pp. 14-15].

Geräte

Der Einsatzweck eines Angriffs hängt von der „Methode und [des] Ziel[s]“ [11, p. 15] ab s. [11, p. 15]. Darunter können „vorhandene Geräte … zu einem Angriffswerkzeug“ [11, p. 15] umfunktioniert werden s. [11, p. 15]. Folgende Geräte können für Angriffe genutzt werden, was auch in Kombination möglich ist:

- „Standard-IT
- Mobiltelefone
- Wanzen
- Keylogger
- Mikrokameras
- IMSI-Catcher
- Messgeräte
- Störgeräte
- Lesegeräte
- Ausgesonderte und funktionsfähige Komponenten“ [11, p. 15].

Angriffsunterstützende Informationen

Ohne Informationen sind Angriffe schwieriger zu bewerkstelligen s. [11, p. 15]. Bspw. ermöglichen „[g]estohlene Identifikationsmerkmale … Zugriff auf Dienste und Dateien, Insider-Wissen … das Auffinden lohnender Ziele und die Durchführung von Angriffen.“ [11, p. 15]. Folgende Informationen sind hilfreich für Angreifer:

- „Gefälschte Identitätsmerkmale
- Gestohlene Identitätsmerkmale
- Gefälschte Kryptodaten
- Gestohlene Kryptodaten
- Schwachstellendatenbanken
- Insider-Wissen“ [11, p. 15].

Angriffstarnung

Damit der Angriff möglichst unbemerkt bleibt, was auch die Minimierung von digitalen Angriffsspuren miteinschließen kann, gibt es „verschiedene Methoden zur Tarnung.“ [11, p. 15].

Diese sind wie folgt aufgelistet:

- „Anonymisierungsdienste
- Fälschung von IP-Adressen, Absendern, etc.
- Nutzung mehrerer Zwischenstationen

- Tarnung auf dem Angriffsziel
- Abschalten vorhandener Sicherheitsmaßnahmen
- Protokollierung
- Missbrauch fremder Identitäten“ [11, pp. 15-16].

2.2.3 Angriffsdurchführung

Angriffsmethode

Angreifer haben - je nach Angriffsziel - eine Auswahl an unterschiedlichen Methoden zur Verfügung, die auch in Kombination eingesetzt werden kann s. [11, p. 17].

Denial of Service-Angriff

Denial of Service-Angriffe werden dazu benutzt, um „gegen die Verfügbarkeit … der … Dienste, einzelne Systeme oder ganze Netze zu stören oder vollständig betriebsunfähig zu machen. Wird ein Angriff mittels mehrerer Systeme parallel ausgeführt, spricht man von einem verteilten DoS, einem sogenannten Distributed Denial of Service-Angriff (DDoS). Angriffspunkte sind häufig Webserver, Mailserver, Applikationsserver oder darauf laufende Dienste.“ [11, p. 17]. Bei dieser Art von Angriffen gibt es diverse Methoden wie Überflutung, Störung, Abschaltung etc. s. [11, p. 17].

Schadsoftware-Infiltration

Je nach Angriffsziel kommen diverse Schadsoftwarearten in Betracht. Bei diesem Schritt liegt der Fokus „auf welchem Weg die Verteilung erfolgen soll“ [11, p. 18]. Folgende Möglichkeiten kommen in Betracht:

- gezielte Verteilung

„Für gezielte Angriffe werden häufig E-Mails mit Anhängen verwendet“ [11, p. 18].

- Massenverteilung

„Im Fall der Massenverteilung von Schadsoftware versuchen Angreifer z. B., hoch frequentierte Webseiten so anzugreifen, dass Besuchern der Webseite mittels Drive-by-Download Schadsoftware installiert wird“ [11, p. 18] oder über manipulierte E-Mails mit Schadcode im Anhang.

- Verteilung über Innentäter

Innentäter haben die größten Erfolgschancen zur Verteilung von Schadsoftware, da die Schutzmechanismen der Organisation i.d.R. nicht darauf ausgerichtet sind s. [11, p. 18].

Ergänzend nimmt aufgrund der hohen Verbreitung von Smartphones auch „die Verbreitung von Schadsoftware für unterschiedliche mobile Plattformen über Apps und App-Stores zu.“ [11, p. 18].

Identitätsdiebstahl

Ziel von Identitätsdiebstählen ist es, die Identität des Opfers zu erlangen, „um diese für eigene Zwecke“ [11, p. 18] zweckentfremden zu können, wovon die „Bandbreite der Nutzungsszenarien“ [11, p. 18] sehr breit ist. Das Motiv ist meist finanzieller Natur oder „dient der Diskreditierung einer Person.“ [11, p. 18]. Eine Auswahl an Möglichkeiten sind wie folgt aufgelistet:

Phishing

„Beim Phishing wird z. B. mittels gefälschter E-Mails und/oder Webseiten versucht, Zugangsdaten für einen Dienst oder eine Webseite zu erlangen. … Andere Varianten des Phishings setzen auf gefälschte Near Field Communication (NFC)-Tags oder Barcodes, die vom Opfer eingelesen werden und auf eine Phishing-Seite weiterleiten.“ [11, pp. 18-19].

Spear-Phishing/Whaling

Bei Spear-Phishing wird „nur ein kleiner Empfängerkreis … attackiert.“ [11, p. 19].

Maskerade

Maskerade ist das Vortäuschen einer falschen Identität, die in Zusammenhang mit Identitätsdiebstählen steht s. [11, p. 19].

Man-in-the-Middle-Angriffe

Beim Man-in-the-Middle-Angriff klingt sich der „Angreifer in die Kommunikation zwischen mindestens zwei Teilnehmern [ein], um Daten lesen oder manipulieren zu können.“ [11, p. 19].

Replay-Angriffe

„Replay-Angriffe beschreiben allgemein Angriffe, bei denen ein Informationsaustausch zuerst aufgezeichnet wird und die gewonnenen Informationen im Anschluss daran missbräuchlich wiederverwendet werden. Anhand eines aufgezeichneten Login-Vorgangs kann ein Angreifer … versuchen, sich selbst unberechtigt Zugang zu dem jeweiligen System zu verschaffen.“ [11, p. 19].

Nicknapping

„Als „Nicknapping“ bezeichnet man einen Cyber-Angriff, bei dem der Angreifer unter einem bekannten Namen oder Pseudonym auftritt … [um] … gegenüber Dritten den Eindruck zu erwecken, er sei der eigentliche/ursprüngliche Inhaber des Namens oder des Pseudonyms.“ [11, p. 19].

Domain-Hijacking

„Mittels Domain-Hijacking wird ein Domainname unerlaubt auf einen Dritten übertragen. Dieser kann dann über die Domain verfügen, beliebige Inhalte bereitstellen und so z. B. Zugriff auf Authentisierungsmerkmale erhalten.“ [11, p. 19].

Spoofing

„Der Begriff „Spoofing“ bedeutet allgemein die Verschleierung der eigenen Identität, was für Identitätsdiebstahl in vielfältiger Weise genutzt wird. Beim klassischen Phishing, Spear-Phishing oder Spam werden z. B. E-Mails mit gefälschten Absenderadressen verschickt. Webseiten, die für Phishing- oder Pharming-Angriffe genutzt werden, geben vor, die Webseite eines vertrauenswürdigen Anbieters zu sein.“ [11, p. 19].

Pharming

„[B]eim Pharming [wird] die Infrastruktur so manipuliert …, dass das Opfer auch dann auf einer gefälschten Webseite landet, wenn er die korrekte Adresse des Dienstes eingeben hat.“ [11, p. 19].

Brute-Force-Angriff

Ein Brute-Force-Angriff ist eine Angriffsmethode, mit dem ein Angreifer durch „wiederholtes Ausprobieren von Passwörtern (Brute-Force-Angriff) Zugang zu einem Benutzerkonto verschaffen.“ [11, p. 19].

Missbrauch voreingestellter, schwacher oder mehrfach verwendeter Passwörter

„Hard- und Software-Komponenten können im Auslieferungszustand öffentlich bekannte oder einfach ableitbare Standard-Passwörter beinhalten. Werden diese nicht geändert, erhalten Angreifer mit geringem Aufwand Zugriff darauf. Durch die Vielzahl unterschiedlicher Benutzerkonten ist es wahrscheinlich, dass ein Nutzer identische Passwörter bei unterschiedlichen Diensten nutzt. Kommt ein Angreifer in Besitz eines gültigen Passwortes, kann dieser probieren, ob damit weitere Accounts des Nutzers übernommen werden können.“ [11, p. 20].

Session-Hijacking/-Fixation

„Webapplikationen erkennen authentisierte Nutzer anhand von Session-IDs oder ähnlichen temporären Identifizierungsmerkmalen … Wenn ein Angreifer Zugriff auf diese Merkmale hat (Session-Hijacking) oder wenn er diese Merkmale von vornherein festlegen kann (Session-Fixation), hat er die gleichen Zugriffsrechte auf den Dienst wie der Benutzer der Zugangsdaten.“ [11, p. 20].

Diebstahl von Credentials

„Typische Beispiele für Credentials sind Passwörter, kryptografische Schlüssel und Zertifikate, sog. „Authentisierungs-Tickets“ oder auch „Session-Cookies“. Ein Diebstahl von Credentials kann z. B. Folge einer Attacke auf die Benutzerdatenbank von Webseiten oder Online-Diensten sein … [oder] auch durch Schadsoftware-Infektionen auf Clients mitgeschnitten und so unbefugt an Dritte übermittelt werden. Es können aber auch gezielt Geräte wie Smartphones, Hardware-Tokens oder mobile Datenträger gestohlen werden, wenn ein Angreifer Zugangsdaten auf diesen Komponenten vermutet.“ [11, p. 20].

Fälschung von Credentials

Bei einem erfolgreichen „Angriff auf eine Zertifizierungsstelle (Certificate Authority) kann … [e]in Angreifer … dadurch unter Umständen … gefälschte Zertifikate … erstellen und sie weitestgehend unbemerkt einzusetzen.“ [11, p. 20].

Skimming

Skimming ist „das unbemerkte Auslesen von Zahlungskarten (Bank- und Kreditkarten) durch physikalische Manipulation von Geldautomaten oder Zahlungsterminals. Mit den ausgelesenen Daten werden in der Folge Karten-Kopien erstellt. Um auf das Konto des Opfers zugreifen zu können, w[erden] meist … mithilfe einer kleinen, unauffälligen Kamera oder einer manipulierten Tastatur“ [11, p. 20] die Zugangsdaten erspäht.

Hacking

„Angreifer, die sich unbefugt Zugang zu Systemen oder Netzen verschaffen“ [11, p. 20] werden als Hacker bezeichnet. Folgende Angriffsmethoden stehen dabei zur Verfügung:

Fuzzing

„Fuzzing ist eine automatisierte Testmethode für Software, bei der ein Programm eine Vielzahl automatisch generierter Eingabedaten verarbeiten muss, ohne dabei eine Fehlfunktion zu zeigen. Findet ein Hacker durch Fuzzing ein Eingabemuster, das eine Fehlfunktion erzeugt, muss überprüft werden, ob sich der gefundene Fehler als Sicherheitslücke ausnutzen lässt.“ [11, p. 20].

Injection-Angriffe

„Viele Applikationen sind für Injection-Angriffe anfällig, wenn Benutzereingaben nicht ausreichend gefiltert werden. Eine SQL-Injection-Schwachstelle gibt einem Angreifer die Möglichkeit, Datenbankabfragen über eine Applikation so zu manipulieren, dass der für den Angreifer interessante Teil einer Datenbank zurückgegeben wird, anstatt des Teils, der ursprünglich für die Anwendung vorgesehen ist.“ [11, p. 20].

Cross-Site-Scripting (XSS)

„Cross-Site-Scripting-Schwachstellen entstehen, wenn Benutzereingaben in einer Webanwendung ungefiltert durch den Server verarbeitet und an andere Clients zurückgegeben werden. Ein Angreifer hat damit unter Umständen die Möglichkeit, Programmcode wie JavaScript im Kontext des Benutzers einer Webseite auszuführen.“ [11, p. 20].

Cross-Site-Request-Forgery (CSRF)

„Cross-Site-Request-Forgery ist eine weitere Angriffsform, die sich gegen Benutzer von Webanwendungen richtet. Mit dieser Vorgehensweise lassen sich Funktionen einer Webanwendung von einem Angreifer im Namen des Opfers nutzen. Ein Beispiel ist die Versendung einer gefälschten Statusnachricht in einem Sozialen Netzwerk: Ein Angreifer formuliert die Nachricht und schiebt sie dem Opfer beim Abruf einer Webseite unter.“ [11, pp. 20-21].

Poisoning

Poisoning ist „das Einschleusen von manipulierten Daten in einen Zwischenspeicher (Cache), der dann von anderen Anwendungen oder Diensten genutzt wird. Beispiele sind Angriffe mittels Poisoning auf DNS-…Caches. Ein Angreifer kann so z. B. allgemein die Routen von Datenpaketen ändern oder gezielt Anfragen für Webseiten einer Bank auf eine gefälschte Seite umleiten.“ [11, p. 21].

Reverse Engineering

Mittels Reverse Engineering analysiert „die Funktionsweise einer kompilierten Software …, ohne dabei auf den Quelltext oder die Spezifikation der Software zugreifen zu müssen. Als Vorbereitung eines Cyber-Angriffs können z. B. Sicherheits-Updates mittels Reverse Engineering untersucht werden, um Erkenntnisse über Sicherheitslücken zu sammeln, die durch das Update geschlossen werden.“ [11, p. 21].

Missbrauch von Passwort-Zurücksetzen-Funktionen

„Anwendungen und Dienste bieten Nutzern häufig die Möglichkeit, ihr Passwort selbstständig zurückzusetzen, falls der Benutzer sein Passwort vergessen hat. Dabei werden häufig Informationen aus dem persönlichen Umfeld des Benutzers abgefragt“ [11, p. 21].

Ausnutzen von Fehlkonfigurationen

Bei „Einsatz von IT in vielen unterschiedlichen Bereichen … kann es schnell zu Fehlkonfigurationen kommen, die ein System für Cyber-Angriffe anfällig machen.“ [11, p. 21].

Ausnutzen von Schwachstellen oder Implementierungsfehlern

„Implementierungsfehler und Schwachstellen können in jeder Software enthalten sein und unter Umständen als Einfallstor für Cyber-Angriffe dienen. Schwachstellen in Webbrowsern und Browser-Plugins werden z. B. häufig mittels Drive-by-Downloads zur Installation von Schadsoftware ausgenutzt. Schwachstellen im Betriebssystem selbst können in vielen Fällen dazu verwendet werden, die eigenen Benutzerrechte auszuweiten oder das System zum Absturz zu bringen.“ [11, p. 21].

Ausnutzen von Design-Fehlern

„Schwachstellen durch Design-Fehler haben ihren Ursprung in fehlerhaften oder unvollständigen Spezifikationen von Anwendungen und Protokollen. … Konkrete Beispiele sind Angriffe auf Signaturverfahren, in denen Teile der signierten Daten ausgetauscht werden können, ohne die Signatur ungültig werden zu lassen (XML Signature Wrapping) oder die im Portable Document Standard (PDF) vorgesehene Möglichkeit, Programmcode außerhalb des Dokuments zu starten.“ [11, p. 21].

Menschliche und soziale Faktoren

Erfolgreiche Angriffe laufen fast immer unter Zuhilfenahme vom Faktor Mensch, da dieser das jeweilige IT-System bedient und bei Erfolg darüber die weiteren Angriffe laufen s. [11, p. 21]. Daher werden folgende Risiken aufgezeigt, die den Faktor Mensch betreffen:

Diskreditierung/Rufschädigung

„Gelingt es einem Angreifer, interne bzw. vertrauliche Informationen zu veröffentlichen oder falsche Informationen in Umlauf zu bringen, kann damit die Integrität und das Ansehen von Personen oder Institutionen in der Öffentlichkeit beeinflusst werden. Eine Verunstaltung einer Webseite (Defacement) schadet dem Ansehen einer Organisation.“ [11, p. 21].

Ablenkungsmanöver

„Ablenkungsmanöver können Cyber-Angriffe flankieren und die Wahrscheinlichkeit für einen Erfolg erhöhen. Beispielsweise könnte ein Angreifer einen DDoS-Angriff als Ablenkungsmanöver starten, um Ressourcen aufseiten des Angriffsziels zu binden. An anderer Stelle könnte dann parallel versucht werden, in das Netzwerk einzudringen.“ [11, p. 21].

Irreführung

„Durch Verbreitung von falschen Informationen können Entscheidungen auf der Seite der Empfänger beeinflusst und so gezielt Fehlentscheidungen verursacht werden.“ [11, p. 22].

Erpressung/Nötigung/Korruption

Dazu gehören u.a. „Drohungen und Einschüchterungen per E-Mail, Erpressung zum Schutz vor DDoS-Angriffen sowie die Forderung von Lösegeld für Daten nach erfolgreicher Platzierung von Ransomware. Nach einem erfolgreichen Datendiebstahl kann das Opfer zusätzlich erpresst werden, indem mit einer Veröffentlichung von Daten oder Informationen über Sicherheitslücken gedroht wird.“ [11, p. 22].

Angriffspunkte

IT-Komponenten, die über die Netze - einschließlich des Internets - zu erreichen sind, gelten als „primäre Angriffspunkte“ [11, p. 22], s. [11, p. 22]. „Je größer diese exponierte Angriffsfläche ist“ [11, p. 22], desto einfacher ist es die einzelnen „Angriffspunkte zu identifizieren“ [11, p. 22], um anschließend einen Angriff durchzuführen s. [11, p. 22].

Folgende Angriffsmöglichkeiten können dabei genutzt werden:

Anwendungen mit Internetzugang: „Browser, E-Mail-Programme, mobile Endgeräte, usw. sind Angriffspunkte für die über sie verarbeiteten Informationen.“ [11, p. 22].

Server: „Webserver, Kommunikationsserver, Firewalls, Remote-Wartungszugänge, usw. sind Angriffspunkte für Daten, die durch sie verarbeitet, übertragen oder geschützt werden.“ [11, p. 22].

Schnittstellen und Zugänge: „...sind Angriffspunkte, um Zugriff auf dahinterliegende Systeme und Netze zu erhalten oder diese zu stören.“ [11, p. 22].

Dienste: „...sind Angriffspunkte, um die durch sie bereitgestellte Funktion zu stören, zu manipulieren oder um Identitäten innerhalb des Dienstes zu missbrauchen.“ [11, p. 22].

Spurenbeseitigung

Um das Entdeckungsrisiko eines Angriffes zu minimieren, wird von vornherein versucht, möglichst „keine Spuren zu erzeugen … oder die Spuren des Angriffs im Nachhinein zu beseitigen.“ [11, p. 22]. Dabei gibt es folgende Methoden, die auch in Kombination genutzt werden können:

„Löschen oder Verbergen der auf dem Angriffspunkt genutzten Software, wie Hacking-Tools oder Schadsoftware. Löschen oder Verbergen der Spuren in Logdateien und Protokollen, mittels derer ein Cyber-Angriff im Nachhinein entdeckt werden könnte. … Löschen oder Verbergen von Dropzones, Command & Control-Servern und ähnlicher Infrastrukturen, die den Angreifern während des Angriffs als Hilfsmittel dienten.“ [11, p. 22].

Prävention ist auf der einen Seite wichtig, aber auch Maßnahmen für den Ernstfall sind zu treffen. Welche Handlungsschritte müssen folgen, wenn bspw. ein Identitätsdiebstahl stattfand etc..

2.2.4 Zwischenfazit

Diese kurze, nicht abschließende Übersicht zeigt exemplarisch auf, dass es de facto unbegrenzte Angriffsmöglichkeiten gibt. Daher muss der Bürger nicht nur seine eigenen IT-Systeme umfassend schützen, sondern auch Organisationen - dessen (Online-)Dienste der Bürger in Anspruch nimmt - müssen ebenso Schutzvorkehrungen treffen, sonst ist die Informationssicherheit gefährdet, wenn ein Teil seinen Betrag nicht oder nur zum Teil leistet. Zudem liegt prinzipiell ein Ungleichgewicht vor. Während Angreifer nur eine einzige Schwachstelle finden müssen, um an das Ziel zu gelangen, muss der Bürger sowie die genutzten Onlinedienste einer Organisation alle Schutzmaßnahmen gleichzeitig im Blick haben, sonst ist die Informationssicherheit gefährdet. Zudem greifen beim Bürger die Schutzmaßnahmen nicht bei staatlichen Angreifern einschließlich Geheimdiensten, da diese prinzipiell über unbegrenzte Ressourcen verfügen, sei es technischer oder personeller Natur.

3. Aufstellung von Gefährdungen und Risiken bei Nutzung von IT-Systemen

3.1 Technische Risiken und Schwachstellen bei Nutzung von IT-Systemen

Es folgen ausgewählte Fallbeispiele von wesentlichen technischen Risiken und Schwachstellen bei Nutzung von IT-Systemen. Hinsichtlich des Begriffes Risiko im jeweiligen Titel bei den Aufzählungen in den Kapiteln 3.1 und 3.3 handelt es hier nur um eine allgemeine Einordnung, eine detailliertere Betrachtung erfolgt im jeweiligen Abschnitt. Aufgrund der Vielzahl an Risiken und Schwachstellen sowie der zunehmenden Vernetzung der IT-Systeme untereinander und der daraus erhöhten Komplexität ist eine abschließende Aufzählung nicht möglich.

3.1.1 Bedrohungen durch Hardware- und hardwarenahe Trojaner

Im einleitenden Bericht des Fraunhofer-Instituts für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) steht, dass Hardware- und hardwarenahe Trojaner „nicht nur ein akademisches Forschungsfeld, sondern … seit Jahren [auch] im produktiven Einsatz bei Geheimdiensten“ [14, p. 12] sind s. [14, p. 12]. Inzwischen sind „Hardware- und hardwarenahe Trojaner günstig zu beschaffen bzw. einfach zu implementieren.“ [14, p. 12], wie es für Hardware-Keylogger auf einem Geldautomaten bereits erfolgreich umgesetzt wurde s. [14, p. 12]. Hardware- bzw. hardwarenahe Trojaner ermöglichen es, dass „fast jedes elektronische Gerät [dafür] anfällig“ [14, p. 12] ist. Dies gilt auch für lebenswichtige Bereiche wie der Gesundheitssektor oder die Wasserversorgung, so dass beim Gebrauch dieser Bedrohungsart „weitreichende Folgen im privaten Leben, der Wirtschaft und der Landessicherheit“ [14, p. 12] entstehen können s. [14, p. 12]. Gegen diese Bedrohung können herkömmliche Schutzmöglichkeiten wie „Intrusion Detection Systeme (IDS), Firewalls und Virenscanner“ [14, p. 12] wenig bis gar nichts ausrichten, so dass es vor diesem Hintergrund „als eine der größten Bedrohung dieses Jahrzehnts“ [14, p. 12] angesehen wird. Denn „mögliche Schutztechniken … [sind] wenig verbreitet und zudem [bieten diese] in vielen Fällen keinen umfassenden Schutz“ [14, p. 12]. Hardware- bzw. hardwarenahe Trojaner hebeln alle Schutzziele wie Vertraulichkeit, Integrität und Verfügbarkeit aus s. [14, p. 15]. Es gibt drei Arten von Hardware- bzw. hardwarenahen Trojanern - 1. Firmware Trojaner, 2. Malicious Hardware, 3. Integrated Circuit Trojaner -. Folgende fünf Verbreitungswege von Trojanern gibt es: 1. Entwicklungs-/Designphase, 2. Produktionsphase, 3. Transportweg, 4. Remote Infektion, 5. Vor Ort s. [14, p. 15].

Nachfolgend werden exemplarische Anwendungsbeispiele von Trojanern aufgezeigt.

Angriffsmöglichkeit Firewall

Selbst Sicherheitsprodukte, die Nutzer vor unbefugten Zugriffen schützen sollen, sind betroffen, was besonders u.a. für Firewalls gilt. Hier können Firewalls „als Brückenköpfe

und für Man-in-the-Middle-Angriffe“ [14, p. 30] sowie für „nicht autorisierte Kommunikation … zwischen den (Sub-)Netzen [genutzt]“ [14, p. 30] werden. Man-in-the-Middle-Angriffe kann von der Firewall „nicht erkannt werden“ [14, p. 30]. Die NSA hat laut NSA Advanced Network Technology (ANT) Katalog „mindestens fünf Produkte, die auf Firewalls abzielen“ [14, p. 30]. Bspw. stellt Halluxwater „einen persistenten Remote Zugang zur Firewall her, der zur Datenexfiltration gedacht ist.“ [14, p. 30]. Hier sind in der Vergangenheit öfter US-amerikanische Hersteller von Sicherheitsprodukten dadurch aufgefallen, dass mehrfach Hintertüren aufgefunden wurden, wie es u.a. bei der Firma Cisco sowie der Firma Juniper der Fall ist s. [14, p. 30], s. [15]. Beim „Netzwerkausrüster Juniper [wurden] offensichtlich absichtlich eingebaute Hintertüren im Source-Code seines hauseigenen Betriebssystems ScreenOS“ [14, p. 30] gefunden, was bei Sicherheitsprodukten besonders kritisch zu betrachten ist. Denn hier ist sowohl die Organisation als auch der Nutzer darauf angewiesen, dass Sicherheitsprodukte genau die Funktion ausführen sollen, wofür diese beschafft worden sind.

Home Entertainment

Zum Home Entertainment gehören u.a. Fernseher, Set-Top-Boxen sowie Spielekonsolen [14, p. 33]. Sofern diese einen Netzwerkanschluss aufweisen „können [diese] als Brückenkopf genutzt werden.“ [14, p. 33]. Als Beispiel kann auf die „Vault 7 Leaks“ [14, p. 33] verwiesen werden, in der „die CIA [Central Intelligence Agency] und der MI5 [Military Intelligence, Section 5] über ein Implant für Samsung Smart-TVs verfügen, das den Fernseher zur Audio- und Video-Wanze umfunktioniert[e]“ [14, p. 33].

Smart Home / Gebäudetechnik

Smart Home / Gebäudetechnik sind bspw. fernsteuerbare Steckdosen, Lampen, Heizungen einschließlich Fenster- und Türöffner, deren Gemeinsamkeit das Vorhandensein einer Netzwerkschnittstelle ist s. [14, p. 35]. Zu den gefährlichsten Gefahren gehören manipulierte Heizungen, die „potentiell zur Explosion gebracht werden und somit direkt das Leben von Menschen gefährden“ [14, p. 35]. Als weiteres Beispiel sei das „Mirai Botnet“ genannt, die sich „nicht nur auf Routern und Gateways, sondern auch auf IP-Kameras und Video-Rekordern“ [14, p. 35] verbreiten konnte. Ebenfalls großflächig ging mutmaßlich die NSA vor, in dem diese „Backdoors ab Werk in die Überwachungssysteme der Firma NetBotz (heute: Schneider Electric) eingebaut hat“ [14, p. 35].

Medizintechnik

Mittlerweise werden im Medizinbereich „Embedded Devices eingesetzt“ [14, p. 36]. Dazu gehören u.a. Zuckermessgeräte, diverse Monitoring-Systeme, Infusionspumpen, Ultraschall- oder Röntgengeräte s. [14, p. 36]. Hier stehen zwei Angriffsoptionen zur Verfügung, einerseits Manipulation oder unbefugte Nutzung von Patientendaten, anderseits die direkte Schädigung des Patienten s. [14, p. 36]. Ein Beispiel ist die Manipulation an einer Infusionspumpe, so dass „[e]ine permanente Schädigung oder gar der Tod des Patienten … nicht auszuschließen“ [14, p. 36] sind.

Fahrzeugtechnik

Gegenwärtig befinden sich in Fahrzeugen „oft mehr als 50 Embedded Devices, die über einen Can-Bus [Controller Area Network] verbunden sind“ [14, p. 37]. Dabei ist die größte Bedrohung „der Zugang zum Can-Bus“ [14, p. 37], da ein unbefugter Zugriff „darauf genutzt werden kann, um die Bremsen auszulösen oder den Motor zu stoppen“ [14, p. 37], was u.U. tödlich enden kann. Zudem „können Freisprecheinrichtungen [dazu] genutzt werden, um Gespräche im Fahrzeuginnenraum aufzuzeichnen.“ [14, p. 37]. Desweiteren ist ein Tracking mithilfe des Globalen Positionsbestimmungssystems (GPS) des Navigationssystems möglich s. [14, p. 37].

Firmware Rootkits

Firmware Rootkits sind für jedes IT-System eine erhebliche Bedrohung, „da diese in der Lage sind, am Betriebssystem vorbei Daten zu manipulieren, abzugreifen und sie im Rahmen der Möglichkeiten der befallenden Komponente sogar auszuleiten.“ [14, p. 41]. Aus diesem Grund kann es selbst mit Hilfe von technischen Mitteln auf dem Host fast nicht erkannt werden s. [14, p. 41].

BIOS / UEFI

Das Basic Input Output System (BIOS) und das Unified Extensible Firmware Interface (UEFI) „bieten vielfältige Angriffsmöglichkeiten“ [14, p. 42], s. [14, p. 42]. Das BIOS wird dafür genutzt, „um Malware insbesondere in den Bootsektoren der Festplatten zu persistieren“ [14, p. 42]. Bei UEFI gibt es viel mehr Möglichkeiten, da diese auch „Treiber für diverse Dateisysteme, Human Interface Devices (HID) … und auch für Netzwerkkarten mit.“ [14, p. 42]. Daher kann es „hervorragend für Remote-Zugänge mit umfangreichen Funktionen“ [14, p. 42] genutzt werden, um bspw. „mittels der vorhandenen Treiber eine akustische Raumüberwachung“ [14, p. 42] zu ermöglichen. Selbst besonders gesicherte Systeme, wie „Live-Linux-Systeme, die Read-Only von CD booten, [lassen sich] ausspionieren.“ [14, p. 42]. Diese Art von Trojanern ist besonders für Geheimdienste attraktiv, weil es für die o.g. Angriffsvektoren „im Moment keine Erkennungsmethoden“ [14, p. 42] gibt - außer über den nicht normalen Netzwerkverkehr, der „potentiell von IDS erkannt werden kann“ [14, p. 42] -. Allein der NSA ANT Katalog bot zum damaligen Zeitpunkt mindestens drei folgende Produkte an, um Malware im BIOS zu persistieren, die teilweise Backdoor Funktionalitäten aufwiesen s. [14, pp. 42-43].

Management Engine / Systeme Management Unit

Die Intel Management Engine (ME) und das AMD System Management Unit (SMU) können für Direct Memory Access (DMA) „Angriffe genutzt werden“ [14, p. 44], s. [14, p. 44]. Bei dieser Angriffsart ist es möglich, dass „[g]estohlene Daten … am Betriebssystem vorbei direkt über die Netzwerkkarte gesendet werden“ [14, p. 44] kann. Bislang gibt es keine Erkennungsmethoden gegen diese Art von Angriffen s. [14, p. 44].

Zusammenfassend ist festzustellen, dass Firmware-Trojaner „leicht zu implementieren und sehr einfach zu verbreiten“ [14, p. 50] sind, welches vielfältige Funktionsmöglichkeiten beinhalten kann s. [14, p. 50]. Auch „vermeintlich sichere Verfahren, wie z.B. Signaturen … [können] umgangen werden“ [14, p. 50]. Erschwerend kommt hinzu, dass „weder vom Einkäufer noch vom Nutzer feststellbar [ist], ob und welche proaktiven Sicherheitsmaßnahmen von den Herstellern zum Schutz der Firmware getroffen wurden.“ [14, p. 50]. Das gilt auch für mögliche Angriffe in Form von manipulierten Firmware-Updates s. [14, p. 50]. Dass dies kein Einzelfall ist, zeigen die „weit verbreiteten Botnetze auf Embedded Devices“ [14, p. 50] auf, in der „Firmware-Trojaner bereits im Malware-Massenmarkt angekommen sind“ [14, p. 50]. Zum oben genannten Bericht des Forschungsteam erschien ein Artikel darüber, in dem „diese Gefahr [der Hardwaretrojaner] von vielen IT-Verantwortlichen und Entscheidern in Unternehmen entweder nicht wahrgenommen oder zumindest unterschätzt.“ [16] wird. Denn „[d]ie wachsende Verbreitung von Hardware- und hardwarenahen Trojanern erklären sich die FKIE-Forscher damit, dass diese Bedrohungslage bislang relativ vernachlässigt wurde - sowohl von den Geräteherstellern wie auch den Nutzern“ [16].

3.1.2 Schwachstellen in der Central Processing Unit-Architektur (CPU)

Mit Meltdown und Spectre ist ein neuer Bereich von Mikroarchitektur entstanden s. [17]. Während bei diesen Seitenkanalangriffen nur Metadaten geleakt worden sind, ist es jetzt möglich durch Angriffe auf die transiente Ausführung tatsächliche Daten einzusehen s. [17]. Sie sind „das Ergebnis falscher Vorhersagen von Kontroll- und Datenflüssen wie die außerordentliche Ausführung nach Ausnahmen.“ [17].

3.1.3 Schwachstellen bei Software-Produkten

Bei Schwachstellen in Software-Produkten konstatiert das BSI, dass die Software „immer komplexer geworden“ [18, p. 22] ist, so dass „eine Prüfung aller Eventualitäten, mit denen ein Software-Produkt konfrontiert werden könnte, momentan faktisch unmöglich“ [18, p. 22] ist. Daher können Software-Produkte „unerkannte Fehler oder ungewünschte Fehlfunktionen“ [18, p. 22] enthalten, so dass diese „von unbefugten Dritten ausgenutzt werden können, um schädliche Operationen auf einem Computersystem auszuführen“ [18, p. 22]. „Die Kritikalität einer Schwachstelle ergibt sich … aus drei Aspekten: der Relevanz des betroffenen Software-Produkts für Anwenderinnen und Anwender, dem Aufwand oder den Voraussetzungen zur erfolgreichen Ausnutzung der Schwachstelle sowie den möglichen Auswirkungen auf die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit.“ [18, p. 23]. Daher ist „[d]er Umgang mit Schwachstellen in Software-Produkten … ein wesentlicher Faktor für die sichere Digitalisierung in Deutschland.“ [18, p. 23]. Hier appelliert das BSI an die Eigenverantwortung der Nutzer, wozu „das Einspielen von Aktualisierungen und das Reagieren auf Herstellerhinweise, falls noch kein Patch zur Verfügung steht.“ [18, p. 23] zählt. Besonders kritisch sieht das BSI, dass selbst bei kritischen Schwachstellen die „zur Verfügung stehende[n] Aktualisierungen verzögert oder

gar nicht eingespielt werden.“ [18, p. 23]. Auch war im Berichtszeitraum das Remote Desktop Protocol (RDP), ein Fernwartungsdienst der Firma Microsoft, von mehreren Schwachstellen betroffen gewesen s. [18, p. 25]. Sowohl die Schwachstelle BlueKeep als auch DejaBlue ermöglichten Angreifern aus der Ferne „beliebige Programme - auch Schadprogramme - auf dem angreifenden System auszuführen“ [18, p. 25], wobei letztere dies sogar „ohne Authentifizierung oder Interaktion eines Nutzers“ [18, p. 25] möglich war s. [18, p. 25].

3.1.4 Schwachstellen in Hardware-Produkten

Angriffen auf Hardware-Produkte setzt Spezialwissen und entsprechendes Equipment voraus, da diese „in der Regel sehr tief in der jeweiligen Architektur oder dem organisatorischen Prozess ansetzten, wie etwa an der Physik von Transistoren … oder auch den Schritten Produktion und Lieferkette“ [18, p. 26]. Erfolgreich ist der Angriff dann, wenn die Hardware entweder kompromittiert ist oder „darin enthaltende Schwächen ein hinreichend großes Einfallstor“ [18, p. 26] aufweist. Der erhebliche Vorteil bei Hardware-Angriffen Angreifer ggü. der Softwareebene ist die Tatsache, dass jede „aufsetzende Sicherheitsmechanismen grundsätzlich ihre Wirkung“ [18, p. 26] verlieren s. [18, p. 26].

Als Beispiel für erfolgreiche Angriffe auf Hardware-Ebene sind Authentisierungstoken sowie aufgefundene Schwachstellen in SmartCards. Daher empfiehlt das BSI zukünftig SmartCards einzusetzen, die auf den „Verschlüsselungsstandard (Advanced Encryption Standard, AES)“ [18, p. 27] aufbauen s. [18, p. 27].

3.1.5 Risiken bei Nutzung von Kryptographie

Ohne kryptografische Mechanismen würden viele IT-Sicherheitsfunktionen nicht sicher betrieben werden können s. [18, p. 30]. Folgende Szenarien würden das Kryptosystem schwächen bzw. unterlaufen: „Schwächen in kryptografischen Mechanismen …, Implementierungsfehler, [u]nzureichend abgesicherte Seitenkanäle, Hardware-Schwachstellen …, Schwache Zufallszahlen, die zu vorhersagbaren und damit weniger sicheren kryptografischen Schlüsseln führen können.“ [18, p. 30].

Zur o.g. Aufzählung gehört seit kurzem die Künstliche Intelligenz (KI) dazu. Die KI wird für die „Analyse auf Anfälligkeit für *Seitenkanalangriffe*, und als Werkzeug in der mathematischen Kryptoanalyse“ [18, p. 31] genutzt. Wenn in der Zukunft ein „leistungsstarker Quantencomputer zur Verfügung steh[en]“ [18, p. 31] würde, gelten “[d]ie Sicherheitsgarantien der heute eingesetzten kryptografischen Mechanismen … [dann] nicht mehr“ [18, p. 31].

3.1.6 Risiko Router

Ein sicherer und damit vertrauenswürdiger Router ist entscheidend, da dieser einerseits den Zugriff auf das interne Netz schützt und andererseits die Kommunikation über das

Internet sicherstellt. Falls der Router eine Schwachstelle aufweist, sind schnell die Grundwerte der Vertraulichkeit, Integrität und Verfügbarkeit hinsichtlich der darüber ausgetauschten Informationen betroffen. Hier reicht nur eine einzige Sicherheitslücke aus, um das gesamte System einschließlich der Nutzung von VPN zu gefährden. Router zählen zu den sog. „Embedded Devices“, in der der Router-Hersteller das Betriebssystem und die darauf lauffähige Software meist nicht selbst entwickeln und daher bestehen diese in der Regel aus zugekauften Standardsoftwarekomponenten s. [18, p. 26]. Dies hat den erheblichen Nachteil, dass „Malware und Exploits für Embedded Devices oft ohne große Anpassungen auf einer ganzen Reihe von teilweise sogar unterschiedlichen Geräteklassen lauffähig sind.“ [18, p. 26]. Daher kann im Falle von „Abgreifen und Manipulieren von Daten auf dem Router … selbst … mit lokalen Maßnahmen, wie z.B. IDS, weder detektier[t] noch verhinder[t]“ [18, p. 27] werden. „Dies gilt auch für Angriffe, die durch den Router auf andere Ziele im Internet durchgeführt werden.“ [18, p. 27], wie es bspw. bei Bot-Netzen, die aus Home-Routern bestanden, der Fall war s. [18, p. 27]. Die NSA hatte selbst „mindestens vier Produkte im NSA ANT Katalog, die auf Router abzielen:“ [18, p. 27]. Die eben genannten Ausführungen sind keine Einzelfälle, sondern kommen auch in modernen Routern immer wieder vor bspw. „in LTE-Routern von Quanta [in der] gleich mehrere Backdoors vorhanden sind.“ [18, p. 28] und das „[p]erfide ist, dass Quanta auch Geräte für anderer Hersteller produziert, die ähnliche Backdoors enthalten.“ [18, p. 28].

Wie verwundbar Router sind, zeigt zuletzt ein Report des Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) auf, in dem „bei fast allen Geräten von insgesamt 127 getesteten Routern für Privatnutzer von sieben großen Herstellern … Sicherheitsmängel festgestellt [wurden], teilweise sogar ganz erhebliche.“ [19]. Weiter heißt es im Pressebericht „Die Auswertung hat ergeben, dass kein einziger Router ohne Fehler war. Manche waren sogar von Hunderten bekannter Schwachstellen betroffen“ [19], davon hatten „46 Router … in den letzten zwölf Monaten kein Sicherheitsupdate erhalten“ [19]. Ein Router „hatte sogar 2.000 Tage lang kein Sicherheitsupdate mehr erhalten.“ [19]. Weitere Sicherheitsmängel sind „einfach zu entschlüsselnde, hartcodierte Passwörter bis hin zu bereits bekannten Schwachstellen, die eigentlich längst behoben sein müssten.“ [19]. Über 90 Prozent der „Router setzen Linux als Betriebssystem ein, allerdings werden oftmals sehr alte Versionen genutzt.“ [19]. Einer der Forscher hat angesichts der Prüfergebnisse sich sogar zu der Aussage verleiten lassen, dass „[d]ie Hersteller müssten eigentlich nur die aktuellste Software aufspielen, aber sie integrieren diese nicht in dem Maße, wie es könnten und müssten.“ [19], was erst recht für „hartcodierte Anmeldedaten“ [19] gilt. Selbst Router der Firma AVM hatten Sicherheitsmängel s. [19]. Aufgrund der teilweise erheblichen Sicherheitsmängel ist es für Angreifer bzw. Geheimdienste ein leichtes Spiel, um auf die dahinter liegende Infrastruktur über die Schwachstelle Router anzugreifen s. [20]. Hinzu kommt die Tatsache, dass es nur wenige Hersteller auf dieser Sparte gibt, so dass bei gefundenen Schwachstellen ein überproportionaler Anteil an Routern gleich mitbetroffen ist. Daher lautet das Fazit vom beteiligten Forscher, „dass die Hersteller noch viel mehr Anstrengungen unternehmen müssen, um die Geräte deutlich sicherer zu machen.“ [19].

Vor diesem Hintergrund fordert der Computer Chaos Club (CCC) ein „Mindesthaltbarkeitsdatum für die Pflege der auf dem Router laufenden Software“ [21] und die Option „alternative Software - wie z. B. OpenWrt - auf seine Router einzuspielen.“ [21]. Damit sollen Nutzern die Möglichkeit gegeben werden, im Falle eines Falle Selbsthilfe betreiben zu können, falls der Hersteller keine Updates mehr anbietet und gleichzeitig wird damit auch für Langlebigkeit gesorgt, um unnötige Käufe zu ersparen s. [21].

Bei Routern gibt es folgende Bedrohungen / Risiken:

„1. Manipulation der Konfiguration

2. Angriffe unter Ausnutzung bekannter und nicht geschlossener Sicherheitslücken

3. Angriffe unter Ausnutzung von neu entdeckten Sicherheitslücken (Zero-Day Exploits)

4. Angriffe über IP-Telefonie-Verbindungen

5. Diebstahl (insbesondere auch Router im Außenbereich / Mobilfunk)

6. Verfügbarkeitsangriffe (DoS-Angriffe)

7. Zugriff durch undokumentierte Schnittstellen (s.g. Hintertüren/ Backdoors)

8. Ausführen von Fremdcode und Integration in Botnetze

9. Angriffe über unzureichend abgesicherte WLANs“ [22, p. 46].

3.1.7 Risiko der Zweckentfremdung von ursprünglichen Funktionen

Ein israelisches Forschungsteam hat eine Software - SPEAKE(a)R - geschrieben, die einen am PC angeschlossenen Kopfhörer unbemerkt in ein Mikrofon verwandeln kann s. [23]. Es ist sogar mit Hilfe einer Malware in der Lage, auch dann den Computer als Abhörgerät zu nutzen, wenn kein Mikrofon vorhanden, stummgeschaltet, abgedeckt oder ausgeschaltet ist s. [23].

3.1.8 Risiko Drittfirmen über Apps

Bspw. hat die Firma „Alphonso“ eine Software entwickelt, die in mindestens 1.000 Spiele-, Messaging- und Social-Apps integriert ist und unbemerkt über das Mikrofon des Smartphone-Nutzers lauscht s. [24], s. [25]. Die Software identifiziert anhand von Audiosignalen Werbespots und Sendungen, die der Nutzer gerade hört und gleicht diese mit Ortsdaten ab, um zielgruppenorientiertes Marketing zu ermöglichen s. [24].

3.1.9 Risiko Drucker

Ein weiteres Angriffsziel sind Drucker, die sich inzwischen selbst zu komplexen Netzwerkcomputersystemen entwickelt haben s. [26]. Laut einer Studie konnten Forscher mit einem Open Source Tool „PRinter Exploitation Toolkit (PRET)“ [26] folgende Angriffe

ausführen: Denial-of-Service (DoS)-Angriffe oder angepasste Angriffe, um an Druckaufträge bzw. Systemdateien heranzukommen s. [26]. Im Fazit schreiben sie explizit: „Geräte mit aktueller Firmware können immer noch mit einfachen Angriffen angegriffen werden, die schon seit mehr als einem Jahrzehnt bekannt sind, … erlauben Angreifern … sogar in Firmennetzwerke einzudringen. Dies zeigt, dass die Druckerhersteller die Sicherheitsvorfälle nicht ernst nehmen oder sie haben keine richtigen Sicherheitsanalysetools.“ [26]. Darüber hinaus besteht ein Risiko durch die intransparente Funktionsweise der Firmware s. [26].

3.1.10 Risiko Undokumentierte Funktionen

Ein hohes Risiko stellen undokumentierte Funktionen dar, die fast immer mit Entwicklungs- oder Supportangelegenheiten zusammenhängen s. [27, p. 3]. In diesem Falle sind meist alle drei Schutzziele betroffen, wenn damit die Möglichkeit besteht, Sicherheitsmechanismen zu umgehen wie es bspw. in Intel-Chips über sog. Debugging-Schnittstellen der Fall war, in dem ein Zugriff auf sensible Daten ermöglicht wurde s. [27, p. 3], s. [28]. Allein im letzten Jahr wurden bei den Prozessoren von Intel 22 Schwachstellen gefunden, davon einige kritischer Natur s. [29]. Eine Übersicht über prinzipielle Risiken der Intelarchitektur ist dem Paper von Joanna Rutkowska zu entnehmen [30]. Ein weiteres Beispiel ist der sog. Machine Identification Code (MIC), bei der viele Farbdruckergeräte einen fast unsichtbaren MIC mitdrucken s. [31]. Damit ist es möglich, den Drucker zu identifizieren, mit dessen Hilfe bspw. eine Whistleblowerin identifiziert wurde s. [32].

3.1.11 Risiko IT-Sicherheitsprodukte

Bspw. sind Antiviren Produkte per se nicht sicher. Selbst Golem hat als Titel „Das Jahr der unsicheren Sicherheitssoftware“ [33] für Antivirenprogramme gewählt, da diese Sicherheitsprobleme aufwiesen s. [33]. Der Einsatz von Sicherheitssoftware löst bei Nutzern ein falsches Sicherheitsgefühl aus, da diese nicht die Sicherheit gewährleisten können, wie es suggeriert wird s. [33]. Dies beginnt mit Scans mit Signaturen, die bei Zero Days nicht hilft bis hin zu weiteren Funktionalitäten, die zu mehr Komplexität führen und damit mehr Angriffsflächen bieten s. [33]. Selbst Microsoft sowie die auf Sicherheit spezialisierte Firma Fireeye waren über mehrere Monate den beiden Malwarearten Sunburst und Supernova, welches über die IT-Managementsoftware Orion des Software-Herstellers Solarwinds eingeschleust wurde, betroffen gewesen s. [33]. Ein weiteres Beispiel ist die Schadsoftware Emotet, welches bei Windowssystemen sich über Office-Makros aktivieren lässt, was die hauseigene Sicherheitssoftware Defender als „wirkungslos“ [33] dastehen lässt s. [33]. Die Sicherheitsfirma Rack911 Labs konnte „mit Hilfe von Verzeichnisverknüpfungen (Windows) und Symlinks (macOS & Linux) fast jede Antiviren-Software in ein selbstzerstörerisches Werkzeug verwandeln“ [34], dies betraf fast alle marktgängigen 28 Antivirenprogramme s. [34]. Ein weiteres Negativbeispiel ist die Firma Avast. Zum einen hatte die gleichnamige Software eine Schwachstelle in der Ja-

vascript-Engine, die es Angreifern ermöglicht hatte, „Code aus der Ferne mit Systemrechten ausführen zu lassen und Rechner, auf denen die Avast-Software installiert ist, zu übernehmen.“ [33]. Zum anderen hat die Tochterfirma von Avast, Jumpshot, zeitgleich über einen Browserplugin die Webnutzungsdaten von mehreren Hundert Millionen Nutzern gesammelt und an Unternehmen wie Google, Microsoft, McKinsey etc. verkauft s. [33]. Die Firma Jumpshot „bietet Einblicke in die Online-Reisen der Verbraucher, indem jede Suche, jeder Klick und jeder Kauf in 1.600 Kategorien von mehr als 150 Websites, darunter Amazon, Google, Netflix und Walmart, gemessen wird.“ [33]. Darunter wurden Youtube-Videos, Suchanfragen sowie der Aufruf von pornografischen Webseiten gesammelt s. [33]. Die größte Sicherheitslücke ist die Anwendung von Zero Days in Sicherheitssoftware, mit deren Hilfe Angreifer in IT-Systeme eindringen können s. [33]. Vor diesem Hintergrund ist es nachvollziehbar, dass es einen Diskurs darüber gibt, ob Sicherheitsprodukte, hier speziell Virenschutzprodukte die Angriffsfläche eher erhöhen können und damit eher Schaden als Nutzen. Zum anderen sind die Daten auf dem Rechner nicht sicher in dem Sinne, da ggf. als „infizierte markierte Dateien“ auf das Firmennetzwerk der jeweiligen Antivirenherstellers hochgeladen werden können und damit das Schutzziel Vertraulichkeit ausgehebelt ist. Zudem können die Antivirenfirmen selbst durch Geheimdienste gehackt bzw. zu einer Zusammenarbeit bewegt werden, so dass die Daten unbefugt an Dritte - hier Geheimdienste oder kriminelle Organisationen - gelangen können wie es bspw. durch den israelischen Geheimdienst bei Kaspersky geschah s. [35]. Ein weiteres exemplarisches Beispiel ist das Produkt Cb Response von Carbon Black, was ein Endpoint Detection Respond (EDR) Tool ist. Sicherheitsexperten der Fa. Directdefence haben herausgefunden, dass die Architektur des Tools ein Datenleck darstellt und es fast nicht möglich ist, dies zu verhindern s. [36]. Folgende Informationen konnten u.a. durch das Datenleck wiederhergestellt werden, wie bspw. „Cloud keys (AWS [Amazon Web Services], Azure, Google Compute), … App store keys (Google Play Store, Apple App Store) … Internal usernames, passwords, and network intelligence … Customer data“ [36]. Die Aufzählung zeigt auf, dass es sich um ein sog. „Super-Gau“ handelt, da durch den Einsatz dieses Sicherheitsprodukts sensible Daten wie bspw. Zugangsdaten erbeutet werden können.

3.1.12 Risiko Meldeverhalten zu Schwachstellen

Was den Austausch von Schwachstellen, Angriffen und Gegenmaßnahmen angeht, so agieren derzeit viele Unternehmen mehr für sich anstatt wie die Angreifer sich untereinander auszutauschen s. [37, p. 6]. Viele Unternehmen veröffentlichen Vorfälle nicht, weil dadurch Aufträge verloren gehen können und damit verbunden ein Reputationsverlust folgen kann. Der Nachteil dieser Vorgehensweise ist, dass andere Unternehmen als auch der Nutzer nichts von diesen Vorfällen erfahren können und dadurch ebenso erhöhten Risiken ausgesetzt sind s. [37, p. 6].

3.1.13 Risiko Schnittstellen

Laut BSI dienen Schnittstellen von IT-Systemen „der Kommunikation und dem Austausch von Daten.“ [38]. Das Hauptrisiko bei der Schnittstelle ist der Einfall von Schadsoftware mit den daraus möglichen Folgen eines Informationsabflusses s. [38]. Eine reale Gefahr von der anderen Seite ist die Tatsache, dass bspw. ein Pharmaunternehmen und ein Anbieter von elektronischen Krankenakten sich abgesprochen haben, die Schnittstelle der Krankenakte so zu modifizieren, dass Klinikmitarbeiter veranlasst wurden, die Verschreibung von Opioiden mit verlängerter Wirkstofffreisetzung zu erhöhen, einer Klasse von Opioiden mit hoher Suchtwirkung s. [39]. Dies führte zusätzlich zu hohen Todesfällen in den letzten zwei Jahrzehnten s. [39].

3.1.14 Risiko Clouddienste

Neben technischen Risiken, die in einem umfangreichen Kriterienkatalog Cloud Computing C5:2020 des BSI aufgelistet sind, wird hier insbesondere das Risiko der Zugriffsmöglichkeiten kurz beleuchtet s. [40]. Folgende Zugriffsmöglichkeiten haben Beschäftigte bei Cloudanbietern, die potentiell missbraucht werden können:

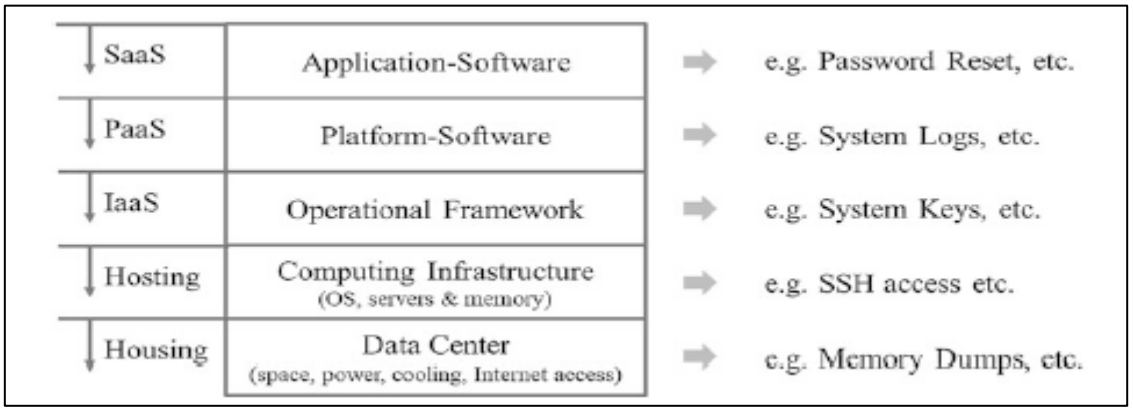


Bild 2: Zugriffsmöglichkeiten der Cloudanbieter [41, p. 17]

Wie dem o.g. Schaubild entnommen werden kann, gibt es auf jeder Schicht die Möglichkeit an Daten des Kunden heranzukommen. Selbst wenn die Daten auf der Cloud verschlüsselt sind, darf nicht außer Acht gelassen werden, dass diese Daten jederzeit unbemerkt kopiert werden können und mit diesen verschlüsselten Daten dann u.a. Brute-Force-Attacken ausgeführt werden können. Darüber hinaus darf der Cloudanbieter die Schlüssel zur Ver- und Entschlüsselung nicht selbst verwalten, da sonst ein unbefugter Zugriff möglich ist. Auch sind die Nutzungsbedingungen und Datenschutzbestimmungen zu prüfen, die ggf. nachteilig für den Nutzer sein können.

3.1.15 Risiko Forensiktools

Durch den Einsatz von Forensiktools ist es möglich, bei IT-Systemen des Bürgers - sowohl befugt als auch unbefugt - an Daten zu gelangen. Als Beispiel sei der Weltmarktführer Passware genannt, dessen Tool Passware Kit Forensic in der Lage ist, mehr als 300

verschiedene Arten von verschlüsselten Datentypen automatisiert zu erkennen s. [42]. Die Software kann die Festplatten entschlüsseln, Arbeitsspeicher analysieren, um Verschlüsselungsschlüssel sowie Passwörter zu extrahieren s. [42]. Dies gilt auch für Mobile - und Cloudlösungen, wo verschlüsselte Backups bzw. Images vorliegen s. [42].

3.1.16 Aktuelle Berichte zur Lage der Cybersicherheit in Deutschland

Vertiefende Berichte zur aktuellen Lage der Cybersicherheit bieten das BSI, das BKA sowie das Bundesamt für Verfassungsschutz (BfV) an, deren jeweiligen Berichte einmal im Jahr veröffentlicht werden. Zu diesen Berichten kann insgesamt konstatiert werden, dass Cyberangriffe „immer ausgefeilter" [18, p. 3] werden und „[g]leichzeitig wird die IT-Abhängigkeit der Unternehmen, des Staates und der Bürger immer größer, wodurch das Schadenspotenzial zunimmt." [18, p. 3]. Des Weiteren nehmen „Abflüsse von personenbezogenen Daten … u.a. von Patientendaten" [18, p. 9] zu, was ebenso für „kritische Schwachstellen in Software- und Hardwareprodukten" [18, p. 9] gilt. Derzeit entstehen „rund 322.000 neuen Schadprogrammen-Varianten pro Tag" [18, pp. 9-10]. Hierbei wird zwischen einem Zero-Day-Schadprogramm, die noch nicht als Schadprogramm erkannt wurden und einem bekannten Schadprogramm unterschieden, wobei erstere die gefährlichere Variante ist, da unerkannt ein IT-System angegriffen und weitere Aktionen vorgenommen werden kann. Für das BSI stellt Ransomware derzeit eine der größten Bedrohungen dar s. [18, p. 11]. Hinsichtlich Botnetze wurden derzeit „täglich bis zu 20.000 Bot-Infektionen deutscher Systeme registriert" [18, p. 16]. Hier stellt das BSI selbst nach drei Jahren fest, dass offenbar weiterhin „viele betroffene Anwenderinnen und Anwender ihre infizierten Systeme noch nicht bereinigt haben." [18, p. 17], s. [18, p. 17]. Darüber hinaus nehmen Infektionen aufgrund von unzureichend gesicherten Internet of Things-Geräten (IoT) und mobilen Systemen zu s. [18, p. 16]. Zum Diebstahl und Missbrauch von Identitätsdaten hat das BSI Identitätsdaten wie folgt definiert: „die Menge von Merkmalen …, die die Echtheit einer Person oder Sache nachweist … durch ein einziges Merkmal oder aber durch die Kombination diverser Merkmale bestimmt werden. … [D]ie Identität einer Person [wird] meist aus Identifikations- und Authentisierungsdaten geschlossen wie zum Beispiel aus der Kombination von Benutzername und Passwort." [18, p. 18]. Hier konstatiert das BSI, dass „[d]ie Fülle kompromittierender Nutzerinformationen und deren Missbrauchsmöglichkeiten macht private Informationen zu einem weithin verfügbaren und wertvollen Handelsgut, wodurch Sicherheit und Vertrauen in die gesamte digitale Infrastruktur gefährdet sind." [18, p. 18]. Dadurch steigt die Attraktivität für Angreifer, die damit „Manipulations- und Erpressungsbestrebungen sowie automatisierte Authentisierungsversuche (sogenanntes „Credential Stuffing") bis hin zum Direktzugriff auf fremde Konten" [18, p. 18] an Handlungsoptionen haben s. [18, p. 18]. Auch Sextortion gehört dazu, in dem Angreifer behaupten, das Opfer beim Besuch einer Webseite mit pornografischen Darstellungen beobachtet und aufgezeichnet zu haben s. [18, p. 19]. Eine Gefahr droht auch durch Browser-Erweiterungen, da hier persönliche Daten wie bspw. Surfverhalten meist unerkannt erfasst werden und für weitere Zwecke missbraucht werden, wie es zuletzt sogar durch einen IT-Sicherheitshersteller möglich wurde, ohne

den Nutzer darüber zu informieren s. [18, p. 20]. Hier wird besonders deutlich, dass auch „scheinbar unbedeutende Programme wie beispielsweise Browser-Erweiterungen … großen Schaden anrichten“ [18, p. 20] können. In diesem Zusammenhang spielen auch Daten-Leaks eine große Rolle, an dem alle Branchenbereiche betroffen waren s. [18, p. 20]. Daher konstatiert das BSI an dieser Stelle, dass „[d]ie Vielfalt und Häufigkeit von Vorfällen, bei denen immer wieder sensible Daten unfreiwillig veröffentlicht werden, … besorgniserregend“ [18, p. 20] sind. Das gilt besonders für Vorfälle im Gesundheitssektor, da die Veröffentlichung „sensibler Daten auch gleichzeitig negative Auswirkungen auf die jeweilige Gesundheit der Patientinnen und Patienten haben - mit möglicherweise lebenslangen Folgen.“ [18]. Desweiteren nehmen Advanced Persistent Threats (APT) zu. APT sind „oft langfristig und mit großem Aufwand geplante Angriffe auf einzeln ausgewählte … Ziele.“ [18, p. 28] Die vorwiegende Motivation ist hier die „Beschaffung von Informationen über das Ziel und ggf. der Sabotage.“ [18, p. 28]. Die Angriffsmethoden reichen von manipulierten E-Mail-Anhängen oder Links über legitime Software-Produkte, über Schwachstellen in Fernwartungsdiensten oder der Nutzung von Zugangsdaten, die zuvor ausgespäht wurden s. [18, p. 28]. Darüber hinaus werden zunehmend „die Infrastrukturen und Zugangsdaten von Zulieferern“ [18, p. 28] als Sprungbrett genutzt, um die tatsächlichen Ziele anzugreifen. Diese Vorgehensweise fußt auf der Tatsache, dass Zulieferer nicht immer wie - das eigentliche Ziel - das gleiche IT-Sicherheitsniveau vorweisen, so dass über „schlecht gesicherte Zulieferer … [diese] an das … Netzwerk“ [18, p. 28] der Zielorganisation gelangen s. [18, p. 28]. Die Zunahme gilt auch für Distributed-Denial-of-Service-Angriffe (DDoS-Angriffe), bei der das Schutzziel Verfügbarkeit betroffen ist.

Laut dem Cybercrime-Bericht des Bundeskriminalamts (BKA) sind folgende Feststellungen für das Jahr 2020 in Deutschland getroffen worden:

1. „Die Anzahl erfasster Cyberstraftaten steigt weiter an.

2. Der Fokus von Cyberkriminellen liegt vermehrt im Bereich „Big Game Hunting“.

3. Die Täter sind global vernetzt und agieren zunehmend professioneller.

4. Ransomware bleibt weiterhin die Bedrohung für öffentliche Einrichtungen

und Wirtschaftsunternehmen.

5. Die Anzahl an DDoS-Angriffen steigt weiter an – auch ihre Intensität nimmt zu.

6. Die Underground Economy wächst – sie stellt eine kriminelle, globale

Parallelwirtschaft dar, die maßgeblich auf finanziellen Profit aus ist.“ [43, p. 3].

Bei der Durchsicht der Cybercrime für das Jahr 2020 fällt auf, dass keine Branche von Cyberangriffen im Berichtszeitraum verschont blieb s. [43, pp. 5-6]. „Cybercrime im engeren Sinne“ [43, p. 42] sind laut BKA „Straftaten, die sich gegen das Internet, informationstechnische Systeme oder deren Daten richten“ [43, p. 42]. „Cybercrime im weiteren

Sinne“ [43, p. 42] sind „Straftaten, die unter Nutzung von Informationstechnik begangen werden (Tatmittel Internet)“ [43, p. 42].

Zum Bundeslagebild ist hinzuzufügen, dass diese unvollständig ist, zum einen durch die Nichtbetrachtung von Delikten, „die lediglich unter Nutzung von Informationstechnik begangen“ [43, p. 9] wurde und zum anderen hier noch eine hohe Dunkelfeldziffer hinzukommt, da nicht jeder Cyberangriff zur Anzeige gebracht wird und eine Unterscheidung bei Wirtschaftsspionage getroffen wird, für die der Verfassungsschutz zuständig ist. Es wird ausdrücklich im Bericht betont, dass „das zugehörige Dunkelfeld weit überdurchschnittlich ausgeprägt“ [43, p. 9] ist und zwar ausfolgenden Gründen:

1. „Eine große Anzahl strafbarer Handlungen im Internet kommt … meist nicht über das Versuchsstadium hinaus und wird von den Geschädigten nicht bemerkt.

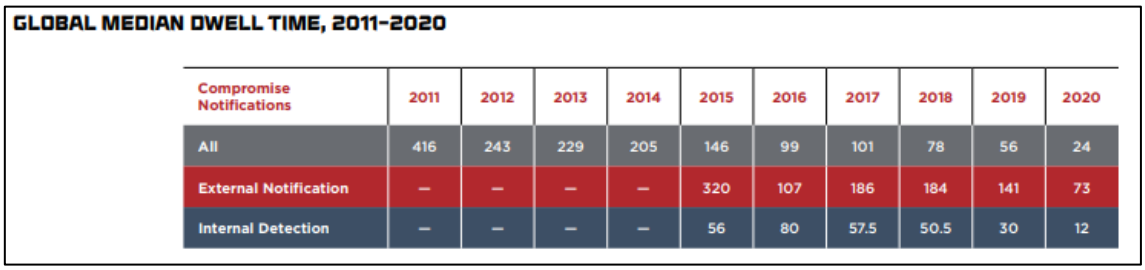
2. Die Opfer erkennen ihre Betroffenheit nicht ….

3. Straftaten werden durch die Betroffenen oftmals nicht angezeigt … wenn noch kein finanzieller Schaden entstanden ist ….

4. Geschädigte, insbesondere Wirtschaftsunternehmen, zeigen erkannte Straftaten nicht an, um u.a. die Reputation … nicht zu verlieren.

5. Geschädigte erstatten oftmals … nur dann Anzeige, wenn trotz Zahlung eines Lösegelds keine Dekryptierung … erfolgt.“ [43, p. 9].

Zu Punkt 2 wird dieser Eindruck auf der folgenden Grafik dahingehend bestätigt, aus dem hervorgeht, dass es vom Einbruch bis zur Entdeckung - je nach Branche - von 329 Tagen im Gesundheitssektor bis zu 233 Tagen im Finanzbereich andauert s. [44]. Darüber hinaus wird festgestellt, dass die interne Detektion von der Zeitdauer viel kürzer ist als wenn ein Hinweis bei den betroffenen Institutionen durch Externe kommt, wie es in der folgenden Grafik dargestellt wird s. [45, p. 11]:



Compromise Notifications	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
All	416	243	229	205	146	99	101	78	56	24
External Notification	–	–	–	–	320	107	186	184	141	73
Internal Detection	–	–	–	–	56	80	57.5	50.5	30	12

Bild 3: Globale mittlere Verweildauer 2011-2020 [45, p. 11]

Für 2020 stellt die Sicherheitsfirma Fireeye fest, dass die weltweite Durchschnittsdauer vom Einbruch bis Entdeckung „Dwell Time“ bei externen Benachrichtigungen 73 Tage beträgt, während die interne Detektion 12 Tage andauert, so dass ein Durchschnittswert von 24 Tagen errechnet wurde s. [45, p. 11].

Bei der Gesamtstatistik zu Cybercrime im engeren Sinne hat das BKA für das Jahr 2020 108.000 Delikte registriert, was einer Steigerung von 7,9 % im Vergleich zum Vorjahr bedeutet s. [43, p. 9]. Die aufgeklärten Fälle bleiben relativ konstant im Bereich zwischen

31.000 und 35 .000 Fällen, was einer Aufklärungsquote von knapp unter 30 % entspricht, d.h. es bleiben über 70 % der Straftaten ungeklärt s. [43, p. 10]. Der Anstieg ist auf folgende Anzeichen zurückzuführen:

1.„Stark voranschreitende Digitalisierung aller Lebensbereiche, … dadurch entstehen mehr Tatgelegenheiten für Cyberkriminelle.

2. Zunehmende Professionalisierung der Täter und steigende Fähigkeiten der Schadsoftware zur Verschleierung vor Sicherheitsmechanismen ….

3. Niedrige Eintrittschancen in die Cybercrime – durch Cybercrime-as-a-Service werden kaum technische Kenntnisse zur Begehung einer Cyberstraftat benötigt.“ [43, p. 10].

Die Underground Economy ist ein System, welches auf „arbeitsteiligen Wertschöpfungsketten, losen interpersonellen Strukturen und vornehmlich finanzieller Motivation“ [43, p. 12] basiert. Die beliebteste Handelsweise sind Digitale Identitäten, die als Ausgangspunkt für weitere kriminelle Handlungen genutzt werden s. [43, p. 12]. Die Webseite des Hasso-Plattner-Instituts (HPI) hat mit Stand vom 16.08.2021 12.414.154.697 kompromittierte Accounts gezählt s. [46]. Das sind durchschnittlich 1.602.724 geleakte Accounts pro Tag s. [46].

Die neun Säulen der Cybercrime basieren darauf, dass die Täter sich auf einzelne Bereiche spezialisiert haben und daher aus diesem Grunde arbeitsteilig vorgehen, um auch komplexere Straftaten begehen zu können s. [43, p. 45]. Hierdurch ist es möglich - Cybercrime-as-a-Service - als Dienstleistung anbieten zu können, so dass auch weniger technisch versierte Täter Straftaten durchführen zu können s. [43, p. 45]. Bei einem Fallbeispiel zur Ransomwareattacke schreibt das BKA, dass beim Universitätsklinikum Düsseldorf „vermutlich 100.000 Patientendaten aus dem Netzwerk entwendet“ [43, p. 26] wurden, die genaue Höhe der entwendeten Daten konnte anscheinend nicht ermittelt werden. Bei den Angriffen auf die Wirtschaft sind die „beliebtesten Eintrittsvektoren … (Spear-)Phishing, Malspam, kompromittierte RDP-Protokolle sowie die Nutzung illegitim erlangter Log-In-Daten.“ [43, p. 29]. In diesem Zusammenhang ist hier mit der Kompromittierung der Software „Orion“ von der Firma SolarWinds bislang eine der größten Cyberangriffe in der Geschichte am 13. Dezember 2020 bekannt geworden s. [43, p. 29]. Hier haben Angreifer die Software „Orion“ nach einem Netzwerkeinbruch der Firma SolarWinds kompromittiert, mit der es möglich wurde, über die legitime Softwareaktualisierung, die auf dem Updateserver manipuliert wurde, mit Hilfe der Malware „SUNBURST“ persistent Zugriff auf die IT-Netzwerke der Kunden zu erlangen s. [43, p. 29]. Hierbei wurde die Kommunikation mit den Command-and-Control-Servern „als legitime Kommunikation der Orion-Software getarnt“ [43, p. 29], dabei wurden in „legitimen Konfigurationsdateien“ [43, p. 29] die erlangten Daten zwischengespeichert s. [43, p. 29].

Davon waren weltweit über 18.000 IT-Systeme betroffen, darunter Hersteller wie Microsoft sowie Behörden und Institutionen, die dem kritischen Dienstleistungssektor angehören s. [43, p. 30]. Diese Angriffsart gehört zu den sog. Supply-Chain Angriffen, bei dem

die Lieferkette kompromittiert wird, um das eigentliche Ziel darüber anzugreifen s. [43, p. 29]. Damit wird hier exemplarisch aufgezeigt, wie „durch die Vernetzung und gleichzeitige Ausnutzung von Lieferketten Dimensionen mit großer Reichweite annehmen können." [43, p. 30], denn „[d]urch die Verflechtung von Wirtschaftskreisläufen, IT-Systemen und Lieferketten genügt es" [43, p. 30] allein nur ein einziges „Element in diesem Beziehungsgeflecht anzugreifen, dass über die meisten Verbindungen in andere Systeme verfügt." [43, p. 30]. Durch die „voranschreitende Globalisierung" [43, p. 30] und Digitalisierung wird die Vulnerabilität hier besonders eindrucksvoll dargestellt s. [43, p. 30]. Darüber hinaus zeigt dieser Fall exemplarisch auf, wie gut die Angreifer einerseits organisiert und andererseits sehr professionell vorgegangen sind, so dass selbst bei technisch sehr gut ausgerüsteten Unternehmen mit jeweils eigener großen Sicherheitsorganisation wie die Firma Microsoft, die Malware über ein Jahr unentdeckt blieb s. [43, pp. 29-30].

Daher hat angesichts der o.g. Entwicklungen das Fraunhofer-Institut für Sichere Informationstechnologie (SIT) folgende Problemfelder identifiziert:

„Der Sicherheitsstatus der ausgerollten Technologie" [47, p. 7] wurde überwiegend ohne Berücksichtigung von IT-Mindestsicherheitsstandards entwickelt, so dass diese Schwachstellen aufweisen, die für Angriffe genutzt werden s. [47, p. 7]. Daher ist nicht nur die sichere Entwicklung neuer IT-Systeme zu betrachten, sondern auch die gegenwärtigen Dienste und Produkte müssen abgesichert werden s. [47, p. 8]. Die IT-Systeme einschließlich des Internets sind so komplex und dynamisch, dass selbst Experten nicht alles überblicken können s. [47, p. 8]. Aus diesen Gründen gibt es keine Person, die „alle internetrelevanten Standards, Methoden und Werkzeuge kennt" [47, p. 8]. Derzeitige „Methoden, Denkweisen und Lösungen" [47, p. 8], die die IT-Systeme absichern sollen, sind nicht mehr hinreichend s. [47, p. 8]. Die meisten Informations- und Kommunikationstechnik-Produkte (IKT) und Dienstleistungen sowie der Bereich Cybersicherheit befinden sich außerhalb von Europa s. [47, p. 8]. Darüber hinaus bestehen IKT-basierte Systemen in der Regel aus einer Vielzahl von Komponenten, die wiederum aus verschiedenen Ländern mit unterschiedlichen Rechtssystemen stammen s. [47, p. 8]. Dies impliziert, dass bei bestimmten Ländern Zusicherungen oder rechtliche Bedingungen für Anwender unerwünschte Risiken gibt s. [47, p. 8]. Es herrscht ein Mangel an Fachkräften für den Bereich Cybersicherheit, was u.a. darauf zurückzuführen ist, dass IT-Sicherheit an Hochschulen zumindest vor dem Jahr 2000 nicht enthalten war s. [47, p. 8]. Hinsichtlich des Problems „Sicherheitsprozesse in Unternehmen und Behörden" [47, p. 9] sind jeweils Aufwände für die Behandlung identischer Sicherheitsfragen erforderlich s. [47, p. 9]. Dadurch wird Cybersicherheit teurer, da dieser Ansatz ineffektiv ist s. [47, p. 9]. Beim nächsten Problem zum „Forschungsrahmen und Forschungssteuerung für Cybersicherheit" [47, p. 9] sei auf die Rahmenbedingungen verwiesen, die beispielsweise unvereinbar sind für schnelle Reaktionen auf tagesaktuelle Ereignisse s. [47, p. 9]. Als nächstes genügt die Konzentration der Fortentwicklung der Cybersicherheit allein auf die Technik nicht, daher müssen Instrumente und Mechanismen angewendet werden, um das Sicherheitsniveau in Produkte, Dienstleistungen und Infrastrukturen auf hohem Niveau aufrecht

zu erhalten s. [47, p. 10]. Darüber hinaus haben die Anwendung von IT-Systemen und die dazu genutzten Informationssicherheitsprodukte Auswirkungen auf Werte wie Meinungsfreiheit, Privatsphärenschutz, Schutz der demokratischen Grundordnung s. [47, p. 10]. Diese Werte können durch bestimmte Anwendungen in IT-Systemen gefährdet sein s. [47, p. 10]. Daher ist „ein tiefes Verständnis potenzieller Auswirkungen dieser Technologien auf grundrechtlich verankerte oder sonstige Werte“ [47, p. 10] notwendig.

Vor diesem Stand ist eine Weiterentwicklung der Cybersicherheit für folgende Ziele notwendig:

1. Steigerung von Sicherheit und Privatsphäre: Das derzeitige Sicherheitsniveau muss erhöht werden s. [47, p. 11].

2. Berechtigtes Vertrauen: Nur durch die Stärkung der Cybersicherheit kann ein berechtigtes Vertrauen hergestellt werden s. [47, p. 11].

3. Gestaltung von Cybersicherheit und Datenschutz durch Strategie und Umsetzung: Durch die Gestaltung des Rahmens zur Verbesserung der Cybersicherheit und Datenschutz ist die Identifikation von relevanten Ansatzpunkten erforderlich s. [47, p. 11].

Aus den o.g. Rahmenbedingungen sind folgende sieben Thesen zur Cybersicherheit in Deutschland entwickelt worden:

1. „Strategisches Ziel „Digitale Souveränität““ [47, p. 13]: Hier ist vor allem die Abhängigkeit von IKT gemeint, wo der Hersteller vertraut werden muss, aufgrund mangelnder Überprüfbarkeit der IKT s. [47, p. 13]. Daher muss in Deutschland und Europa die Forschung und Entwicklung ausgebaut werden s. [47, p. 13].

2. „Mindeststandards und Produkthaftung“ [47, p. 15]: Vertrauen kann durch Mindeststandards und Privatsphärenschutz sowie Testierung nachgewiesen werden s. [47, p. 15]. Darüber hinaus müssen Haftungsregeln für Produkte und Dienstleistungen geregelt werden s. [47, p. 15].

3. „Cybersicherheitsinfrastrukturen“ [47, p. 16]: Es sind Cyberinfrastrukturen notwendig, um digitale Identitäten, Verschlüsselung in der Breite anbieten und nutzen zu können s. [47, p. 16].

4. „Stärkung von Grundrechten“ [47, p. 17]: Datenbasierte Geschäftsmodelle bzw. die damit verbundene Möglichkeit der Überwachung muss hinter den Grundrechten der Bürger stehen, dies gilt auch für Verschlüsselungstechnologien, die nicht eingeschränkt werden dürfen s. [47, p. 17].

5. „Aus- und Weiterbildung“ [47, p. 18]: Hier sind mehr Fachkräfte notwendig s. [47, p. 18].

6. „Cybersicherheitsforschung“ [47, p. 18]: Es sind mehr Grundlagen und Technologieforschung notwendig, um den Bedrohungen der Informationssicherheit entgegenwirken zu können s. [47, p. 18].

7. „Innovationsrahmen für Cybersicherheit“ [47, p. 20]: Innovation und Entwicklung muss ausgebaut werden s. [47, p. 20].

Diese o.g. Punkte bleiben bis heute weiterhin aktuell und haben sich bis dato nicht verändert.

3.1.17 Zwischenfazit

Am schwerwiegendsten ist die Existenz von Hardware- bzw. hardwarenahen Trojanern zu betrachten, weil hierfür meistens keine adäquaten Schutzmöglichkeiten existieren und darüber hinaus auch keine Verschlüsselung hilft, weil diese ausgehebelt wird. Dies gilt auch analog für Schwachstellen in der CPU-Architektur. Danach sind fehlerhaft umgesetzte kryptografischen Mechanismen als schwerwiegend zu betrachten, weil hierfür fast keine Erkennungsmöglichkeiten existieren, um den Fehler zu erkennen, was im Worst-Case-Szenario dazu führt, dass alle Daten - anstatt verschlüsselt - offen vorliegen. Der Einsatz von IT-Sicherheitsprodukten stellt zum einen nicht sicher, dass das IT-System wirklich geschützt ist, da es selbst u.a. auch Schwachstellen vorweist und zum anderen geht der durchschnittliche Nutzer fälschlicherweise davon aus, dass dessen IT-System sicher sei, was selbst ein Risiko darstellt. Da Nutzer ohne Router nicht in das Internet gelangen können und deswegen von diesem IT-System abhängig sind, ist ein sicherer Betrieb unumgänglich, da sonst bspw. IoT-Geräte - einschließlich des Datenflusses - im Haushalt des Nutzers ungeschützt sind, was u.U. durch manipulierte Heizungen Menschenleben gefährden kann. Der Einsatz von Clouddiensten bringt vielfältige und teilweise nicht transparente Risiken mit sich, so dass von einer Nutzung abzuraten ist. Darüber hinaus ist bei der zunehmenden Digitalisierung und der damit verbundenen Vernetzung die Komplexität gestiegen, so dass die Risiken bzw. die Schwachstellen nicht mehr eindeutig überschaubar sind. Vor diesem Hintergrund wird die Eruierung von passenden Schutzmaßnahmen bzw. -verhalten aufwendiger, um einen ganzheitlichen Schutz zu ermöglichen. Die durchschnittlichen Nutzer sind bereits mit der Komplexität eines E-Mail-verschlüsselungsprogrammes - hier Pretty Good Privacy (PGP) - überfordert, wie es durch eine Studie festgestellt wurde s. [48]. Daher sind Software-Hersteller und Hardware-Produzenten weltweit zu verpflichten, dass IT-Produkte u.a. sowohl sicher zu entwickeln als auch nutzerfreundlich zum sicheren Umgang mit dem IT-Produkt zu gestalten sind. Bei Verstoß gegen diese Prinzipien muss eine Haftung möglich sein.

3.2 Risiko Plattformen

Die gegenwärtigen Plattformen wie Alphabet und Meta sind Gatekeeper und Aggregatoren zugleich und lösen somit einen „Sog hin zu Winner-takes-all-Märkten“ [49, p. 34] aus s. [49, p. 34]. Hinzu kommen sog. Netzwerkeffekte hinzu, „auch durch ein >>kognitives Lock-in<< (wenn die Nutzung eines Angebots zur Gewohnheit wird und dadurch ein Wechsel überproportionalen Aufwand bedeutet).“ [49, p. 34]. Weitere Gründe für die digitale Konzentration sind „[g]eschlossene statt offene Standards“ [49, p. 36] (bspw. ist

es nicht möglich von Whatsapp zu Threema zu kommunizieren) sowie „[h]ohe technologische Kosten/Einstiegsbarrieren“ [49, p. 36]. Darüber hinaus übernehmen „IT-Konzerne wie Apple oder Alphabet … staatliche Verantwortlichkeiten, … [bspw. durch die] Bereitstellung digitaler Patientenakten.“ [50, p. 183]. Bei letzterem handelt es sich um Hegemoniebestrebungen, um Beziehungspunkte zu kontrollieren s. [50, p. 183]. Denn daraus „entstehen Abhängigkeiten, die zur „Präsenz der herrschenden Macht“ [50, p. 183] beitragen“, was durch die „Errichtung von Äquivalenzketten“ [50, p. 183] ermöglicht wird. Bspw. entstehen durch die Übernahme von „vorher nationalstaatliche[n] Aufgaben durch IT-Unternehmen“ [50, p. 183] Äquivalenzketten. Vorreiter auf diesem Gebiet ist die Firma Google, jetzt Alphabet. Das Bundeskartellamt stellt fest, dass Alphabet mit den darin verbundenen Tochterfirmen „eine überragende marktübergreifende Bedeutung für den Wettbewerb“ [51, p. 1] darstellt. „Insbesondere bietet Google eine breite Vielzahl von Diensten markt- und reichweitenstart an, hat bei diesem Angebot und seiner Erweiterung die Möglichkeit, von Verbundvorteilen zu profitieren und marktübergreifend gegenüber anderen Unternehmen die Rolle eines Regelsetzers einzunehmen, kann dabei auf einen breiten und tiefen Datenzugang zurückgreifen und seine Position ohne hinreichende wettbewerbliche Kontrolle weiter konsolidieren, ausweiten oder auf sonstige Weise zum eigenen Vorteil nutzen.“ [51, pp. 2-3]. D.h. jede interaktive Handlung mit den unterschiedlichen Diensten von Google wird erfasst und ausgewertet. Allein die Suchmaschine Google hat hier in Deutschland einen Marktanteil von über 80 % und übt damit eine marktbeherrschende Stellung aus. Hier ist auch zu berücksichtigen, dass Google durch „Vereinbarungen mit Originalgeräteherstellern (OEMs) über Vorinstallationen und Voreinstellungen (etwa in Android) … förder[t]“ [51, p. 3]. Selbst das “datenschutzfreundliche“ Unternehmen wie Apple lässt sich von Google bis zu fünfzehn Milliarden Dollar für das Jahr 2021 allein nur dafür zu bezahlen, „damit Google weiterhin die Standardsuche in Safari auf I-Phone, iPad und Mac bleibt.“ [52]. Das Bundeskartellamt konstatiert, dass die Suchmaschine von Google „unter dem Aspekt der Teilhabe eine Schlüsselfunktion für das gesellschaftliche Leben in Deutschland und weltweit“ [51, p. 5] hat. Darüber hinaus gibt es kaum eine Möglichkeit den Diensten von Alphabet Inc. beim Aufrufen von Webseiten auszuweichen, da der Konzern „über 90 Prozent der Internetnutzer weltweit“ [51, p. 3] über das Google-Display-Netzwerk erreicht. Auch zu Facebook hat das Bundeskartellamt ein Verfahren eingeleitet und hat u.a. folgendes festgestellt: „Der Schaden liegt hier … in einem Kontrollverlust für den Nutzer: Er kann nicht mehr selbstbestimmt über seine persönlichen Daten verfügen. Er kann nicht überschauen, welche Daten aus welchen Quellen für welche Zwecke zu einem detaillierten Profil zusammengeführt werden. Die einzelnen Daten erhalten durch die Zusammenführung einen nicht vorhersehbaren Stellenwert. Durch die Marktmacht kann sich der Nutzer der Datenzusammenführung auch nicht entziehen. Dies ist auch ein Eingriff in sein grundrechtlich geschütztes Recht auf informationelle Selbstbestimmung.“ [53, pp. 4-5]. Diese Feststellung kann auch 1:1 auf Alphabet, Apple, Amazon und Microsoft übertragen werden. Selbst Apple ist mit Abstand der größte Kunde von Google Cloud, in dem die Daten von iCloud Nutzern hinterlegt werden s. [54]. Hier wurde auch eine gegenseitige Abhängigkeit geschaffen. Hinsichtlich der Nichtinformation von Nutzern, hier speziell die Nutzung

von Patientendaten, sticht Alphabet wieder negativ hervor. Im Rahmen des „Project Nightingale“ wurden von der amerikanischen Gesundheitsorganisation Ascension Millionen Patientendaten auf den Servern von Alphabet gespeichert und verarbeitet s. [55]. Darüber hinaus haben 150 Mitarbeiter von Alphabet Zugriff auf diese Daten s. [55]. Von der Zusammenarbeit der Gesundheitsorganisation mit Alphabet wurden weder die Ärzte noch die Patienten informiert s. [55].

Ein weiteres Risiko bei der Nutzung von Plattformen besteht in der „Kuratierung von Inhalten“ [56, p. 16]. D.h. „[v]iele Plattformen bestimmen … mit welcher Priorität solche Inhalte anderen … Nutzern präsentiert und welche zusätzlichen Angebote und Empfehlungen unterbreitet werden.“ [56, p. 16]. Dies geschieht mit Hilfe von Algorithmen, „die das Verhalten von … Nutzern primär mit dem Ziel auswerten, deren Aufmerksamkeit mithilfe personalisierter Informationen möglichst lange zu binden und auf gezielt präsentierte Werbeinhalte zu lenken.“ [56, p. 16]. Wie die Auswertung der Daten vonstattengeht bzw. nach welchen Kriterien die Algorithmen funktionieren, erfolgt in i.d.R. intransparent für die Nutzer s. [56, p. 17]. Hier besteht das Risiko, dass „[m]ithilfe der Nutzungsdaten … die Plattformen … das Interesse, die Aufmerksamkeit und teilweise auch das Verhalten von … Nutzern beeinflussen oder sogar lenken, beispielsweise durch gezielte, aber kaum merkliche „Schubser“ („Nudging“, „Gamification“ usw.).“ [56, p. 17].

Die o.g. Vorgehensweise hat Shoshana Zuboff als Überwachungskapitalismus bezeichnet s. [57]. Der Überwachungskapitalismus nutzt Verhaltensdaten u.a. dazu, um einerseits die Produkte und Dienste zu verbessern, anderseits werden auch „Vorhersageprodukte“ [57, p. 22] erstellt s. [57, p. 22]. „[D]ie aussagekräftigsten Verhaltensdaten … bekommt [man], indem man Verhalten anstößt, herauskitzelt, tunt und in der Herde in Richtung profitabler Ergebnisse treibt.“ [57, p. 23]. Das langfristige Ziel lautet „*uns selbst* zu automatisieren“ [56, p. 23], was mit Hilfe von „Verhaltensmodifikationsmitteln“ [57, p. 23] geschehen soll. Vor diesem Hintergrund ist „[d]igitales Verbundensein … heute ein Mittel zu anderer Leute geschäftlichen Zielen.“ [57, p. 24]. Erfinder des Überwachungskapitalismus war Google - jetzt Alphabet - gewesen, was sich dann auf die Firmen Facebook - jetzt Meta - sowie Microsoft und später auf Amazon ausbreitete s. [57, p. 24]. Mit derartigen Praktiken konnte Google sich damals über das Internet ausbreiten, ohne dabei auf Hindernisse in Form von Gesetzen oder Wettbewerb ausgesetzt zu sein s. [57, p. 24]. Aufgrund der Sogwirkung und des finanziellen Erfolgs von Google hat inzwischen fast jedes webbasierte Unternehmen „die ökonomischen Imperative und Mechanismen“ [57, p. 25] übernommen. „Überwachungskapitalisten beanspruchen einseitig die Kontrolle über menschliche, gesellschaftliche und politische Territorien, die weit hinausgehen über das … Territorium der privaten Unternehmung oder des Markts.“ [57, p. 587]. Auch heute bringen „Extraktion und Ausbeutung“ [57, p. 588] von Verhaltensdaten die höchsten Margen s. [57, p. 588]. Die Macht der Plattformen - hier Alphabet und Meta - veranlasste Amnesty International zu einer Studie, in dem festgehalten wird, dass diese Geschäftsmodelle gegen die Menschenrechte verstoßen, hier insbesondere das Recht auf Privatsphäre sowie die daraus resultierenden Folgen, die folgende Rechte gefährden: „Meinungs- und Redefreiheit, Gedankenfreiheit und das Recht auf Nichtdiskriminierung.“ [58,

p. 5]. Das Internet Society sieht eine weitere Gefahr bei den Plattformen. Diese können „Innovationen einschränken, in dem sie die Interessen der Plattformen über die der Nutzer stellen und so den Wettbewerb und die Wahlmöglichkeiten der Nutzer einschränken“ [59]. Dies geschieht durch „die zunehmende Verwendung … plattformgesteuerter API's [Application Programming Interface] … [in dem] einen größere[r] Teil der Funktionen und der Interoperabilität des Internets in die Hände von immens mächtigen Ökosystemen“ [59] gelegt wird. Als Fazit wird wie folgt festgestellt: „Die Entwicklung neuer Anwendungen, Dienste und Unternehmen in der gesamten Weltwirtschaft hängt zunehmend von einer kleinen Zahl privater Plattformen ab, die sich im Besitz der größten Internet-Unternehmen befinden.“ [59], so dass die Gefahr einer zunehmenden Abhängigkeit besteht. „Die Auswirkungen von Konsolidierung und Konzentration auf die Internet-Wirtschaft … sind schwer abzuschätzen.“ [59].

Zwischenfazit

Die Zusammenführung von Daten aus internen und externen Quellen, die in einer Plattform verarbeitet werden, ermöglicht es den Betreibern dieser Plattformen ein umfassendes Bild der jeweiligen Nutzer zu verschaffen, was nicht nur zu Lasten des Schutzziels Vertraulichkeit führt, sondern zu weiteren wirtschaftlichen Folgen. Letztes Jahr wurde durch ein Gerichtsverfahren in Texas bekannt, dass Google u.a. „eine geheime Abmachung - … Codename „Jedi-Blue““ [60] mit Facebook geschlossen hat s. [60]. Dafür erhält Facebook „Informationen über Netznutzer:innen, anhand derer Facebook 60 % der Desktopnutzer und 80 % der Mobilnutzer eindeutig identifizieren kann.“ [60]. Allein dieses Vorgehen ist eine Manipulation des digitalen Werbemarktes. Tim Cook, Vorstandschef von Apple, äußerte sich wie folgt zu datensammelnden Firmen: „Am Ende werden „unsere eigenen Informationen, vom Täglichen bis zum sehr Persönlichen, mit militärischer Effizienz gegen uns gerichtet““ [61], was letzten Endes nichts als Überwachung ist. Daher hat er folgende Aussage getätigt: „Die Möglichkeit, dass jeder weiß, welche Seiten du jahrelang besucht hast, wer deine Kontakte sind, wer deren Kontakte sind, welche Dinge man mag oder nicht mag und jedes intime Detail deines Lebens kennt - das sollte meiner Meinung nach nicht existieren“ [61], was zu bejahen ist. Selbst wenn die Daten offensichtlich nicht nach der Datenschutz-Grundverordnung (DSGVO) konform erhoben worden sind, hat sich Irland auffallend zurückgehalten bei der Durchsetzung der DSGVO. Dort liegen 98 % aller Datenschutzangelegenheit bislang ungelöst vor s. [62]. Selbst der Europäische Datenschutzausschuss musste erstmalig nach Art. 65 DSGVO eine Anweisung an die irische Datenschutzbehörde erlassen, nachdem die anderen europäischen Aufsichtsbehörden mit dem irischen Vorschlag nicht einverstanden waren s. [63]. Ein Jahr später musste erneut eine Anweisung in einem neuen Verfahren gegen die Datenschutzbehörde von Irland erlassen werden s. [64]. Denn Datenschutz ohne Durchsetzung ist de facto kein Schutz. Als einzige Schutzmöglichkeit bleibt die Option übrig, diese Plattformen so lange nicht zu nutzen, bis die bisherige Maxime „nur … das Beste aus der Technologie herausholen …, wenn Nutzer [dabei] ihr Recht auf Privatsphäre abgeben“ [61] aufgegeben wird. Vor diesem Hintergrund sind die Dienste designtechnisch so konzipiert,

dass die Nutzer einerseits - meist unbewusst - möglichst viel über sich preisgeben, andererseits von der Nutzung langfristig „abhängig“ gemacht werden, um einen kontinuierlichen Datenstrom zu erzeugen. Denn mit zunehmender Nutzungsdauer werden die erhobenen Daten präziser für den Anbieter. Abschließend darf die finanzielle Kapazität der Plattformen nicht außer Acht gelassen werden, da dieses Mittel für Übernahmen bzw. Fusionen genutzt werden, so dass noch mehr Daten zur jeweiligen Plattform gelangen bzw. fließen. Allein die Marktkapitalisierung von Apple, Amazon, Google, Meta, Microsoft zusammen beträgt mehr als 5,5 Billionen Dollar s. [65]. Zum Vergleich beträgt das Bruttoinlandsprodukt (BIP) von Deutschland 3,33 Billionen EUR s. [66]. Das folgende Schaubild enthält die 100 größten Plattformen weltweit:

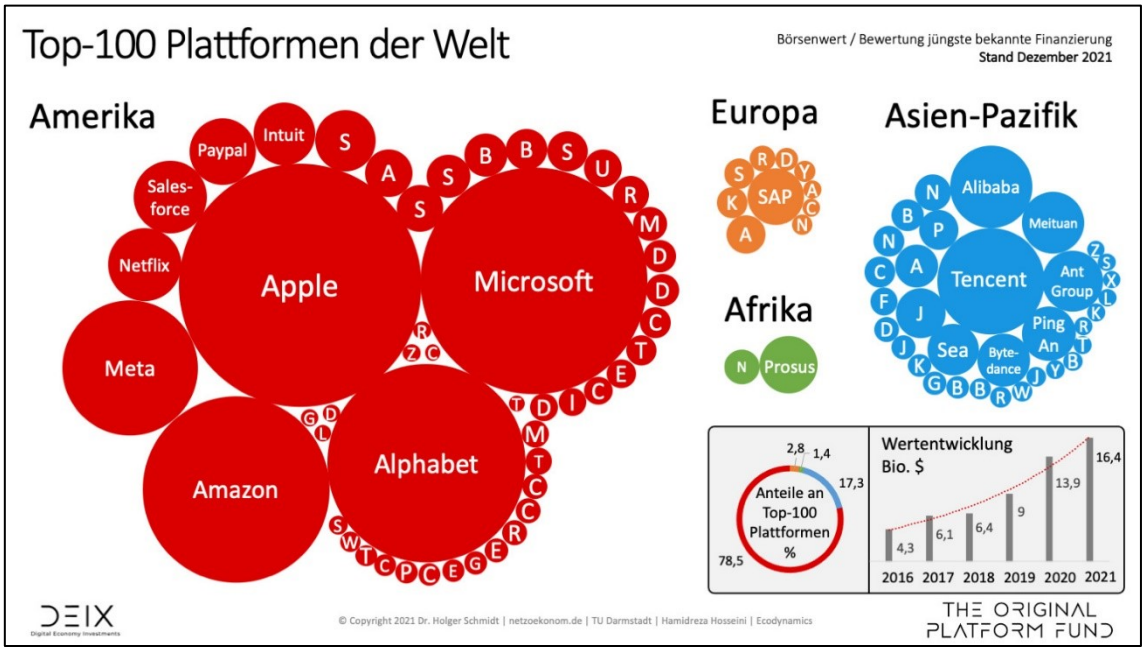


Bild 4: Top100 Plattformen der Welt (Stand: Dezember 2021) [67]

Das o.g. Schaubild zeigt exemplarisch auf, dass Amerika und China sowohl die meisten als auch größten Plattformen vorweisen. Aufgrund ihrer Geschäftsmodelle wird bei Nutzung von deren Diensten insbesondere das Schutzziel Vertraulichkeit gefährdet, so dass von einer Inanspruchnahme abzuraten ist.

3.3 Risiko Daten einschließlich Nutzung von Big Data

Big Data wird wie folgt definiert: „‚Big Data‘ steht für die Verfügbarkeit großer digitaler Datenmengen und deren … Auswertungsmöglichkeiten.“ [68, p. 66]. Dabei zeichnet sich Big Data durch vier Dimensionen aus: die (verfügbare) Datenmenge, die Datenvielfalt (z.B. Bilder, Textdateien), die Geschwindigkeit der Datenverarbeitung sowie der Wert der Daten s. [68, pp. 66-67]. Dabei werden die meisten anfallenden Daten (2/3) von Nutzern erzeugt s. [69, p. 92]. Eine grundlegende Herausforderung ist, dass „wir … in einer Sprachnot [gefangen sind], da wir die allumfassende Digitalisierung nicht verstehen können“ [69, p. VII]. In diesem Kontext hat der ehemalige Chef von Google, Eric Schmidt,

folgende Aussage getätigt: „Ich glaube nicht, dass die Gesellschaft versteht, was passiert, wenn alles zugänglich ist, man alles wissen kann und alles von jedem ständig aufgezeichnet wird.“ [70]. Er geht sogar einen Schritt weiter und meint bei der Nutzung von dessen Diensten: „Ich glaube, dass die meisten Menschen eigentlich nicht wollen, dass Google ihnen ihre Fragen beantwortet. Sie wollen, dass Google ihnen sagt, was sie als nächstes tun sollen.“ [70]. Hinsichtlich der Gefährdung der Privatsphäre hat dieser wie folgt geantwortet: „Wenn es etwas gibt, von dem Sie nicht wollen, dass es irgendjemand erfährt, sollten Sie es vielleicht ohnehin nicht tun.“ [71]. Das Fazit eines Autors dazu: „Der Eintrittspreis [von Googles Diensten] ist die totale Überwachbarkeit.“ [71], was durch Eric Schmidt selbst bestätigt wird: „Wir wissen, wo du bist. Wir wissen, wo du warst. Wir wissen mehr oder weniger, worüber du nachdenkst.“ [72]. Nachfolgend werden Fallbeispiele aufgezeigt, die die Risiken durch die Inanspruchnahme von Big Data Mechanismen aufzeigen.

3.3.1 Risiko Internet der Dinge (IoT)

Das IoT ermöglicht die passive Erfassung personenbezogener Daten durch allgegenwärtige Geräte, wovon Dienstleister und Serviceanbieter dauerhaft profitieren. IoT Geräte sind aufgrund ihres Systemdesigns kaum in der Lage, Anforderungen zum Schutz der Privatsphäre zu erfüllen wie bspw. Hinweise zu geben, dass u.a. personenbezogene Daten Richtung Hersteller fließen s. [73]. „Je nach Messhäufigkeit eines einzelnen Sensors oder ganzer Sensorgruppen ist die Auswertung und abgeleitete Aussage unter Umständen sehr unterschiedlich und kann aufgrund der ableitbaren Informationen über die Nutzerinnen und Nutzer einen unterschiedlichen Schutz der Daten erfordern.“ [74, p. 99]. Als Beispiel sei die Nutzung von Temperatursensoren im Schlafzimmer für die Heizungssteuerung genannt. Wenn die „Temperaturdaten in kurzen Abständen und über einen längeren Zeitraum aus[gewertet werden], kann man sehr genau feststellen, wie viele Personen sich wann und wie lange im Schlafzimmer aufhalten“ [74, pp. 99-100], auch ist eine Aussage darüber möglich „ob diese Personen schlafen oder einer anderen Tätigkeit nachgehen“ [74, p. 100]. Erschwerend kommt hinzu, dass „[m]it dem Fortschritt der Algorithmen zur Auswertung dieser Daten … diese Informationen immer genauer“ [74, p. 100] werden. In diesem Zusammenhang können „[e]inmal gegebene Einverständniserklärungen im Bereich Datenschutz … daher sehr leicht durch Fortschritte bei der Analyse und Verknüpfung von Daten dazu führen, dass ungewollt und vor allem auch unbemerkt neue Erkenntnisse über Nutzerverhalten und - vorlieben möglich sind.“ [74, p. 100]. Darüber hinaus sind „viele Geräte, die … im Smart Home-Umfeld verwendet werden, nicht ausreichend auf die Gewährleistung von Datensicherheit ausgerichtet und gegen Cyberangriffe geschützt.“ [75, p. 12]. Allein die Sicherheitslücke im TCP/IP Stack - als „Ripple20“ [76] bekannt geworden - ermöglicht das Auslesen von Daten bzw. die Ausführung von Remode Code Execution s. [76]. Betroffen sind davon mind. „„hunderte von Millionen“ Geräte“ [76], konkret u.a. Smarthomes, Router, Drucker s. [76]. Ein Sicherheitsupdate ist in der Regel nicht möglich, da eine Updatefunktion nicht implementiert ist s. [76]. Es ist beim Kauf für Nutzer nicht ersichtlich, „wie sicher die …Komponenten der Produkte

sind, noch wie lange der Hersteller den vorhandenen Sicherheitsgrad durch Updates und Wartung aufrechterhalten wird.“ [75, p. 12]. Die Komplexität nimmt durch weitere Smart Home Geräte und der damit verbundenen Vernetzung zu, so dass hierdurch weitere Risiken entstehen können. Daher ist - neben der Ausfallsicherheit - auch eine „ausfallsichere Interaktionstechnik“ [74, p. 101] notwendig, um bei Funktionsstörungen jederzeit eingreifen zu können.

3.3.2 Risiko Standortdaten sowie weitere Identifikationsmöglichkeiten

Selbst wenn Nutzer bei Twitter ihre geografische Position bewusst nicht preisgeben, ist es trotzdem möglich, diese durch deren geposteten Text und deren Freundschaftsnetzwerk den Standort dennoch zu ermitteln s. [77]. Falls die Datensammlung an einigen Stellen zu gering war, können dabei Daten aus anderen sozialen Netzwerken wie Facebook und FourSquare integriert werden s. [77]. Hier wurden „Informationen aus einer Informationsquelle … [entnommen], um andere versteckte Variablen abzuleiten. Der Grad des Erfolgs hängt vom Korrelationsgrad der beiden Informationsquellen ab.“ [77].

Eine Studie aus 2011 zeigt auf, wie allein die Analyse von Webnutzungsdaten zur Entdeckung von Zugriffsmustern der Nutzer führt, um letzten Endes die Navigationspräferenz der Nutzer besser zu verstehen und somit transparent werden s. [78].

Es gibt drei Akteure, die Ortsdaten auswerten können:

1. Mobilfunk-Betreiber - über das Handynetz s. [79, p. 128].
2. Der Hersteller der Betriebssysteme - über WLAN, Mobilfunk, und GPS s. [79, p. 128].
3. Anbieter von Apps - über das Betriebssystem s. [79, p. 128].

Mit Hilfe einer „stillen SMS“ [79, p. 128], die beim Nutzer nicht angezeigt wird, kann eine präzisere Standortermittlung durchgeführt werden s. [79, p. 128]. „Weder die personenbezogene Weitergabe noch die anonymisierte Verwendung der Daten über die Mobilfunkprovider lässt sich unterbinden.“ [79, p. 128], was ein umfangreiches Profil über einen längeren Zeitraum ermöglicht. Bei GPS ist eine Genauigkeit auf bis zu 5 Meter möglich s. [79, p. 128]. Apple, Google und Microsoft nutzen Datenbanken, in denen die Standorte von Mobilfunkmasten und WLAN-Hotspots abgespeichert sind, d.h. jeder neue Mobilfunkmast sowie WLAN-Hotspot wird in die Datenbank eingetragen s. [79, p. 128]. Dies ermöglicht den Konzernen eine Ortung auf mehrere Meter genau zu bestimmen s. [79, p. 128]. Heutzutage kann anhand allein von Bluetooth-Kopfhörern und schnurlosen Headsets, die die gleiche Kennung aussenden, der Standort und die Gewohnheit der Person herausgefunden werden s. [80]. Im Bericht wird ausdrücklich davor gewarnt, diese Geräte mit eigenen Namen zu versehen, da dann die Identifizierung leichter möglich ist s. [80].

3.3.3 Risiko Tracking, Profiling und Beeinflussung in Echtzeit

Das folgende Schaubild illustriert sehr plastisch, wie weit mit Hilfe von Big Data die Auswertungs- und Beeinflussungsoptionen inzwischen geworden sind:

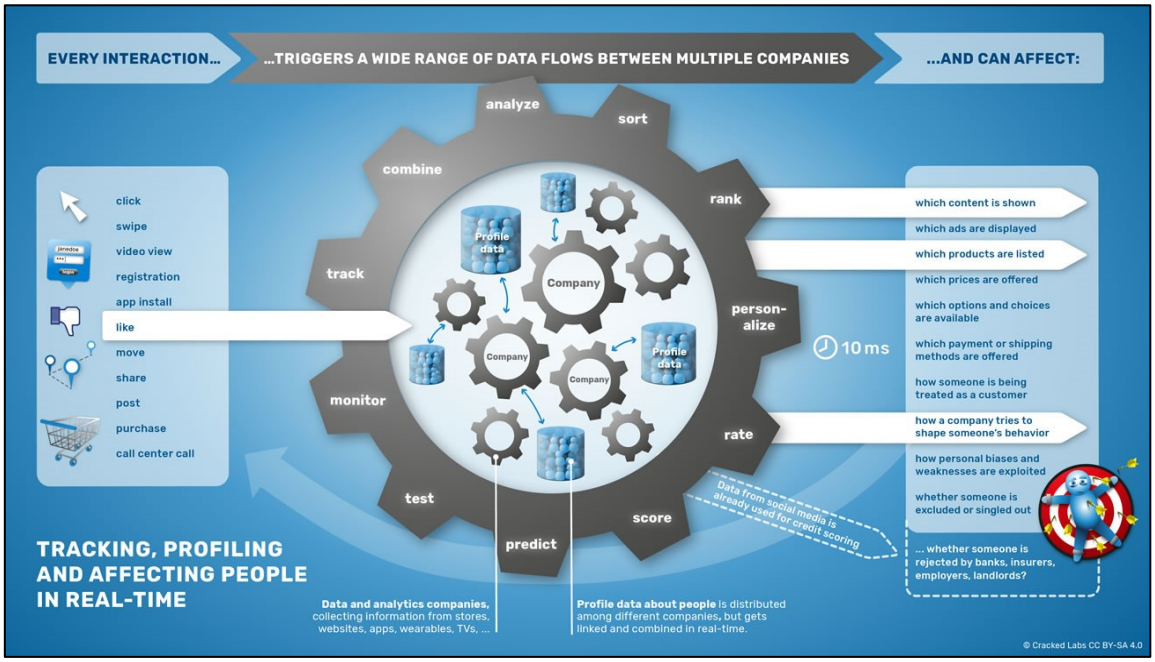


Bild 5: Verfolgung, Profiling und Beeinflussung von Personen in Echtzeit [81]

Im Grunde ist die Essenz im oben genannten Schaubild enthalten, dass „[j]ede Interaktion eine Vielzahl von Datenströmen zwischen mehreren Unternehmen auslöst“[4]. D.h. jede - technische - Interaktion kann analysiert und damit ausgewertet werden, die im Zweifel zu Lasten des Nutzers gehen. Darüber hinaus sind die ausgewerteten Daten i.d.R. nicht für den Nutzer sichtbar, da diese i.d.R. unter das Betriebsgeheimnis der jeweiligen Organisation fallen. Hier ist die Diskrepanz hinsichtlich der Transparenz zwischen den Nutzer und der Organisation am größten, da i.d.R. der Nutzer für die Organisation maximal Transparenz ist, während es im umgekehrten Fall i.d.R. max. Intransparenz bei der Organisation vorherrscht. Das gilt auch für Trackingsdienste, die der Nutzer in der Regel nicht sieht, während umgekehrt - je nach Funktionsumfang - eine maximale Transparenz für Trackinganbieter vorherrscht. Einen kleinen Auszug über die Kategorien, wonach Google trackt, ist im Anhang A gelistet. Facebook hat bereits 2012 mindestens 84 Datenkategorien über jeden Nutzer gespeichert s. [82].

[4] Siehe Bild 5 oben.

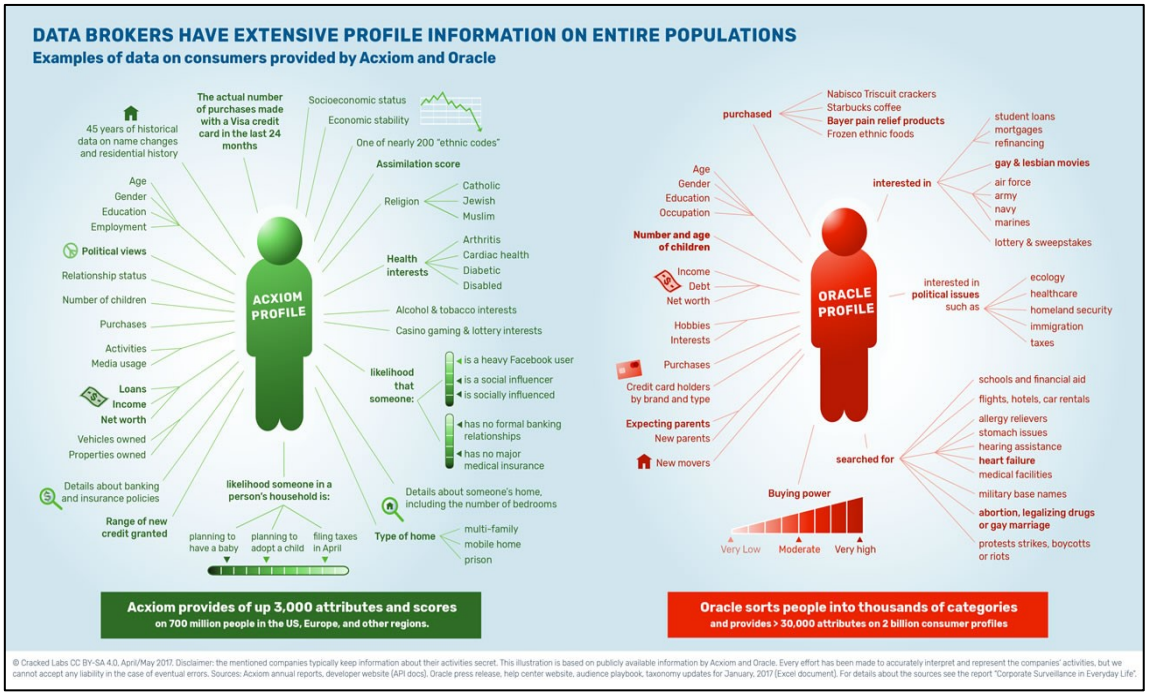


Bild 6: Beispiele von Acxiom und Oracle bereitgestellte Daten über Verbraucher [81]

Die beiden weltgrößten Datenhändler haben in ihren Datensilos mind. 3.000 Attribute pro Person (Acxiom) bzw. über 30.000 Attribute pro Person (Oracle), was aufzeigt, wie tief inzwischen die Auswertungsmöglichkeiten geworden sind und noch weiter ausgebaut werden. Inzwischen ist in diesem Bereich ein undurchschaubarer Industriezweig (einschließlich Infrastruktur) zur Datenextraktion und - analyse entstanden (siehe folgender Auszug eines Schaubildes, was in voller Darstellung im Anhang B enthalten ist).

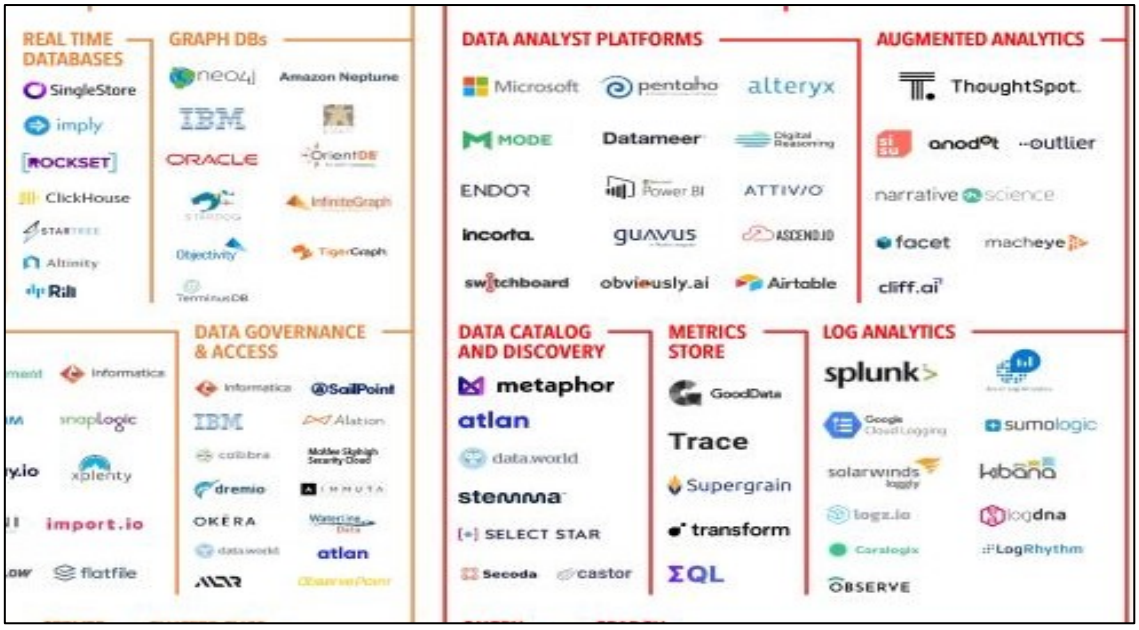


Bild 7: Auszug von einer Gesamtübersicht über Daten- und KI-Firmen [83]

Durch das Vorhandensein von Data Warehouses ist es möglich geworden, dass der Markt für das Daten- und KI-Ökosystem enorm gewachsen ist s. [84]. Dabei werden „Methoden

der datenbasierten Aufmerksamkeitslenkung, Verhaltensvorhersage und - beeinflussung“ [56, p. 17] eingesetzt, die die „Basis des Geschäftsmodells zahlreicher Plattformen“ [56, p. 14] bilden. Das gleiche gilt auch für Suchmaschinen s. [56, p. 14]. Diese Entwicklung bringt unabsehbare Folgen für den Nutzer, da diese Firmen sich i.d.R. bedeckt halten, was ihr jeweiliges Geschäftsmodell genau leisten kann. Somit sind berechtigte Zweifel gegeben, die u.U. zur Nichtnutzung bestimmter Dienste führen kann.

3.3.4 Risiko Gesichtserkennungssysteme

Gesichtserkennungssysteme können leicht ausgetrickst werden. Israelische Forscher haben einen sog. Masterface entwickelt, die jeweils in der Lage sind, mehrere Identitäten zu verkörpern s. [85], s. [86]. Die Forschungsarbeit brachte zum Ergebnis, dass es möglich ist, mit weniger als zehn Mastergesichtern über 40 % bei den derzeit drei führenden Gesichtserkennungssystemen eine Authentifizierung zu erreichen s. [85]. Die Fa. Clearview hat über 10 Mrd. Gesichtsfotos aus dem Internet einschließlich Nachrichtenseiten heruntergeladen. Anschließend lief eine Gesichtserkennungstechnologie darüber, die dann in einer Datenbank hinterlegt wurde s. [87]. Angeblich ist die Firma in der Lage, „[a]nhand nur eines Fotos … sich dann weitere Aufnahmen des gleichen Menschen ausfindig [zu] machen“ [88]. Selbst Kanada oberster Datenschützer scheitert gegen die Firma, weil diese seiner Anordnung - der Löschung der Fotos von kanadischen Bürgern - nicht nachkommt s. [88]. Aus aktuellem Anlass wird ersichtlich, dass damit Missbrauch betrieben werden kann. Die Firma hat der Ukraine 2 Mrd. Bilder aus VKontakte zur Verfügung gestellt, insgesamt sind es 10 Mrd. Fotos s. [89]. Es wird nicht nur bei Gesichtserkennungssystemen bleiben, da weitere Erkennungssysteme wie bspw. „Personen an ihrer Körperform sowie an ihrem Gang erkennen“ [90] von einer chinesischen Behörde bereits benutzt werden. Das Unternehmen Apple misst seit iOS 14 zusätzlich „Gehgeschwindigkeit, Schrittlänge, Gangasymmentrie sowie die Doppelstützzeit.“ [91]. Diese Techniken können miteinander kombiniert werden, so dass die Identifikation zuverlässiger sein wird. Gegen letztgenannte Erkennungssysteme ist eine Fälschung nicht mehr möglich.

3.3.5 Risiko Soziale Medien

Eine Studie hat sich zu Risiken beim Umgang mit Instagram beschäftigt. Instagram gehört der Firma Facebook an und hat sich von einer einfachen Foto-Teilen-Anwendung zu einem Zusammenschluss verschiedener Social-Media-Dienste entwickelt s. [92]. Wer einen Instagram Account besitzt, muss hinnehmen, dass permanent Daten aus den Benutzeraktivitäten wie Beiträge, Kontakte, Direktnachrichten etc. gesammelt werden - insbesondere übergreifend mit der Firma Facebook -, um letzten Endes personalisierte Werbung automatisiert durch einen Algorithmus anzeigen zu lassen s. [92]. Die Herausforderung für Nutzer ist, dass Instagram mit verschiedenen anderen Webseiten von Drittanbietern verknüpft oder abhängig ist, so dass Sicherheitsmaßnahmen wie der Schutz der Privatsphäre ein komplexes Thema ist s. [92]. Bei einer Studie zu Twitter wurde festgestellt, dass es möglich ist, nur anhand von Metadaten die Nutzer zu identifizieren s. [93].

Hier wurde eine Genauigkeit von 96,7 % erreicht, um einen Nutzer aus 10.000 Nutzern zu identifizieren. Die Methodik kann auch auf anderen sozialen Plattformen angewendet werden.

3.3.6 Risiken durch Drohnen

Drohnen sind in erster Linie Datenerfassungsgeräte s. [94]. Die Bedrohung liegt darin begründet, dass Drohnen bislang die einzige Technologie sind, die visuelle Beobachtungen von Räumen in der Wohnung durchführen kann, die sonst der Öffentlichkeit verborgen bleibt s. [94]. Eine effektive Schutzmaßnahme wie Barrieren können die Aufnahmen nicht verhindern, es sei denn, es werden Abwehrtechnologien genutzt, die eher von Firmen bzw. Behörden genutzt wird s. [94]. Häufig wurden Drohnen unerlaubt bei Badelandschaften gesichtet s. [95]. Wenn der Datenfluss in und aus einer Drohne verfolgt wird, können potentiell viele Parteien Zugriff auf die von Drohnen erfassten Daten haben s. [94]. Sobald eine Drohne Daten über eine Person erfasst, hat diese Person de facto keine Option, die Weitergabe und Verbreitung zu verhindern s. [94]. Darüber hinaus kann ggf. der Drohnenhersteller über die Drohnenbetriebssoftware sowie Drittanbieter auch Zugriff auf die Daten haben s. [94].

3.3.7 Risiko Augmented-Reality-Dienste (AR)

Eine weitere Bedrohung sind sog. Augmented-Reality-Dienste (AR). Mit diesen Geräten kann sowohl die Privatsphäre als auch der Schutzbedarf Vertraulichkeit verletzt werden s. [96]. Bei derzeitigen AR-Systemen kann es zum Missbrauch von Sensordaten führen - hier durch Seitenkanäle des Gestensteuerungsgeräts - was Forscher ermöglicht hat, sensible Informationen wie Passwörter, die auf einer Tastatur eingegeben wurden und PIN-Sequenzen, die über einen Touchscreen eingegeben wurden, wiederherzustellen s. [96]. Die Forscher entwickelten einen Algorithmus, der in der Lage war komplexe Passwörter, die aus Kleinbuchstaben, Großbuchstaben, Zahlen und Symbolen bestehen, mit einer Erfolgsrate von 91 % wiederherzustellen s. [96].

3.3.8 Risiko Wearable Technologien

Weitere Bedrohungen sind Wearable Technologien. Wearables sind drahtlose Geräte, die am Körper getragen werden. Die Verbreitung von in Kleidung eingebetteten Geräten, medizinischer Smart Wear, Hautpflastern, Smartwatches und Armbändern zusammen mit Smartphones generiert eine Vielzahl von Informationen, vor allem durch die Kombination von Wearables mit einem Smartphone s. [97]. Durch den technologischen Fortschritt bei den Wearable Technologien hat sich die Anzahl der Risiken erhöht, die die Sicherheit und die Privatsphäre der Benutzer gefährden können s. [98]. Das liegt u.a. an der Verfügbarkeit von GPS-Tracking sowie der Verwendung von Bluetooth Low Energy bei verschiedenen Arten von Produkttypen s. [98]. Hierfür zählen insbesondere folgende Möglichkeiten der Datenfelderhebung: „drahtlose Kommunikation, Tracking, Indoor- und

Outdoorpositionierung, eHealth-Monitoring, Sportanalyse und Gestenerkennung.“ [97]. Dazu gehört die Verwendung von Mikrofonen und Kameras einschließlich der Aufnahmen, was ebenfalls Bedenken der Privatsphäre nicht nur der Benutzer, sondern allen Personen, die sich im Umkreis des Benutzers befinden, hervorruft s. [98]. Ein konkretes Beispiel ist die Smartwatch. Vielen Benutzern sind sich des Umfangs der Daten, die von diesen Geräten gesammelt werden und des damit verbundenen Risikos der Datensicherheit und der Verletzung der Privatsphäre kaum bewusst s. [98]. Smartwatch sammeln u.a. Vitaldaten, Kalenderdaten, Benutzerprofil sowie Audio- und Videodaten, die sowohl für den Benutzer als auch für andere im Umfeld des Benutzers ein Risiko darstellen s. [98]. Darüber hinaus wurde festgestellt, dass Wearables, die u.a. die Herzfrequenz messen, keine genauen Vorhersagen des Wohlbefindens treffen können s. [99]. Denn die Genauigkeit und Validität kann durch die Bewegungen des Wearables negativ beeinflussen werden s. [99]. Daher sind Auswertungen bzw. Vorhersagen von Wearables bislang mit Vorsicht zu betrachten, weil keine wissenschaftlich validen Daten hier vorliegen.

3.3.9 Risiken der dauerhaften Datengenerierung bei Smartphone Nutzung

Über Smartphones werden zahlreiche sicherheitsrelevante Aktivitäten verwendet, z. B. für elektronische Bankgeschäfte und Einkäufe, soziale Netzwerke, das Fotografieren und das Versenden von E-Mails, die Rückschlüsse auf den Nutzer ermöglichen s. [100]. Die Authentifizierung des Kunden ist die erste und bislang meist auch die einzige Verteidigungslinie, um einen unberechtigten Zugriff auf das Mobiltelefon verhindern zu können s. [100]. Bei unbefugten Lauschangriffen können folgende Komponenten infiltriert sein: „systemfremde Anwendungen, Bibliotheken von Drittanbietern und die Ökosystemanbieter selbst.“ [101]. Als Abhörkanal können auch Bewegungssensoren genutzt werden s. [102]. Die Nutzung von Smartphone-Anwendungen selbst hat Auswirkungen auf die Privatsphäre der Nutzer s. [103]. Das prinzipielle Problem ist die Unsichtbarkeit der Verarbeitung sensibler Informationen durch den Nutzer s. [103]. Daher sind diese nicht in der Lage, das Ausmaß der Auswirkungen zu beurteilen, da diese oftmals nicht bewusst sind, dass Anwendungen auf sensible Ressourcen zugreifen und verarbeiten s. [103]. Durch die API haben Entwickler Zugang zu einer Vielzahl von sensiblen Ressourcen und Informationen wie dem aktuellen Standort des Geräts oder die Kontaktdaten des Nutzers s. [103]. Ein negatives Beispiel ist die App von Carrier IQ, die u.a. Tastatureingaben ohne Wissen der Nutzer mitprotokolliert hat s. [104]. Dies gilt erst recht über langfristige Auswirkungen dieser Informationsflüsse. Hinzu kommt die Schwierigkeit, dass der tatsächliche Grad der Auswirkung stark abhängig von den Eigenschaften der spezifischen Ressource ist s. [104]. „Empfindliche Ressourcen können als statisch oder dynamisch, kontextabhängig oder kontext-unabhängig, identifizierend oder nicht-identifizierend oder mit anderen Eigenschaften beschrieben werden“ [104]. Hinzu kommen noch die Variablen Zeitpunkt und Häufigkeit des Zugriffs s. [104]. Wenn eine Anwendung nur einmalig geolokalisiert, kann kein Bewegungsprofil erstellt werden, wenn diese aber alle 30 Minuten 7 Tage die Woche erfolgt, ist es möglich s. [104]. Des Weiteren muss der Aspekt der Kombination von sensiblen Informationsflüssen berücksichtigt werden s. [104]. Aus

diesen Gründen ist es sehr schwierig Nutzer entsprechend zu sensibilisieren, da die Extraktion und Darstellung von verständlichen Informationen komplizierter werden s. [104]. In einer Analyse zu den Auswirkungen auf die Privatsphäre für Android-Apps wurde zu Recht festgehalten, dass Smartphone-Apps die Macht haben, einen Großteil des Privatlebens von Menschen zu überwachen s. [105]. Daher wurde untersucht, wie viele Informationen eine bestimme App auf einem Smartphone abrufen kann und will s. [105]. Die Ergebnisse zeigen auf, dass es „erhebliche Lücken zwischen den Datenschutzrichtlinien und den Privilegienanfragen gibt sowie in einigen Fällen verdächtiges App-Verhalten festgestellt wurde“ [105]. Besonders risikoreich ist die Anwendung von Gesundheits-Apps, da ein Missbrauch persönlicher Gesundheitsdaten prinzipiell möglich ist s. [106, p. 20].

3.3.10 Risiko Überwachung durch Eltern

„Der neue Überwachungswahn im Kinderzimmer“ [107] war der Titel eines Onlineartikels der Welt.de. Darin wird festgehalten, dass die Elektronik den Ratschlag der Großeltern ersetzt mit Hilfe von „alle nur denkbaren Sensoren, Kameras, Mikrofone Richtung Kind zu richten, um den Eltern dieses unbezahlbare Gefühl der Sicherheit zu geben, für das sie bereit sind, bedenkenlos viel Geld auszugeben.“ [107]. Weiter steht im Artikel „Start-ups geben für jede nur denkbare Situation das beruhigende Gefühl, alles unter Kontrolle zu haben - bis der Akku alle ist.“ [107]. Der letzte Teil Satz ist der entscheidende Punkt: Die beste Kontrolle nützt nichts, wenn im entscheidenden Moment der Akku leer ist oder nicht mehr funktioniert. Dies gilt als sog. Single Point of Failure. Auch hier fließen sensible Daten an die Hersteller der Geräte ab. Darüber hinaus sind diese Geräte i.d.R. nicht gut geschützt, so dass bereits in der Vergangenheit eine unbefugte Fremdnutzung möglich war. Ein weiteres erhebliches Risiko ist die Nutzung von sog. Spy-Apps, die Eltern es ermöglicht, alle Daten vom Smartphone des Kindes einsehen zu können einschließlich GPS-Tracking s. [108].

3.3.11 Risiko Medizinische Daten

Ein weiteres Negativbeispiel ist der Umgang mit medizinischen Daten, hier bspw. Röntgenaufnahmen. Die Firma Greenbone hat in einem Bericht festgestellt, dass mehrere hundert medizinische Bildarchivierungssysteme, hier PACS Server (Picture Archiving and Communication Systems), „weltweit ohne jegliche Art von Schutz der auf ihnen gespeicherten persönlichen und medizinischen Daten mit dem öffentlichen Internet verbunden sind.“ [109, p. 3], s. [109, p. 3]. Deutschland war wie folgt betroffen: „[C]a. 15.000 Datensätze von Bundesbürgern öffentlich zugänglich, wobei diesen Datensätzen etwa 2,85 Mio. Bilder zugeordnet sind. Davon sind wiederum 1,38 Mio. abrufbar (ohne Passwort oder Authentifizierung)“ [109, p. 3]. Dies schließt folgende Daten ein: „Namen des Patienten, das Geburtsdatum, das Datum der Untersuchung und einige medizinische Anmerkungen zum Grund der Untersuchung“ [109, p. 3]. In diesem Bericht sind vier Szenarien

aus den geleakten Patientendaten genannt worden, diese sind: Medizinischer Identitätsdiebstahl, Weaponizing von medizinischen Daten, Geldbetrug und Cyber-Kampagnen s. [109, pp. 12-13]. Darüber hinaus besteht die Gefahr der Manipulation von medizinischen Bildern, wie es bereits durch israelische Sicherheitsforscher erfolgreich durchgeführt wurde s. [110]. Diese waren in der Lage gewesen, mit Hilfe von Deep Learning in einem 3D-Scan bspw. Lungenkrebs künstlich entweder einzufügen oder zu entfernen s. [110]. Dies hat - je nach Diagnose - für die Gesundheit des Patienten zum Teil gravierende Auswirkungen. Darüber hinaus wurden mehrmals in der telematischen Infrastruktur des Gesundheitswesens Sicherheitslücken gefunden, die es u.a. ermöglicht hätte, die elektronische Patientenakte zu lesen s. [110]. Besonders schwerwiegend ist es, dass „[i]n mehr als 90 % der Praxen, die an das bundesweite Gesundheitsdatennetzwerk angeschlossen sind, … Sicherheitsrisiken“ [111] gibt. Erschwerend kommt hinzu, dass „[n]eben den Nachrichtendiensten … ein ganzer Zweig der organisierten Kriminalität … medizinische Daten“ [112] sowohl gezielt über das Internet abgreift als auch im Darknet s. [112]. Ein weiteres Negativbeispiel ist das Verhalten des finnischen Psychotherapie-Unternehmens Vastaamo, die - neben der schlechten Absicherung - den Hack über ein Jahr verschwiegen hat s. [113]. Bis zu 40.000 Patienten sind von diesem Diebstahl der Gesprächsinhalte einschließlich ihrer Identitätsdaten betroffen gewesen s. [113]. Auch die Nutzung eines SMS-Beratungsdienstes für Menschen in psychischen Krisen wurden entgegen des Vertraulicheitsversprechen weitergeleitet s. [114]. Ebenso sind Falschaussagen bei Datenschutzerklärungen für Gesundheits-Apps problematisch, wie es zuletzt bei der App Ada der Fall war s. [115].

3.3.12 Risiko Datensammlung durch mobile Fortbewegungsmittel

Anonym Autofahren ist fast nicht mehr möglich. Das fängt bei den Sensoren im Pkw an und geht bis hin über Datenerfassungsgeräte im Straßenverkehr. Gegenwärtig gibt es allein im Pkw bis zu 200 Sensoren und somit können „im Auto pro Minute [bis zu] fünf Gigabyte Daten zur Verarbeitung an[fallen]“ [116], s. [117, p. 148] . Eine Übersicht aller Mobilitätsdaten kann als vergrößertes Bild ebenfalls im Anhang C entnommen werden.

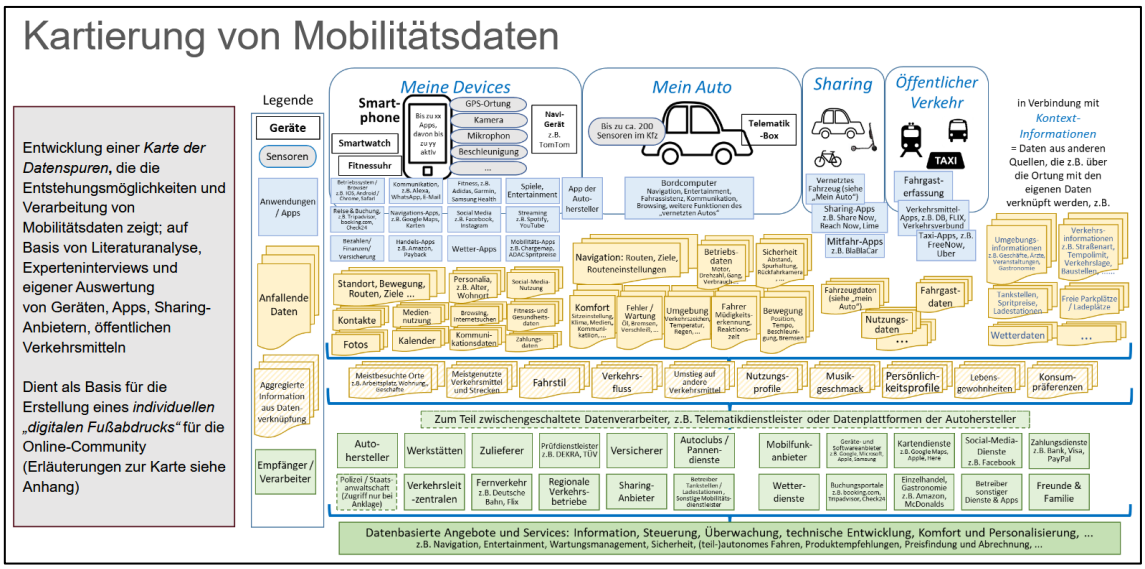


Bild 8: Übersicht aller Mobilitätsdaten [117, p. Folie 24]

Zu den erhobenen Daten gehören neben Betriebsdaten sowie Navigationsdaten u.a. auch „die Erfassung von Vitaldaten der Fahrer, z.B. die Messung der Herzfrequenz über [Elektrokardiogramm]-Sitze“ [117, p. Folie 25]. All die Daten zusammen ermöglichen „Rückschlüsse auf Lebensgewohnheiten, soziale Strukturen oder … auf die Persönlichkeitsstruktur des Fahrers“ [118]. Die EU-Kommission hat in einer Verordnung festgelegt, dass für die Einführung des „On-Board Fuel Consumption Meter“ [119] (OBFCM) eine „Direktübertragung der Daten von Fahrzeugen in regelmäßigen Abständen“ [120] erfolgen soll, u.a. Fahrzeug-Identifizierungsnummer sowie Gesamtfahrstrecke s. [120]. Für diese Verordnung hat die EU-Kommission 2021 einen Big-Brother-Award erhalten s. [121].

Die Gefährdung des Schutzziels Vertraulichkeit gilt genauso auch für sog. Sharingdienste einschließlich der Leihe von Fahrrädern oder Mopeds, die ohne Smartphone als digitalen „Schlüssel“ nicht genutzt werden können.

Als weiteres Negativbeispiel fiel hier der deutsche Autovermieter Buchbinder auf. Bei der Firma waren durch einen Konfigurationsfehler über das Internet ungeschützt Backup-Daten von drei Millionen Kundendaten frei verfügbar gewesen s. [122]. Darin waren über „neun Millionen Mietverträge, von 2003 bis heute“ [122] enthalten gewesen, darunter sind neben „Mietern … auch Fahrer mit Namen, Adresse, Geburtsdatum, Führerscheinnummer und -Ausstellungsdatum aufgeführt“ [122]. Fraglich ist an dieser Stelle, warum die Firma Daten weit über der gesetzlichen Vorgabe aufbewahrt hatte, anstatt diese fristgemäß zu löschen.

3.3.13 Risiko Virtuelle Assistenten

Eine Studie befasste sich mit der Sicherheit und Privatsphäre beim Umgang mit virtuellen Assistenten s. [123]. Derzeit existieren hierzu mehrere Forschungslücken s. [123]. Es gibt zwar Forschungen zum Bedenken der Nutzer, Bedrohungen durch bösartige Angriffe und der Verbesserung der Authentifizierung, aber keine der Studien bietet eine übergreifende

Sichtweise, wie diese Themen zusammenhängen s. [123]. Es ist möglich, anhand der Stimme des Nutzers heraus zu finden, ob dieser unter Depressionen leidet s. [124]. Dies gilt auch für weitere Krankheiten wie Herzerkrankungen s. [125]. Darüber hinaus ist die Infrastruktur hinter einem stimmgesteuerten Lautsprecher sehr komplex und weist somit eigene Risiken auf. Laut eines Forschungsteam ist es mehr als ein „Stack, der für eine Interaktion mit einem Amazon Echo erforderlich ist, [da es] weit über den vielschichtigen 'technischen Stack' von Datenmodellierung, Hardware, Servern und Netzwerken hinausgeht" [126]. Es hat daher System, dass „die wahren Kosten - Sozial, Umwelt, Wirtschaft … - verborgen sind" [126]. Als Negativbeispiel hat Amazon Echo „unbemerkt ein Privatgespräch eines Ehepaares aufgezeichnet und an einen Arbeitskollegen" [127] gesendet. Vor diesem Hintergrund kann einer anderen Studie gefolgt werden, die die Sicherheit und Privatsphäre von Smart Speakern-Nutzern prüfte und feststellte, dass sog. Offline-Smart-Speaker fast alle Sicherheits- und Datenschutz Risiken beseitigten, die mit Cloud-Smart-Speakern verbunden sind s. [128].

3.3.14 Risiko Beherbergungsstätte

Nach dem Bundesmeldegesetz (BMG) - § 30 Besondere Meldescheine für Beherbergungsstätten - sind Beherbergungsstätten verpflichtet, Meldedaten zu erheben. Des Weiteren fallen je nach Beherbergungsstätte weitere Daten wie Zahlungsdaten, Videoüberwachung, der Anlegung von Gästeprofilen, welches folgende Daten beinhalten kann, wie Ess- und Schlafgewohnheiten, Freizeitaktivitäten, Begleitpersonen sowie die Inanspruchnahme von Hotelleistungen wie Wellness,- Ausflugs- oder Transportangebote s. [129]. All die eben genannten Daten werden unabhängig von der Löschfrist für das Meldeformular länger gespeichert und stellen somit ein erhebliches Risiko für die Bürger dar, die Beherbergungsstätten nutzen. Bei der Hotelkette Marriott wurden Daten von bis zu 500 Millionen Hotelgästen abgegriffen, wovon ein Teil sogar noch sensiblere Daten wie bspw. Passnummer und Geburtsdatum enthielten s. [130].

3.3.15 Risiko Freiwillige Preisgabe von privaten Informationen für die Gesellschaft

Die sog. freiwillige Preisgabe von Informationen hat langfristig negative Folgen. Bspw. hat die freiwillige Nutzung von Blackboxes in Autos, um an preisgünstigere Versicherungsmodelle zu gelangen, negative Begleiterscheinungen für die Gesellschaft s. [131]. Zum einen hat der Autofahrer weniger Privatsphäre durch die permanente Überwachung seitens der Versicherung, zum anderen müssen andere Autonutzer, die dies bislang freiwillig nicht mitnutzen, mehr für ihre Privatsphäre zahlen s. [131]. Diese Vorgehensweise hebt die sog. Solidargemeinschaft auf, wo alle sonst die gleichen Versicherungsrahmenbedingungen hätten. Hiervon profitiert nur der Versicherer - und potentielle Angreifer -, da dieser zum einen mehr Einblick in die Fahrdaten der Autofahrer erhält und zum anderen mehr Kosten einspart. Dies gilt auch analog für andere Lebensbereiche, wie Krankenversicherungen etc.. Hier muss seitens der DSGVO noch nachgesteuert werden, damit

diese Vorgehensweise der Anbieter nicht zu Lasten der Solidargemeinschaft bzw. Gesellschaft geht.

3.3.16 Zwischenfazit

Folgende Risiken entstehen bei Nutzung von Diensten bzw. Services, die Big Data als Teilprozess nutzen.

Durch die Zunahme der unterschiedlichen Datenarten und -mengen ist eine Überwachung in Form eines „lückenlose[n] Persönlichkeitsprofil[s]“ [68, p. 33] möglich, welches das Schutzziel Vertraulichkeit - hier Verlust der Privatsphäre - verletzt. Auch scheinbar anonymisierte Daten kann mit Hilfe von Big Data wieder de-anonymisiert werden s. [68, p. 33]. Dieser Umstand wird verschärft durch Anbieter, die Trackingdaten kaufen bzw. verkaufen und durch die Zusammenführung von verschiedenen Datenquellen - einschließlich anonymisierter Daten - eine Identifizierung von Nutzern dadurch ermöglichen s. [132, p. 35]. Die Konsequenz ist ein Kontrollverlust, weil nicht nachvollzogen werden kann, welche Daten über den Nutzer gespeichert werden bzw. sind s. [68, p. 33]. Dies gilt vor allem für automatisierte Entscheidungen, in dem aufgrund von mangelnder Datenqualität u.a. es zu falschen Ergebnissen kommen kann s. [68, p. 33]. Darüber hinaus besteht die Gefahr von negativen Verteilungseffekten durch die individualisierte Preisbildung, so dass Nutzer u.U. mehr zahlen müssen als notwendig s. [68, p. 33]. Des Weiteren kommen Lock-In-Effekte zustande, bspw. durch Facebook, in der keine plattformübergreifende Kommunikation möglich ist - bspw. von Whatsapp zu Threema - s. [68, p. 33]. Schließlich ist die digitale Daten- und Machtkonzentration durch Gatekeeper wie Alphabet zu nennen, die durch exklusive Datenzugänge Netzwerkeffekte gleich mitnutzen s. [68, p. 33]. Hinzu kommt eine „Zahlengläubigkeit“ [133, p. 14] bei dem Anbieter hinzu, so dass Betroffene „ihre >>Unschuld<< nachweisen … müssen.“ [133, p. 14], wenn bspw. Betroffene Kredite beantragen wollen, aber nicht bekommen, da diese ein “hohes“ Risiko für die Bank darstellen s. [133, p. 14]. An dieser Stelle wird beim letzten Beispiel besonders deutlich, dass Entscheidungen, die auf die Zukunft des Betroffenen auswirken - z.B. ein Hauskredit beantragen - nicht allein den Datenunternehmen überlassen werden darf, die die Banken als Quelle u.a. nutzen. Durch die erhobenen Daten „ist … nicht nur die Kontrolle von einzelnen Individuen [möglich], sondern auch die umfassende Überwachung von Menschengruppen oder gar ganzer Gesellschaften. Die Kontrolle wird durch diejenigen ausgeübt, die die Hoheit über die Daten haben.“ [134]. Die Nutzer „haben allenfalls als Datenlieferanten Einfluss, manchmal nicht einmal das, wenn die Erfassung heimlich oder unbewusst erfolgt.“ [134]. Von allen aufgeführten Risiken sind Gesichtserkennungssysteme mit am schwerwiegendsten, weil damit eine flächendeckende Überwachung möglich ist und somit die anonyme Bewegungsfreiheit in der Öffentlichkeit erheblich eingeschränkt wird. Zudem kann der Nutzer bei jeglicher Art von Kamerasystemen nicht mehr unterscheiden, ob diese Gesichtserkennungssysteme einsetzen oder nicht. Dies schließt auch unerlaubte Zugriffe auf Kamerasysteme durch Angreifer mit ein. Danach sind die Risiken der dauerhaften Datengenerierung durch Smartphonenutzung - die

vergleichsweise weniger Schutzmöglichkeiten als Notebooks/PC‘s vorweisen - in Kombination mit Tracking, Profiling und Beeinflussung als schwerwiegend zu betrachten. Denn durch die Nutzung des Smartphones ist es möglich, einen dauerhaften Datenstrom zu erzeugen, die alle Lebensbereiche des Nutzers einschließen und somit in Kombination mit Big-Data-Mechanismen einen umfassenden Einblick ermöglicht und damit Vorteile für - meist unbekannte - Organisationen weltweit verschafft. Dies gilt auch analog für virtuelle Assistenten, gefolgt von IoT-Geräten, da letztere i.d.R. ungeschützt sind und ebenfalls einen Einblick in den Haushalt des Nutzers erlauben. Zudem sind die Risiken sowie die damit verbundenen Auswirkungen insgesamt undurchschaubarer geworden, weil die Organisationen, die Big Data einsetzen, i.d.R. Intransparenz agieren und somit kann keine vollständige Risikoeinschätzung vorgenommen werden. Dieser Trend wird sich in Zukunft zu Lasten der Nutzer noch weiter verschärfen, da neue Analysemöglichkeiten entstehen, die eine - de facto - vollkommende Transparenz der Nutzer ermöglichen werden. Die Datenminimierung ist die derzeitig einzige wirksame Schutzmöglichkeit dagegen.

3.4 Künstliche Intelligenz

Das BSI versteht unter Künstliche Intelligenz (KI) „die Technologie und die wissenschaftliche Disziplin, die mehrere Ansätze und Techniken wie zum Beispiel maschinelles Lernen … und die Robotik“ [135] beinhaltet. Darüber hinaus sind „KI-Systeme … Software- und Hardwaresysteme, die Künstliche Intelligenz nutzen, um in der physischen oder digitalen Welt „rational“ zu handeln“ [135]. Laut dem Gutachten der Datenethikkommission sind Daten „beliebig vervielfältigbar“ [136, p. 83], so dass es fast keine Möglichkeit besteht, diese von dritter Seite wieder zurückzuholen s. [136, p. 83]. Darüber hinaus bestehen „zahlreiche … und vielfach unbemerkt bleibende ... Angriffsmöglichkeiten von außen“ [136, p. 83]. Auch können Gefährdungen durch das System selbst entstehen [137, p. 43]. Laut BSI gibt es derzeit vier relevante KI-spezifische Angriffe (Evasion/Adversarial Attacks, Data Poisoning Attacks, Privacy Attacks, Model Stealing Attacks) s. [138, p. 5].

Laut Atlas der Automatisierung bereiten ADM-Systeme[5] bereits Entscheidungen zu Themen der Migration (Asssistenzsysteme des Bundesamtes für Migration und Flüchtlinge), Kriminalität und Terrorismus (Kamera- und Internetverkehrsüberwachung, automatische Grenzkontrollen) sowie Krieg (autonome Waffensysteme) mit vor s. [139, p. 36]. Ein Negativbeispiel ist die Anwendung von Gesichtserkennungssoftware am Berliner Bahnhof Südkreuz, deren Erkennungssystem bis zu 600 fälschliche Identifikationen am Tag hervorruft s. [140]. Darüber hinaus versagt die Erkennungssoftware bereits nur durch das Wegdrehen des eigenen Gesichtes „um mehr als 15 Grad von der Kamera“ [140]. Hinzu

[5] ADM-Systeme: Systeme „automatisierter Entscheidungsfindung (automated decision making)“, welches sich „aus folgenden Bestandteilen zusammensetzt: Entscheidungsfindungsmodell, Algorithmen […], Datensätze […]“ und „dem gesamten politischen und wirtschaftlichen Ökosystem“ [139] aus S. 46.

kommt die Gefahr der Abhängigkeit zum Anbieter seitens der Behörden, wenn diese KI Systeme einsetzen, die sie selbst nicht verstehen s. [141]. Weitere Diskriminierungen durch Algorithmen können bei Bewerbungen stattfinden (Bsp.: Amazon, in der Männer ggü. Frauen bevorzugt wurden), Werbung auf Online-Suchmaschinen (es werden Schwarze Menschen häufiger mit einem Haftbefehl in Verbindung gebracht als Weiße), Preis- und Suchdiskriminierung im Internet (Renditeerhöhung durch Beschaffung von Wohnortsdaten, verwendetes Gerät etc.), Planung von Polizeieinsätzen/Predictive Policing (häufigere Besuche bei sog. Brennpunktvierteln), Profiling (Schwarze Menschen erhalten eine schlechtere Prognose als Weiße) s. [142, pp. 6-7]. Weitere Gefährdungen sind „Deepfakes" [143]. Mit Hilfe von neuronalen Netzen ist es möglich, Fälschungen von Fotos, Videos einschließlich von Stimmen sowie Texten in hoher Qualität durchzuführen s. [143]. Daraus können sich folgende Bedrohungen ergeben: Überwindung biometrischer Systeme, Social Engineering mit Hilfe von Deepfake, Desinformationskampagnen sowie Verleumdung s. [143]. Gegenmaßnahmen gegen diese Bedrohungen können „nicht in allen Situationen angewendet werden können und in der Regel [bietet es derzeit] keinen vollständigen Schutz" [143].

Zwischenfazit

Aus den o.g. Gefährdungen wird sichtbar, dass hier nicht nur die drei Schutzziele betroffen sind, sondern darüber hinaus auch Authentizität. Selbst die ENISA warnt vor dem Einsatz von KI, denn „[d]ie Bedeutung und die Auswirkungen der KI in der heutigen Gesellschaft können nicht überbewertet werden" [144]. Deswegen ist eine „[a]usreichende Informationssicherheit, die eine breite Palette von Maßnahmen auf unterschiedlichen Ebenen umfasst, … eine notwendige Voraussetzung für vertrauensvolles Handeln in der Datengesellschaft." [136, p. 83]. Die derzeitigen Rahmenbedingungen bei KI sind, dass es „keine hinreichend geeigneten Standards, um die Sicherheit von KI-Systemen für kritische Anwendungskontexte (… z.B. … Automobil- und Rüstungsindustrie, … Biometrie, im Gesundheitswesen sowie im Finanz-, IT- und Telekommunikationsbereich vorliegen können) verlässlich zu bewerten und technisch zu prüfen" [138, p. 8] gibt. Darüber hinaus fehlen noch „wirksame Gegenmaßnahmen gegen KI-spezifische Angriffe" [138, p. 8]. Dies gilt auch für die „Erforschung von Methoden der Transparenz und Erklärbarkeit" [138, p. 8]. Zudem ist die Technikfolgenabschätzung bei KI schwierig, da diese sich durch maschinelles Lernen ändert s. [145, p. 31]. Insbesondere muss konstatiert werden, dass hier das strukturelle Ungleichgewicht zwischen dem Nutzer und der Organisation, die KI anbietet, ungleich höher liegt, denn letztere verfügt - als zwingende Voraussetzung - über einen größeren Datenvolumen und ist somit strategisch im Vorteil aufgrund der Auswertungs- und Bearbeitungsmöglichkeiten, die zu Lasten der Nutzer gehen können. Die Informationsasymmetrie wird deswegen weiter zu nehmen. Daher „bergen die heute schon vorhandenen Daten ein riesiges Machtpotenzial. Fortschritte in der KI werden es diejenigen, die Zugang zu den Daten haben, in immer größeren Umfang erlauben, dieses Machtpotenzial auszuschöpfen." [146, p. 32]. Auch kann der Nutzer das „[s]peichern möglichst aller Rohdaten der Netzwerkpartner und Auswertung an anderer

Stelle“ [147, p. 43] sowie die „absichtliche oder unbeabsichtliche Weitergabe [von Daten] an Dritte“ [147, p. 43] und die „Verwendung unseriöser Webhoster“ [147, p. 43] nicht prüfen, geschweige denn unterbinden. Dies gilt erst recht für Entscheidungen seitens der KI, die für den Nutzer i.d.R. nicht transparent erfolgen kann bzw. erfolgt. Damit ist auch die Beweislast für den Nutzer schwieriger, falls die KI fehlerhaft oder voreingenommen entschieden hat. Als Beispiel sei die Möglichkeit genannt, dass KI „von einem totalitären Staat genutzt [werden kann], um kritische Stellungnahmen ausfindig zu machen und zu eliminieren.“ [148] oder in China mit Hilfe von „ca. 200 Millionen Überwachungskameras, die mit … Gesichtserkennungssoftware [laufen, um] u.a. die ethnische Zugehörigkeit der erfassten Personen automatisch“ [146, p. 33] zu erkennen, um damit bspw. die Uiguren zu verfolgen s. [146, p. 33]. Das Gesamtfazit lautet, dass „weitere Fortschritte in der KI-Forschung noch deutlich mehr Möglichkeiten eröffnen, Menschen zu kontrollieren.“ [146, p. 34].

3.5 Psychologische und gesundheitliche Rahmenbedingungen

Aufgrund der Vielzahl an digitalen Diensten konkurrieren viele Organisationen - hier vornehmlich die Technologieplattformen - um die Aufmerksamkeit der Nutzer. Vor diesem Hintergrund ist von einer Aufmerksamkeitsökonomie[6] die Rede, da es sich um einen Wettlauf um die menschliche Aufmerksamkeit handelt. Dieser Wettlauf bleibt nicht ohne Folgen für Bürger, wenn diese - auf langfristige Art - die jeweiligen digitalen Angebote nutzen. Die ersten fünf Kapitelüberschriften sind dem Center for Humane Technology entnommen worden, die sich mit potentiellen Schäden bei Nutzung von digitalen Technologien beschäftigt. Die dazugehörigen Abschnitte orientieren sich stattdessen an den Primärquellen - hier Fachliteratur -. Folgende Risiken entstehen bei der Nutzung von Onlinediensten:

3.5.1 „Fehlinformationen, Verschwörungstheorien, Falschnachrichten“ [149]

Falschnachrichten verbreiten sich schneller als echte Nachrichten s. [150]. Ärger/Wut ist die Emotion, die sich im Vergleich zu allen anderen Emotionen am schnellsten und am weitesten in den sozialen Medien verbreitet s. [150]. Darüber hinaus kommen weitere Risiken hinzu, dass Inhalte, die über die Social-Media-Plattformen verbreitet werden, auch von Bots s. [151][7], weiterverbreitet werden. Die treibende Kraft dahinter, ob jemand eine Information teilt, ist nicht deren Richtigkeit oder sogar deren Inhalt, sondern weil es

[6] Def.: Aufmerksamkeitsökonomie: „Die Ökonomie der Aufmerksamkeit ist ein ökonomischer Ansatz, der menschliche Aufmerksamkeit als knappe Ressource begreift.“ [390].

[7] Def.: Bots: „Social Bots sind Bots, also Softwareroboter bzw. -agenten, die in sozialen Medien (Social Media) vorkommen. Sie liken und retweeten, und sie texten und kommentieren, können also natürlichsprachliche Fähigkeiten haben. Sie können auch als Chatbots fungieren und damit mit Benutzern synchron kommunizieren.“ [151].

von einem Freund kommt s. [152]. Dies begünstigt in digitalen sozialen Medien sog. Echokammern, die durch gleichgesinnte Freunde ermöglicht wird s. [149].

3.5.2 „Verlust wichtiger Fähigkeiten wie Gedächtnis und Konzentration“ [149]

Gezielt werden durch die Technologie Nutzer ständig unterbrochen und abgelenkt, was auf Dauer ihren Tribut fordert s. [149]. Eine Studie hat Meta-Analysen vorgenommen mit dem Ergebnis, dass starke Medien-Multitasker - im Gegensatz zu Personen, die weniger Medien-Multitasking betrieben - schlechtere Leistungen zeigen s. [153]. Häufige Unterbrechungen seitens der digitalen Geräte kosten die Aufmerksamkeit des Nutzers und es dauert länger eine Aufgabe zu erledigen bzw. ist mit einer höheren Fehlerquote verbunden s. [154]. Eine Unterbrechung von weniger als 3 Sekunden aus, um die Fehlerquote zu verdoppeln s. [154]. Folgende Faktoren stärken die Intensität der digitalen Ablenkung: „Aufmerksamkeitsimpulsivität, Internetsucht und gewohnheitsmäßige Technologienutzung“ [155].

3.5.3 „Stress, Einsamkeit, Gefühl der Abhängigkeit, erhöhtes riskantes Gesundheitsverhalten“ [149]

Eine Studie fand an Teenagern heraus, dass die Nutzung der sozialen Medien kognitive Auswirkungen wie das Aufmerksamkeitsdefizitsyndrom auslösen kann s. [156]. Eine weitere Studie stellt fest, dass es einen Zusammenhang zwischen einer intensiven sozialen Mediennutzung und einer Verringerung des Gehirnvolumens gibt s. [157].

Die Nutzung von Instagram durch weibliche Personen führt zu negativen Erfahrungen. Die Darstellung gegenüber dünnen Idealbildern führte zu einer größeren Körper- und Gesichtsunzufriedenheit als durchschnittliche Bilder s. [158]. Verschärfend kommt hinzu, dass je mehr Zeit auf Instagram verbracht wird, desto höher dann die Wahrscheinlichkeit ist, dass diese unter Essstörungen wie Orthorexia nervosa leiden s. [159].

Eine Studie fand heraus, dass bei Vorliegen von Neurotizismus eine erhöhte sozialen Medien Nutzung vorausgesagt werden kann s. [160].

Auch der Aspekt der elektronischen Mediennutzung vor dem Schlafengehen wurde untersucht. Die Nutzung elektronischer Medien war negativ mit der Schlafdauer und positiv mit Schlafstörungen verbunden, die wiederum mit depressiven Symptomen zusammenhingen s. [161].

3.5.4 „Propaganda, verzerrte Dialoge und ein gestörter demokratischer Prozess“ [149]

Forscher konnten in Amerika nachweisen, dass Nutzer von YouTube durchgängig von moderaten zu extremeren Videos wechseln s. [162]. Da das Empfehlungssystem von Youtube die Nutzer zu politisch extremen Inhalten lenkt, ist der Begriff ‘Radikalisierungspipeline‘ in diesem Zusammenhang entstanden s. [162].

Selbst die Reihenfolge der Ergebnisse, die in Suchmaschinen angezeigt werden, hat einen starken Einfluss auf die politische Meinung der Nutzer, wie eine Studie herausfand s. [163]. Nur wenigen Menschen sind sich der Verzerrungen in den Suchmaschinenergebnissen bewusst und wie sich dadurch ihre eigene Wahl für einen politischen Kandidaten verändert hat s. [163]. Dies kommt dadurch zustande, dass Nutzer höher gerankten Ergebnissen mehr vertrauen als niedriger gerankte Ergebnisse s. [163]. Der Einfluss ist besonders groß in Ländern, die von einem einzigen Suchmaschinenunternehmen dominiert werden s. [163]. Dies trifft in Deutschland insbesondere bei Google zu, da diese Firma nicht nur hier Marktführer ist.

3.5.5 „Verstärkung von Rassismus, Sexismus …“ [149]

„Informationsumgebungen haben die Macht, die Wahrnehmung und das Verhalten von Menschen zu beeinflussen“ [164]. Laut Dr. Safiya Umoja Noble findet Datendiskriminierung statt s. [165]. Darin wurde als Beispiel des Suchbegriffs „schwarzes Mädchen“ auf Google aufgezeigt, dass hier als Ergebnis mehr sexuell explizite Begriffe bei den Top-Suchbegriffen angezeigt werden im Gegensatz zum Suchbegriff „weißes Mädchen“, in dem die Ergebnisse ganz anders ausfallen s. [165].

Darüber hinaus kommt die Besonderheit, dass Menschen online mehr über sich freigeben als im persönlichen Gespräch - von Angesicht zu Angesicht - tun würden. Dieses Phänomen wird als „Online-Enthemmungseffekt“ [166] bezeichnet. Eine der Ursachen liegt darin, dass durch soziale Normen in einer Online-Umgebung sich entblockiert fühlt s. [167].

3.5.6 Risiken durch die digitale Medienwelt

Online-Medien streben danach die Zeit und die Aufmerksamkeit der Nutzer zu steuern s. [168]. Es wurde herausgefunden, dass die Steuerung des Onlinepublikums über offene Empfehlungen und das Selektieren von Webseiteinhalten auch weniger sichtbare Mechanismen einbezieht, um Nutzer zu beeinflussen s. [168]. Hier besteht die Gefahr, dass Nutzer auf subtile Weise in Richtungen gebracht werden, die nicht ihren Präferenzen entspricht, so dass es mit der Zeit möglich sein kann, Einstellungen und Verhaltensweisen auszuüben, die sonst anderseits nicht existieren würde s. [168]. Die Ergebnisse dieser Studie liefert systematische Beweise, dass Online-Auswahl-Architekturen die Nutzer tatsächlich beeinflussen s. [168]. Eine Handvoll Plattformen haben unverhältnismäßig viel Macht durch die Kalibrierung von Schnittstellen für verschachtelte Anwendungen und durch die strategische Partnerschaft erlangt, um Nutzer an sich zu binden „(locking-in)“ [168], s. [168]. Sie funktionieren als geteilte, unverzichtbare Dienste wie öffentliche Versorgungseinrichtungen s. [168]. „Digitale Medien kolonisieren jeden Teil des modernen Lebens.“ [168]. Die Institutionen „steuern subtil den Fluss der öffentlichen Aufmerksamkeit auf Informationen, Unterhaltung und Kommerz. Sie sind unsichtbare Entscheider auf dem Marktplatz der Ideen und darüber hinaus.“ [168].

3.5.7 Suchtgefahr steigt mit längerer Smartphone Nutzung

Eine Metaststudie zur Mobiltelefonsucht fand heraus, dass die Sucht im Zusammenhang mit Persönlichkeitsvariablen wie Extraversion, Neurotizismus, Selbstwertgefühl, Impulsivität, Selbstidentität und Selbstbild in Verbindung steht s. [169]. Darüber hinaus wurden Schlafstörungen, Angst, Stress und in geringem Maße Depressionen ebenfalls mit problembehafteter Mobiltelefonnutzung nachgewiesen s. [169]. Sowohl Internet- als auch Handy-Missbrauch sind verbunden mit Problemen des Selbstwertgefühls, des Selbstkonzeptes und des Neurotizismus s. [169].

Folgende Warnzeichen sprechen für eine Smartphone Abhängigkeit:

- „Isolation von Familie und Freunden
- Verheimlichung der Smartphonenutzung
- Angst haben, etwas zu verpassen (Fear of missing out [FOMO])
- Gefühl des Schreckens, der Angst oder der Panik, wenn das Smartphone liegen bleibt, der Akku leer ist oder das Betriebssystem abstürzt“ [170].

3.5.8 Risiko Dark Pattern

Dark Pattern führt den Nutzer zu Handlungen, die nicht in dessen Interesse sind. „Dark Pattern sind Benutzeroberflächen, deren Design - Weboberfläche oder als App - Benutzer absichtlich verwirren, es den Benutzern erschweren, ihre tatsächlichen Präferenzen auszudrücken oder Benutzer manipulieren, damit diese bestimmte Handlungen ausführen“ [171]. Dark Pattern nutzt in der Regel kognitive Verzerrungen aus und veranlassen Benutzer zum Kauf von Waren oder Dienstleistungen, die sie nicht wünschen und/oder zur Preisgabe von persönlichen Informationen, die sie sonst nicht herausgeben würden s. [171]. Es wurden folgende Dark Patterns identifiziert, die am meisten wirkten: versteckte Informationen, Trickfragen und Ablenkungs- bzw. Verzögerungsstrategien sind Mittel, die Benutzer mit hoher Wahrscheinlichkeit erfolgreich manipulieren s. [171]. Mit versteckten Informationen ist gemeint, dass Optionen oder Aktionen für den Benutzer relevant sind, nicht sofort oder leicht zugänglich gemacht wird, z.B. ist in einem langen Text eine Opt-Out Funktion als kleines Kästchen versteckt, was für den Benutzer relevant wäre s. [172]. Dunkle Muster variieren in Designelementen (z.B. Bildmaterial, Text), in Designattributen (z.B. asymmetrisch, verdeckt, trügerisch) und ihren Auswirkungen (individuelle Wohlergehen und Benutzerautonomie) s. [173]. Insgesamt gibt es derzeit 22 Typen von Dark Pattern, die in verschiedenen Webprodukten oder Services verwendet werden s. [174]. Hier kann an dieser Stelle ausgeschlossen werden, dass es in Zukunft nicht weniger wird, sondern im Gegenteil zukünftig weitere Arten von Dark Pattern geben wird.

3.5.9 Risiko des Missbrauchs von Erkenntnissen zu Persönlichkeitsmerkmalen durch die Forschung

Jeder Charakterzug eines Menschen lässt sich anhand von fünf Persönlichkeitsdimensionen „Big-Five-Modell“ messen: “Offenheit (Wie aufgeschlossen sind Sie gegenüber Neuem?), Gewissenhaftigkeit (Wie perfektionistisch sind Sie?), Extraversion (Wie gesellig sind Sie?), Verträglichkeit (Wie rücksichtsvoll und kooperativ sind Sie?) und Neurotizismus (Sind Sie leicht verletzlich?). Anhand dieser Dimensionen kann man relativ genau sagen, mit was für einem Menschen wir es zu tun haben“ [175]. Im gleichen Artikel aus dem Schweizer Magazin geht hervor, dass durch einfache Onlineaktionen zuverlässige Schlüsse gezogen werden können wie bspw. Männer, die die Kosmetikmarke MAC liken, mit hoher Wahrscheinlichkeit schwul sind oder Lada-Gaga-Follower mit sehr hoher Wahrscheinlichkeit extrovertiert sind im Gegensatz zu Nutzern, die Philosophie liken, eher introvertiert sind s. [175].

In einer Studie zu Big-Five-Persönlichkeitsmerkmalen und Facebook Nutzung fanden Forscher heraus, dass Narzissmus der stärkste Prädiktor für die Zeit ist, die pro Tag auf Facebook sowohl von Studenten als von Nichtstudenten verbracht wurde s. [176]. Wenn beide Partner Facebook nutzen, kann mit Hilfe des Big-5-Modells herausgefunden werden, dass es Zusammenhänge zwischen beziehungserhaltenden Aktivitäten auf Facebook („öffentliche Zurschaustellung und Partnerüberwachung“ [177]) und Facebook bezogenen Beziehungsschwierigkeiten („Konflikt und Eifersucht“ [177]) gibt s. [177].

In einer weiteren Studie fanden Forscher anhand der Eigenschaften des Facebookprofils wie beispielsweise „Größe und Dichte des Freundschaftsnetzwerks, Anzahl der hochgeladenen Fotos etc.“ [178] heraus, dass es eine Korrelation mit der Persönlichkeit nach dem Big-Five-Modell gibt. Durch die Analyse von Informationen aus sozialen Netzwerken kann ein „Profil“ von Individuen erstellt und dann in verschiedene Segmente eingeteilt werden“ [178], so dass gezielte Werbung möglich ist. Darüber hinaus werden immer weitere Zusammenhänge entdeckt. Eine Studie aus Taiwan hat eine Beziehung zwischen der Persönlichkeit und auf Facebook hochgeladenen Fotos entdeckt [179]. Dies gilt auch für musikalische Präferenzen, aus dem die Persönlichkeit (Big-5-Modell) aus aktivem Zuhören und Facebook-Likes Rückschluss gezogen werden kann [180].

Selbst aus Fotos kann durch neuronale Netzwerke die sexuelle Orientierung mit einer Zuverlässigkeit von 81 % geschlossen werden zwischen schwulen und heterosexuellen Männern und einer Zuverlässigkeit von 71 % zwischen lesbischen und heterosexuellen Frauen im Gegensatz zu menschlichen Entscheidern, deren Quote niedriger liegt (61 % bei Männern und 54 % bei Frauen) s. [181].

Verschärft wird es durch eine neuere Studie, in der die Gesichtserkennungstechnologie auch sogar die politische Orientierung enthüllen kann, was durch die DSGVO als besonders schützenswert angesehen wird s. [182]. Die politische Orientierung wurde in 72 % der liberal-konservativen Gesichtspaare korrekt klassifiziert, was noch besser als durch Menschen erkannt wurde (55 %) s. [182]. Die Algorithmen können auch sensiblere Attribute vorhersagen, wie beispielsweise sexuelle Orientierung, Persönlichkeit etc. s.

[182]. Das Problem ist, das digitale Fußabdrücke selbst beeinflusst werden können, was bei einem Gesicht nicht möglich ist bzw. schwer zu verbergen ist, da diese leicht oder verdeckt durch Strafverfolgungsbehörden oder aus digitalen bzw. analogen Archiven, einschließlich sozialer Netzwerke, Dating-Plattformen und Regierungsdatenbanken aufgenommen werden kann s. [182]. Facebook- und LinkedIn Profilbilder sind öffentlich und können von jedem ohne Zustimmung oder das Wissen der betroffenen Person eingesehen werden s. [182]. Selbst wenn man genau wüsste, welche Gesichtsmerkmale die politische Orientierung verraten würden, können Algorithmen schnell lernen, wie sie ggf. relevante Informationen aus anderen Merkmalen extrahieren kann, was letzten Endes ein Wettrüsten darstellt, was der Mensch - auf Dauer - nicht gewinnen kann s. [182]. Der Forscher äußert sich dahingehend pessimistisch, dass der technische Fortschritt wie u.a. die KI mehr möglich macht s. [182]. Diese Möglichkeiten können zukünftig bei Wahlen beispielsweise missbraucht werden s. [182]. „Selbst eine grobe Schätzung der psychologischen Eigenschaften eines Publikums kann die Effizienz der Massenbeeinflussung drastisch erhöhen“ [182].

Selbst Forscher sehen die Notwendigkeit, dass politische Interventionen und Regulationen notwendig sind, wenn es sich hierbei um die digitalen Fußabdrücke von Nutzern, um eine überzeugendere Massenkommunikation zu bewirken, handelt s. [183]. Denn durch bessere Hard- und Software sowie durch fortlaufende Erkenntnisse der computergestützten Sozialwissenschaften können digitale Spuren menschlicher Aktivitäten dafür genutzt werden, um persönliche Rückschlüsse auf die Vorlieben, Gewohnheiten und psychologischen Eigenschaften der Nutzer zu ziehen s. [183]. Die daraus gewonnenen Erkenntnisse erlauben die Anwendung von psychologischem Targeting und machen es möglich, das Verhalten großer Gruppen von Menschen zu beeinflussen, indem persuasive Anreize auf die psychologischen Bedürfnisse der Zielgruppen zugeschnitten werden s. [183]. Dies ermöglicht einerseits dem Nutzer bessere Entscheidungen zu treffen, auf der anderen Seite gibt es potentielle Fallstricke in Bezug auf Manipulation, Datenschutz und Verletzung der Privatsphäre s. [183]. Hier wird explizit auf die Datenschutzbestimmungen hingewiesen, in der „nicht adäquat auf den potentiellen Missbrauch von Online Informationen im Kontext mit psychologischem Targeting“ [183] eingegangen wird s. [183]. In diesem Aufsatz geben die Forscher als Beispiel an, dass es bereits nur aufgrund von Facebook-Likes, Tweets oder Transaktionsdatensätze möglich ist, automatisch und genau auf eine Vielzahl von persönlichen Attributen zu schätzen, einschließlich politischer Ideologie, sexueller Orientierung und Persönlichkeit s. [183]. Hier wird explizit auf die Gefahr hingewiesen, dass „automatisierte Einschätzungen auf der Basis von digitalen Fingerabdrücken nicht nur genauer und weniger anfällig für Täuschungen und Falschdarstellungen sind …, sondern sie können auch Messungen über die Zeit ermöglichen, um zeitliche Trends und intra-individuelle Veränderungen im Verhalten erkennen“ [183].

Als Beispiel kann nur aus durchschnittlich 68 (!) Facebook-Likes folgende Rückschlüsse auf die Persönlichkeit getroffen werden wie es aus dem folgenden Schaubild ersichtlich wird s. [183]:

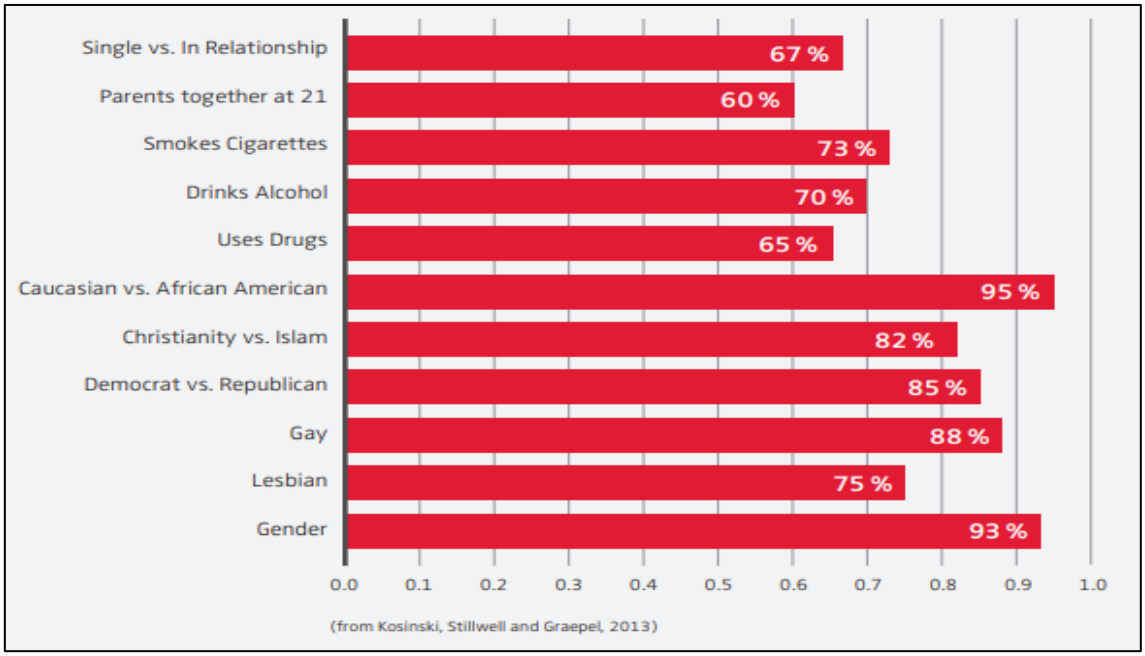


Bild 9: Grad der Zuverlässigkeit über unterschiedliche Kategorien nur aus Likes [183, p. 3]

In diesem Zusammenhang geht aus einem Artikel hervor, dass das Modell von Herrn Kosinski nur „anhand von zehn Facebooks-Likes eine Person besser einschätzen als ein durchschnittlicher Arbeitskollege. 70 Likes reichen, um die Menschenkenntnis eines Freundes zu überbieten, 150 um die der Eltern, mit 300 Likes kann die Maschine das Verhalten einer Person eindeutiger vorhersagen als deren Partner. Und mit noch mehr Likes lässt sich sogar übertreffen, was Menschen von sich selber zu wissen glauben.“ [175].

Manche der o.g. Daten sind sensibel, wie beispielsweise Raucher zu sein. Wenn diese Person zum Zeitpunkt der Antragstellung bei einer privaten Krankenversicherung diesen Status verschwiegen hat, kann dies eine Kündigung nach sich ziehen, wenn es der privaten Krankenversicherungsgesellschaft nachträglich bekannt wird. Nach einem Bericht eines Versicherungsmaklers ist „[d]as Ausspionieren (z.B. Social Media) … nahezu ausnahmslos gerichtlich in Deutschland als zulässig erachtet“ [184] worden.

Ein weiteres Beispiel ist die Analyse von Posts auf Facebook, was wie folgt beschrieben wird: „Zeig mir deine Posts und ich werde wissen, wie du dich fühlst“ [183]. Hier schreiben die Forscher nicht nur explizit die Möglichkeit an, Modelle an Millionen von Menschen anzuwenden, die auf Likes, Posts und Tweets basieren, um ihre psychologischen Eigenschaften genau zu erfassen s. [183]. Sondern auch die Tür für Versuche zu öffnen, große Gruppen von Menschen effektiver zu überreden bzw. große Gruppen von Menschen in Form von psychologischem Targeting effektiver zu beeinflussen s. [183]. Auf der anderen Seite wird in diesem Beitrag auch genau darauf hingewiesen, dass die Vorhersage von persönlichen Attributen aus digitalen Spuren ohne das Bewusstsein und der Zustimmung des Einzelnen erhebliche negative Folgen haben kann s. [183]. „Kommerzielle Unternehmen, staatliche Institutionen oder sogar die eigenen Facebook-Freunde

könnten mithilfe von Software nutzen, um auf Attribute wie Intelligenz, sexuelle Orientierung oder politischen Ansichten zu schließen, die eine Person möglicherweise nicht teilen wollte. In falschen Händen könnten solche Vorhersagen eine Bedrohung für das Wohlbefinden, die Freiheit oder sogar das Leben einer Person darstellen. Psychologisches Targeting könnte zum Beispiel missbraucht werden, um heimlich Schwächen im Charakter eines Menschen auszunutzen und sie zu Handlungen gegen ihr eigenes Interesse zu handeln oder sich auf unmoralische oder ungesetzliche Handlungen einzulassen.“ [183]. Selbst wenn die Absicht in positiver Hinsicht sein wollte und keine Absicht zur Manipulation sowie Datenmissbrauch besteht, können unbeabsichtigte Folgen entstehen und den Verbraucher schaden s. [183]. Hier wurde als Beispiel eine Einzelhandelskette benannt, die Einkaufsdaten von Kunden analysierte und diese u.a. dazu nutzte, um Schwangerschaften der Kundinnen vorherzusagen, um diese zeitlich abgestimmten und gezielten Angebote wie pränatale Vitamine etc. zukommen zu lassen s. [183]. Im schlimmsten Fall könnte die Enthüllung der Schwangerschaft gegenüber dem Partner, Eltern oder anderen Familienmitgliedern das Wohlbefinden oder sogar die Sicherheit der werdenden Mutter bedrohen s. [183]. Auch Schwächen der Regulation zeigen die Forscher am Beispiel der DSGVO auf. Es ist technisch möglich „persönliche Rückschlüsse auch ohne direkten Zugriff auf die Daten des Einzelnen“ [183] ziehen zu können, in dem bspw. Verbraucher verfolgt werden, die auf eine Anzeige klicken oder einen Kauf tätigen s. [183]. Die schärfste Aussage hierzu lautet, dass „keine der derzeit existierenden oder diskutierten gesetzlichen Maßnahmen … vollständig auf die hier beschriebenen Techniken ein[geht]“ [183]. Durch die Nutzung von Erkenntnissen auf Gruppenebene über die Werbeplattform von Facebook ist es möglich, das Verhalten tausender Menschen auf der Basis ihrer psychologischen Eigenschaften zu beeinflussen, was bislang nicht adäquat durch die Datenschutzbestimmungen adressiert wurde s. [183].

Bestätigt wird dies mit der Aussage, dass die Anhäufung digitaler Fußabrücke im Internet es Computermodellen ermöglicht, Analysen nach verschiedenen Zeitlinien durchzuführen und Ergebnisse in verschiedenen Lebensabschnitten eines Menschen zu erzeugen s. [185]. Das Ergebnis basiert auf zehn (oder mehr) Jahren digitaler Fußabdrücke, welches innerhalb weniger Minuten automatisch generiert werden kann s. [185]. Aus einer weiteren Studie über psychologische Zielgruppen als effektiver Ansatz für digitales Massenbeeinflussung wurde feststellt, dass Regierungen, Unternehmen und politische Parteien sog. persuative Techniken nutzen, um Menschen zu einer bestimmten Handlung zu bringen wie bspw. ein bestimmtes Produkt zu kaufen oder für einen bestimmten Kandidaten zu stimmen s. [186]. Daher warnen die Forscher explizit vor den potenziellen Fallstricken in Bezug auf Manipulation und Datenschutz s. [186]. Diese Studie zeigt ebenfalls auch auf, dass Rückschlüsse auf persönliche Vorlieben, Charakteristika auch ohne direkten Zugriff auf die Daten von Einzelpersonen möglich sind s. [186]. Zudem gibt es die Entwicklung, dass immer mehr Verhaltensdaten in Echtzeit gesammelt werden, was es möglich macht, die psychologischen Merkmale von Menschen in einem situativen Kontext zu setzen s. [186].

3.5.10 Gesundheitliche Risiken bei Nutzung von IT-Geräten

Eine weitere Gefahr sind körperliche Beschwerden. Wenn über einen längeren Zeitraum bei nicht korrekter Haltung bspw. das Smartphone genutzt wird, sind Nackenschmerzen eines der Symptome, was wiederum die Wirbelsäule stärker belastet s. [187]. Darüber hinaus ist die Wirkung der zunehmenden und dauerhaften Strahlenbelastung direkt am Körper noch nicht langfristig erforscht. Hinzu fehlt bislang die Technikfolgenabschätzung. Desweiteren sind die langfristigen Auswirkungen des blauen Lichts aus Leuchtdiode (LED) nicht bekannt s. [188]. Vor diesem Hintergrund ist aus präventiver Hinsicht die Nutzung von Bildschirmbrillen zu empfehlen.

3.5.11 Zwischenfazit

Eine der Gründe, warum soziale Medien so erfolgreich sind, ist die Tatsache, dass die Neigung zur Offenlegung privater Gedanken und Gefühle, u.a. daran liegt, dass dies auf einem intrinsischen Wert beruht, der mit der Selbstoffenbarung verbunden ist s. [189]. Zugleich wird das Belohnungszentrum des Gehirns stimuliert, so dass es umgekehrt schwerer fällt, sich nicht zu äußern, um die eigene Privatsphäre zu schützen s. [189]. Zudem erhöht die Gefahr der „digitale[n] Totalvernetzung und Totalkommunikation den Konformitätszwang erheblich. Die Gewalt des Konsens unterdrückt … das Andere, das Unbekannte“ [69, p. 235]. Darüber hinaus führt die „Selbstvermarktung … in Wahrheit [zur] Selbstversklavung“ [190, p. 123], da durch die Preisgabe der persönlichen Daten die sozialen Medienanbieter einschließlich Geheimdienste selbst entscheiden, wie mit diesen Daten umgegangen wird. Jaron Lanier hat die sozialen Medien als „Imperien der Verhaltensmodifkation“ [191] bezeichnet. Insgesamt birgt die Nutzung von sozialen Medien erhebliche Risiken - hier u.a. Manipulation bzw. Steuerung - des Nutzers, ohne sich dabei dessen bewusst zu sein. Darüber hinaus können die sozialen Medienanbieter Erkenntnisse über den Nutzer generieren, die weit über das hinausgehen können, was der Nutzer von sich selbst weiß. Zudem wird es durch die Fortschritte in der Psychologie - unter Einbeziehung von Datenspuren - neue Erkenntnisse geben, die ggf. zu Lasten des Nutzers gehen können. Um ein Missbrauch durch die Nutzung von sozialen Medien vorzubeugen, ist von der Inanspruchnahme jedweder Dienste im Bereich der sozialen Medien abzuraten. Dies gilt auch für datensparsame soziale Medien wie bspw. Mastodon, da hierüber u.a. gegen Scraping keinen Schutz gibt, um zu bestimmten Erkenntnissen zu gelangen. Bei Nutzung von sozialen Medien wird nicht nur das Schutzziel Vertraulichkeit gefährdet, sondern auch die Integrität des Nutzers. Dies geschieht bspw. durch Identitätsdiebstahl oder durch das Bloßstellen von verheimlichten Tatsachen, wie bspw. Homosexualität, die durch die sozialen Medienanbieter zuverlässig erkannt werden können. Zu den größten Risiken zählt die Tatsache, dass Behörden - insbesondere die Geheimdienste weltweit - die Daten der sozialen Medien für ihre eigenen Zwecke nutzen können, worauf der Nutzer ebenfalls keinen Einfluss hat.

3.6 Geostrategische Rahmenbedingen

In einem Frankfurter Allgemeine Zeitungsartikel (FAZ) zum Thema „Überwachungskapitalisten unter sich“ steht: „Wenn die Silicon-Valley-Chefs über das Internet sprechen, dann ist das ihr Internet. Wir sollen die Dienste nutzen, die sie zur Verfügung stellen, zu ihren Bedingungen.“ [192]. Dies gilt nicht nur für amerikanische Soft- und Hardwareprodukte, sondern auch für das Internet. Laut Atlas der Digitalen Welt ist hier vor allem der Traffic entscheidend, da dieser genau aufschlüsselt, wie hoch die Macht des jeweiligen Anbieters ist s. [49, p. 29]. Allein die amerikanischen Konzerne (Alphabet, Apple, Amazon, Meta, eBay) binden in Deutschland „mehr als 50 % des gesamten Web-Traffic“ [49, p. 29] und sind dabei nicht nur in der Nutzungszeit dominierend, sondern binden „auch 45 % der nachfolgenden Nutzungsdauer“ [49, p. 32]. Hinsichtlich der Nutzungsdauer verbleiben die Nutzer innerhalb des Ökosystems eines Anbieters, hier bspw. von der Facebook Webseite zu WhatsApp wechseln und zurück. In diesem Zusammenhang ist nachvollziehbar, dass in Deutschland die ersten sieben meistbesuchten Webseiten ausschließlich amerikanische Anbieter sind. Erst an achter Stelle kommt ein deutscher Anbieter, hier web.de s. [49, p. 18]. Nachfolgend wird auf einzelne Aspekte geostrategischer Rahmenbedingungen eingegangen, angefangen über die militärische Nutzung des Cyberraums, die Sichtweise der EU sowie China und welche Abhängigkeiten durch den Einsatz der IT entstehen.

3.6.1 Gefahr der Kollateralschäden durch Einsatz von digitalen Tools, die potentiell Krieg im betroffenen Staat auslösen können

Eine Forscherin der Stiftung Wissenschaft und Politik schreibt zum Cyberraum, dass „[d]ie Politik … sich der Realität stellen [muss], dass der Cyberraum vermehrt zum Operationsfeld des Militärs wird.“ [193, p. 5]. “Die „neuen Kriege“ sind … gekennzeichnet von dezentralen und asymmetrischen Konflikten, die also nicht mehr zwischen Staaten, sondern zwischen nichtstaatlichen Akteuren … bzw. poststaatlichen Identitäten … geführt werden“ [194]. “Das Bureau of Investigative Journalism oder Wikileaks reagieren dagegen seit den späten 2000er-Jahren mit Sichtbarkeit, Transparenz und Unterwachung des staatlichen Überwachungsapparats („sousveillance“…) auf einen zunehmend unsichtbaren Krieg, indem sie die Informationen zu verschleierten oder in den Randnotizen der Agenturmeldungen untergegangenen Drohnenangriffen in Datenbanken zusammentragen.“ [194]. “ Die Begrifflichkeit vom „Cyberwar“ entstand … Mitte der 1990er-Jahre in den USA. Der Wortteil Cyber leitet sich aus dem anglisierten griechischen Begriff κυβερνήτης (kybernḗtēs) für Steuermann ab. „Cyberwar“ dient also als Diskursbündel für sicherheitspolitische Fragen, außenpolitische Diplomatie und Gegenaufklärung oder schlicht allgemeine Beobachtungen zur globalen Netzkultur und lässt sich so an ganz heterogene Themenfelder anschließen: Propaganda und politische Kommunikation …, Spionage …, geheimdienstliche Mittel wie Sabotage, Abschreckung und Gegenaufklärung …, Terrorismus … Hacking …, bis hin zu seiner kulturanalytischen Untersuchung der Verschaltung von klassischen Militärstrategien mit digitaler Technologie“ [194]. Die „„„sozialen Medien“ [sind] ein Missbrauch von Heeresgerät der Intelligences des Kalten

Krieges. Paradigmen einer totalen Sichtbarkeit und als omnipotent imaginierte Wissensformen unter dem Eindruck elektronischer Datenverarbeitung tauchen hier erstmalig auf, so dass zunehmend das Individuum in den Fokus rückt.“ [194]. „Die Drohnen der nächsten Generation würden, so schreiben sie in Anlehnung an die ubiquitären sozialen Medien, „... alles sehen, während sie selbst verlockend unsichtbar bleiben“ [194]. Dazu ist zu befürchten, dass „Maschinen könnten in Zukunft ganz eigenständig über Töten und Am-Leben-Lassen entscheiden“ [194]. Bei hybriden Bedrohungen greifen „[s]taatliche und nichtstaatliche Akteure … auf hybride Methoden und Ansätze …, um destabilisierende Einfluss auf Staaten auszuüben.“ [194]. Zu den möglichen Optionen zählen u.a.: „Cyber-Angriffe, verdeckte militärische Operationen, wirtschaftlicher Druck oder Desinformation, die in mehreren Domänen Wirkung entfalten und sich gegenseitig begünstigen können.“ [194]. Konkret „können je nach individueller Ausprägung die physische (z.B. Hardware und *Firmware*), die logische (z.B. Virtualisierungen und Betriebssysteme) und die informationelle (z.B. Anwendungen und Daten) Schicht des Cyber-Raums durch einen Aggressor genutzt werden.“ [194]. Als Beispiel wird die Desinformation genannt, in denen technische Hilfsmittel genutzt werden, um „authentische Informationen“ [194] zu manipulieren s. [194].

3.6.2 Europäische Union

Die Europäische Union (EU) hat einen rechtlichen Rahmen zur Cybersicherheitsverordnung vorgelegt, mit dem „die digitale Souveränität mit strategischer Verflechtung kombiniert wird“ [195, p. 1]. Davor ist eine 10 Jahre lang andauernde Verhandlung über eine globale Regelung zu dieser Thematik gescheitert s. [195, p. 1]. „Cyberbedrohungen sind ein Bestandteil und zugleich die Speerspitze des globalen Wettbewerbs zwischen liberalen Demokratien und autoritären Systemen.“ [195, p. 1]. Denn „[w]er die Kontrolle über Hard- und Software hat, der bestimmt auch darüber, welche Innovationen und Geschäftsmodelle möglich sind und wer auf welche Informationen Zugriff hat.“ [195, p. 2]. Darüber hinaus gibt es „eine immer engere Kooperation zwischen privaten Technologienkonzernen und Institutionen, die hoheitliche Aufgaben wahrnehmen.“ [195, p. 2]. Die EU betrachtet Konzerne, die „an der Ausweitung der gesellschaftlichen Überwachung arbeiten … oder kooperieren … nicht mehr als nur als unpolitische, rein marktwirtschaftliche Akteure“ [195, p. 2]. Das Internet ist „heute ein Raum […], in dem Verteilungs- und Wertekonflikte ausgetragen und die zukünftigen Modalitäten der individuellen und gesellschaftlichen Selbstbestimmung ausgehandelt werden.“ [195, p. 2]. Daher ist die Technologie an sich nicht als wertneutral anzusehen, da diese „Entscheidungen und Handlungsweisen“ [195, p. 2] normieren. Denn „digitale Produkte können u.a. „die staatliche Gestaltungs- und Steuerungskompetenz durch technische Hintertüren unterlaufen.“ [195, p. 2]. Vor diesem Hintergrund ist technologische Souveränität unabdingbar, ohne diese ist die Innovation und der Wettbewerb eingeschränkt s. [195, p. 2]. In Bezug auf die Cybersicherheit bleibt es eine globale Herausforderung, denn die „Komplexität und die Interdependenz von digitalen Systemen“ [195, p. 3] nimmt immer mehr zu, während die Qualität der „verwendeten Hard- und Software [weiterhin] mangelhaft“ [195, p. 3] ist und

zu deren Absicherung das Personal nicht ausreicht. Jeden Tag entstehen „neue Angriffsvektoren und -ziele“ [195, p. 3]. Inzwischen ist „[d]ie digitale Transformation der globalen Märkte … nicht nur mit einer wachsenden ökonomischen Interdependenz einher[gegangen], sie hat gleichzeitig auch die Steuerungsfähigkeit der Staaten zunehmend reduziert“ [195, p. 3], was bspw. am Konflikt der USA mit der chinesischen Firma Huawei zu beobachten ist. Für die USA „sind die Produkte und Dienste der amerikanischen Tech-Unternehmen … ein wesentliches Instrument der staatlichen Kontrolle und der internationalen Einflussnahme.“ [195, p. 3]. Selbst der europäische Zahlungsvermittler Society for Worldwide Interbank Financial Telecommunication (SWIFT) wurde von den USA zunehmend als Überwachungsinstrument genutzt s. [196]. Zugute kam ihnen, dass SWIFT ein gespiegeltes Datenzentrum in Virginia (USA) unterhielt bzw. unterhält, so dass die US-Behörden bereits rechtlich die Möglichkeit haben, darauf zuzugreifen s. [196]. Digitale Souveränität wird hier als „Fähigkeit eines Völkerrechtssubjekts zur Kontrolle und Steuerung des Cyberraums“ [195, p. 7] definiert, wofür als Bsp. „[d]ie Zertifizierungsschemata und die Datenschutzregeln der EU“ [195, p. 7] zählt. Um digitale Souveränität zu auszuüben, „sind (1) die Erhaltung und der Ausbau der globalen Wettbewerbsfähigkeit, (2) möglichst faire Wettbewerbsregeln und (3) Investitionen in digitale Infrastrukturen“ [195, p. 7] notwendig. „Unter strategischer Verflechtung ist eine Strategie zu verstehen, die die Komplexität der Realität unter den Bedingungen der Globalisierung und Digitalisierung anerkennt.“ [195, p. 7]. „Sicherheit wird […] als Ergebnis eines Prozesses der ökonomischen und politischen Integration und der Steigerung wechselseitiger Abhängigkeit erreicht“ [195, p. 7], wie es bspw. mit der „gegenseitige[n] Anerkennung von Zertifizierungen im Bereich Produktsicherheit“ [195, p. 7] bereits praktiziert wird.

3.6.3 Volksrepublik China

Laut einer gemeinsamen Mitteilung der hohen Vertreterin der Union für Aussen- und Sicherheitspolitik ist China „ein wirtschaftlicher Konkurrent in Bezug auf technologische Führung“ [197, p. 1]. Wie mächtig China geworden ist, wird mit diesem Satz aufgezeigt: „Weder die EU noch einer ihrer Mitgliedstaaten können ihre Ziele mit China ohne vollständige Einigkeit wirksam erreichen.“ [197, p. 2]. Desweiteren muss „Chinas proaktive und staatlich gelenkte Industrie- und Wirtschaftspolitik, darunter die Initiative „Made in China 2025““ [197, pp. 6-7], welches das Ziel hat, „einheimische Marktführer aufzubauen und sie dabei zu unterstützen, [um] in strategischen Hochtechnologiesektoren eine globale Vormachtstellung zu erlangen.“ [197, pp. 6-7] kritisch betrachtet werden. Denn Deutschland bzw. die EU sind von der Lieferung von Hochtechnologien aus China, einschließlich der IT-Systeme, im höchsten Maße abhängig. Verschärfend kommt insbesondere Chinas Vision hinzu, „bis 2050 über die technologisch fortschrittlichste Streitmacht zu verfügen, … [was] für die EU bereits kurz- bis mittelfristig sicherheitspolitische Fragen auf[wirft]. Sektorübergreifende hybride Bedrohungen, einschließlich Informationsoperationen … untergraben nicht nur das Vertrauen, sondern stellen auch eine Herausforderung für die Sicherheit der EU dar“ [197, p. 4]. Vor diesem Hintergrund sind

„[a]usländische Investitionen in strategische Sektoren, der Erwerb kritischer Vermögenswerte, Technologien und Infrastrukturen in der EU, die Beteiligung an der Normung auf EU-Ebene und die Versorgung mit kritischen Ausrüstungen“ [197, p. 11] sehr kritisch zu betrachten, da diese die Sicherheit in der EU untergraben können. Als Beispiel wird hier das 5G Netz aufgeführt, denn diese bilden „künftig das Rückgrat unserer Gesellschaften und Volkswirtschaften“ [197, p. 11], in dem „darunter sensible Informations- und Kommunikationstechnologien in kritischen Sektoren“ [197, p. 11] befinden. Daher kann „[j]ede Schwachstelle in 5G-Netzen … potenziell sehr schwere Schäden verursachen“ [197, p. 11]. Vor diesem Hintergrund hat die EU eine Reihe von Instrumenten zur Verfügung - u.a. die Richtlinie über die Netz- und Informationssicherheit - um die (IT-)Sicherheit in der EU zu erhöhen s. [197, p. 11]. Das China inzwischen eine Großmacht geworden ist, zeigt auf, dass die bisherige amerikanische Strategie gescheitert ist, „die in den letzten Jahrzehnten als Schlüsselelement der nationalen Strategie der USA das Ziel verfolgt [hatte bzw. haben], die Entstehung von regionalen Hegemonien in Eurasien zu verhindern.“ [198, p. 4].

3.6.4 (Geo-)Strategische Abhängigkeit von Informationstechnik

Wer sich für den Einsatz von Informationstechnik (IT) entscheidet, macht sich automatisch abhängig. Daher ist von den Staaten sowie den (Groß-)Firmen, die IT einsetzen, ein sog. Abhängigkeitsmanagement zu betreiben, was - im Einzelfall - auch für den Bürger gilt. Diese hat die Aufgabe, mögliche Risiken in der Lieferkette frühestmöglich zu identifizieren, um ggf. Maßnahmen zu treffen, so dass es im Idealfall nicht zu Lieferausfällen und damit zum Produktionsstopp bzw. -ausfall kommt. Die Hersteller von sog. neuralgischen Technologien wie Chipproduktion sowie Speichertechnologien sitzen meist in den asiatischen Ländern. Nicht wenige Hersteller sind auf bestimmten Gebieten Monopolisten, was ein besonders hohes Gefährdungspotential aufweist. Als Beispiel wird die taiwanische Firma Taiwan Semiconductor Manufacturing Company Limited (TSMC) gewählt, welches Halbleiterprodukte produziert und nach Intel und Samsung der weltweit drittgrößte Hersteller ist und zugleich der weltweit größte unabhängige Auftragsfertiger für Halbleiterprodukte ist s. [199], s. [200]. Viele Chipdesign-Firmen sind davon abhängig, da diese die Firma TSMC zur Herstellung von „Prozessoren, die in Rechenzentren, Laptops, Smartphones, Automobilen und militärischen Anwendungen“ [201] benötigen. Denn Halbleiter bilden das Rückgrat der heutigen Gesellschaft und ist die Grundlage für neue Technologien wie KI, autonome Fahrzeuge und Quantencomputer s. [201]. US-Exportkontrollmaßnahmen gegen Huawei machen deutlich, wie die Halbleiter-Wertschöpfungskette „waffenfähig“ [201] gemacht werden kann s. [201]. Die Vereinigten Staaten profitieren von diesen Schwachstellen der Wertschöpfungskette, da diese selbst durch die heimische Industrie - hier Intel und AMD - in der Lage sind, dagegen zu halten, was für Europa, einschließlich Deutschland derzeit und auch mittel- bzw. langfristig nicht möglich ist s. [201]. Die Besonderheit liegt hier zum einen darin begründet, dass China noch nicht kurz- bis mittelfristig in der Lage ist, Chips in einer bestimmten Größenordnung selbst herzustellen s. [201]. Zum anderen liegt die Besonderheit darin, dass China

Taiwan militärisch bedrohen kann, was Implikationen nach sich zieht. Daher übt die US-Regierung Druck auf TSMC aus, um die Anlagen von Taiwan weg zu verlagern. Die EU fördert unter dem Aspekt „technologische Souveränität“ [202] und „strategische Autonomie“ [202] die Entwicklung von Halbleiterproduktionsanlagen in Europa s. [202]. In einer weiteren Studie zu Chinas Halbleiterindustrie wird konstatiert, dass „China … seine nationale Position in der globalen Wertschöpfungskette … weiter stärken“ [203] wird, dass Europa - im Gegensatz zu USA - technisch nicht vorn steht und damit „zunehmend auf chinesische Technologieanbieter angewiesen“ [203] sein wird. Daneben besteht u.a. die Gefahr, dass „eine ähnliche Entwicklung wie in der Solarindustrie vollz[ogen wird], in der chinesische Anbieter auf den weltweiten Märkten europäische Konkurrenz verdrängt haben.“ [203].

3.6.5 Technologieunternehmen als Mittel zum Einsatz geopolitischer Interessen

Laut netzpolitik.org sitzen die größten Technologieunternehmen in USA und in China s. [204]. Bspw. wollen bei den Verhandlungen der World Trade Organization (WTO) die USA über die WTO eine Neufassung von Handelsregeln globaler Natur (E-Commerce-Agenda) die Entwicklungsländer in ihrer digitalen Entwicklung ausschließen. Davon würden die „oligopolistischen Macht von Big Tech“ [205] profitieren s. [205]. Ein exemplarisches Beispiel ist Facebook „Free Basics“ Programm für Menschen „im globalen Süden“ [206], die z.T. erstmalig an das Internet angeschlossen werden sollen. Wer daran teilnimmt, muss zustimmen, dass Facebook alle Daten einsehen kann s. [206]. Laut einer Folie der NSA wird bestätigt, wie die USA bis dato und auch noch heute so vorgegangen wird: „Sagen wir es offen - die westliche Welt (insbesondere die USA) hat durch die Setzung von Standards in der Frühzeit des Internets Einfluss gewonnen und viel Geld verdient. Die USA waren der wichtigste Akteur bei der Gestaltung des Internets, wie es uns heute zur Verfügung steht. Dies führte zu einem intensiven Export amerikanischer Kultur und Technologie. Und US-Unternehmen haben dabei viel Geld gemacht.“ [207, p. 240]. Als Beispiel hat Google laut Luzerner Zeitung Geopolitik betrieben. Der Konzern hatte „2012 … einen Kartenwerkzeug entwickelt, das die syrische Opposition beim Sturz von Präsident Assad unterstützen sollte“ [208] und „[d]er Konzern wollte offensichtlich Partei ergreifen in einem internationalen Konflikt und sich dem US-Aussenministerium andienen“ [208]. Durch die Kartierung der Welt übt Google Macht aus, was daran zu erkennen ist, dass der Konzern „das Meer zwischen dem Iran und der arabischen Halbinsel als «Persischer Golf» oder «Arabischer Golf» bezeichnet, … [was] de facto eine politische Entscheidung - oder zumindest eine Entscheidung mit erheblicher politischer Wirkung“ [208] ist s. [208]. Das Fazit des Autors: „Googles Daten werden zur Geheimwaffe in Konflikten“ [208]. Dass dies kein Einzelfall ist, belegt die Zusammenarbeit des Konzerns mit einem Pentagon-Projekt namens Maven s. [209]. Damit will das Verteidigungsministerium „eine führende Rolle bei der „algorithmischen Kriegsführung“ einnehmen“ [209]. Googles Beitrag ist eine KI-Technik für Drohnen bereitzustellen. Dazu wurde eigens Mitarbeiter von Google zur Tarnung an eine „Jobvermittlungsfirma ESC

Federal“ [209] umgesetzt, um „die Zusammenarbeit vor der Öffentlichkeit zu verschleiern.“ [209].

3.6.6. Einbau von Backdoors (Hintertüren) an strategischen Stellen durch geostrategische Überlegungen

Zwei exemplarische Beispiele sind die US-amerikanischen Firmen Cisco und Juniper, die sich auf den Netzwerkbereich spezialisiert haben und deren Produkte weltweit verkauft werden. Der Netzwerkbereich gehört zu den neuralgischen Stellen, wenn hier Sicherheitslücken vorhanden sind, schützen andere Absicherungen nicht (mehr). Daher wurden und werden diese Firmen von US-amerikanischen Geheimdiensten dazu genutzt, um einerseits jederzeit Zugriff auf das Netzwerk von den Käufern zu haben, andererseits im Falle eines Krieges kann es dazu genutzt werden, um diese nachhaltig zu zerstören. Hier fielen beide Firmen in der Vergangenheit mehrfach mit kritischen Schwachstellen auf, die nachweislich in Zusammenarbeit mit der NSA entstanden sind s. [210]. Auch wenn Sicherheitslücken entdeckt worden sind, hat die Firma Juniper explizit Falschaussagen getätigt, wie Forscher nachweisen konnten: „Wir stellen im Gegensatz zu Junipers öffentlichen Aussagen fest, dass ScreenOS VPN-Implementierung seit 2008 anfällig für einen passive Ausnutzung durch einen Angreifer ist.“ [211].

3.6.7 Zwischenfazit

Zum Thema China und USA hat Eric Schmidt folgende Aussage getroffen: „Ich denke, das wahrscheinlichste Szenario ist jetzt keine Zersplitterung mehr, sondern eher eine Aufspaltung in ein chinesisch-geführtes Internet und ein nicht-chinesisches Internet, angeführt von den Vereinigten Staaten“ [212]. Hier drückt mit dieser Aussage der ehemalige Vorstandschef von Google ganz klar die Haltung der amerikanischen Spitze aus, wer die Technologieführerschaft anführt und damit die Macht über das westlich angeführte Internet ausübt. In der internationalen Politik spielen digitale Fähigkeiten eine zunehmend größere Rolle s. [213, p. 103]. „Staaten, die in der Lage sind, Cyberoperationen durchzuführen, können ihren internationalen Gestaltungsspielraum deutlich erweitern.“ [213, p. 103]. Die beiden größten Player, die die digitale Macht ausüben, sind China und Amerika s. [213, p. 104]. Im Zusammenhang mit der Geostrategie ist hauptsächlich das Schutzziel Verfügbarkeit gefährdet, falls es zu Lieferschwierigkeiten bei IT-Systemen - schließt auch Einzelteile mit ein - oder zur temporären bis dauerhafte Einstellung von Onlineanbietern kommt, wie es bspw. durch die Einstellung diverser US-amerikanischer Onlineanbieter bei Paypal im aktuellen Konflikt zu Russland geschieht s. [214]. Hinsichtlich der Auswirkung von Lieferkettenschwierigkeiten bleiben diese überschaubar, da i.d.R. auf vorhandene IT-Systeme zurückgegriffen werden kann. Anders gelagert ist es, wenn sowohl Nutzer als auch Organisationen, die der Nutzer im betroffenen Land in Anspruch nimmt, mittel- bis langfristig keine Onlinedienste nutzen kann wegen Außerbetriebnahme. Dies schließt auch die Inbetriebnahme von gezielten Netzsperren oder gezielten Netzabschaltungen seitens des Staates mit ein. Hier kann es u.U. bis zum Verlust aller

persönlichen Daten einschließlich einer potentiellen Insolvenz kommen, sofern bei letzterem alle Einlagen mit eingefroren sind. Da der Trend immer mehr zu Onlinediensten geht, wird die Nutzungsabhängigkeit und damit verbunden das Risiko immer größer. Eine Option wäre daher, so weit wie möglich die Anzahl der Onlinedienste zu reduzieren bzw. auf ein notwendiges Minimum zu verbleiben. Mit diesem Schritt wird zugleich auch das Schutzziel Vertraulichkeit beim Nutzer erhöht, wenn so wenig wie nötig - im Idealfall nur heimische bzw. europäische - Onlinedienste genutzt werden.

3.7 Digitale Souveränität

Digitale Souveränität wird wie folgt definiert: „Digitale Souveränität ist die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können.“ [215, p. 3]. Beim Nutzer sind hiermit vor allem die souveräne Nutzung und Beschaffung von IT-Systemen sowie die souveräne Nutzung der Daten einschließlich der Kommunikation gemeint s. [215, p. 7]. Als Beispiel kann bei Nutzung von digitalen Monokulturen (sei es Hardware, Betriebssysteme von Microsoft, Software oder Plattformen) keine digitale Souveränität ausgeübt werden s. [215, p. 17]. Dies schließt auch sog. Trusted Platform Module (TPM) ein, wenn der Hersteller mehr Zugriffsrechte als der Nutzer selbst hat. Dies geht für den Nutzer mit einem Kontrollverlust einher, zumal nicht sichergestellt werden kann, dass dort auf Betreiben der amerikanischen Regierung Backdoors eingebaut sind s. [216].

3.7.1 Digitale Souveränität Deutschland

Im Zusammenhang mit der NSA-Überwachungsaffäre gab es einen runden Tisch der Bundesregierung, in der zum Thema digitale Souveränität konstatiert wurde, dass es nicht realistisch sei, wenn dann gäbe es eine Annäherung s. [217, p. 8]. Denn eine „vollständige Unabhängigkeit von IT-Produkten und - Diensten aus dem Ausland ist unrealistisch: Der Technologievorsprung z.B. der USA und der Kostenvorteil z.B. Chinas sind praktisch nicht einzuholen. Deutsche Nutzer wollen an der global vernetzten Welt teilnehmen und wollen und müssen daher auch Dienste aus dem Ausland verwenden.“ [217, p. 8].

Daher ist nur eine Souveränität auf einzelnen Gebieten wie folgt möglich:

- „Vorhanden: Sehr viele IT-Sicherheitslösungen der deutschen Software-Industrie, insbesondere von kleinen mittelständischen Unternehmen (KMU).

- Möglich: Linux-Distribution, Intermediäre Dienste, Router, deutsche/europäische PKI.

- Flankierende regulatorische Maßnahmen sind erforderlich, um solchen Lösungen im deutschen (idealerweise: europäischen) Markt einen Vorteil zu verschaffen. Deutschland sollte hier für und in Europa eine Vorreiterrolle spielen.

- Dies erfordert teilweise signifikante Investitionen und die Bildung von Konsortien aus Industrie und Forschung.“ [217, pp. 8-9].

Da die meisten IT-Produkte - und - Dienste aus dem Ausland kommen, müssen daher alle Lösungen durch Test-Labore überprüft werden:

- „Generelle und bei Beschaffungen der öffentlichen Hand verpflichtende Überprüfbarkeit der Sicherheit aller IT-Lösungen, egal wo sie produziert bzw. erbracht werden.

- Dies umfasst Produkte, Dienste und Herstellungsmethoden (Security by Design!)

- Setzt technische Mindeststandards und verpflichtende Testmethoden und Testwerkzeuge voraus (wenn möglich automatisiert!) …

- Ansätze existieren, aber letztlich besteht hier ein sehr großer Forschungsbedarf: Finden von Trojanischen Pferden, vollautomatische Analyse, Security by Design“ [217, p. 9].

Bei der Entwicklung sicherer IT ist eine geeignete Infrastruktur notwendig und dazu gehört auch die Nutzung sicherer IT in einer Vertrauensinfrastruktur s. [217, p. 9]. Auch muss die Forschung und Entwicklung auf einfache und sichere E-Mailkommunikation sowie sicheren DNS, sicheren SSL/TLS-Next usw. ausgebaut werden s. [217, p. 10].

Die größte Herausforderung ist folgendes: „Vieles in der IT-Sicherheit ist bekannt, noch mehr ist unbekannt!“ [217, p. 10]. Deswegen braucht Informationssicherheit eine umfassende Forschungsagenda s. [217, p. 10].

Eine weitere Herausforderung im Zusammenhang mit der Souveränität ist die IT-Wertschöpfungskette. Hier plädiert die Forschung für einen vermehrten „Einsatz von „Open Source“ Komponenten, strengere Produkthaftung und Sicherheitszertifizierung.“ [218, p. 291]. Dazu gehört die „Öffnung der gesamten Wertschöpfungskette, einschließlich der Entwicklung quelloffener Hardware und entsprechender Entwicklungswerkzeuge.“ [218, p. 291]. Eine umfassende Verbesserung der Sicherheitseigenschaften von IT herbeizuführen ist nur auf internationaler Ebene möglich s. [218, p. 292]. Risiken werden hier nicht nur bei der Veränderung laufender Software gesehen, sondern auch auf Hardwareebene wie folgende Beispiele zeigen:

- „„Zero-day exploits“, wie die WannaCry - Erpressungs-Software, die auf Schwächen beruhte, die den Geheimdiensten bereits bekannt waren

- Hardware-Schwächen wie Meltdown und Spectre, die einen Mikroprozessor dazu bringen, eigentlich geschützte und vertrauliche Informationen ungewollt preiszugeben

- Trojanische Pferde, die sich sogar in der Hardware befinden können, evtl. versteckt durch Manipulation der Dotierungen oder durch Ausnutzung kapazitativer Effekte …

- Diebstahl von Chipdesigns

- Gefälschte, minderwertige oder recycelte Komponenten.“ [218, p. 292].

Die o.g. Auflistung ist nicht abschließend, zeigt aber das Ausmaß an potentiellen Angriffsvektoren anschaulich auf, welches die Sicherheit von kompletten Infrastrukturen unterterminieren kann. Hier ist besonders kritisch die Wechselwirkung zwischen der „funktionalen Sicherheit (Safety)“ [218, p. 292] und der „IT-Sicherheit (Security)“ [218, p. 292] zu sehen. Bspw. können IT-Angriffe auf Safety-kritische Systeme wie Bremsen in Fahrzeugen unter Umständen tödliche Auswirkungen auf Insassen haben s. [218, p. 292], s. [219]. Derzeit ist die internationale Arbeitsteilung so gestaltet, dass die Software vorwiegend aus den Vereinigten Staaten kommt und der größte Teil von Hardware in Asien produziert wird, was aufgrund mangelnden Wettbewerbs die Wahrscheinlichkeit von unsicheren IT-Produkten erhöht s. [218, p. 292]. Vor diesem Hintergrund sind geschlossene Komponenten - hier Hardware - letzten Endes eine „black box“ [218, p. 292], deren Input ggf. aus nicht nachvollziehbaren und kontrollierbaren Quellen stammen kann s. [218, p. 292]. Daher sind alle Vorkehrungen aus Prinzip auf geschlossene Komponenten vertrauenswürdige und zuverlässige Sicherheitsmaßnahmen aufzusetzen, beeinträchtigt s. [218, p. 292]. Um die Qualitäts- und Sicherheitseigenschaften auf allen Funktionsebenen - „d.h. Hardware, Software, Protokolle, Systeme, Dienste und Infrastrukturen“ [218, p. 292] - beweisen zu können und damit das Schutzniveau zu erhöhen, ist die einzige Option die Kontrolle durch den Staat oder durch Unternehmen über die gesamte Wertschöpfungskette wieder zu erlangen s. [218, p. 292]. D.h. strategisch wichtige Lieferanten und Fabriken sind aufzukaufen. China und Indien sind dabei die komplette Wertschöpfungskette unter ihrer Kontrolle zu bekommen s. [218, p. 292]. Eine Alternative bzw. Ergänzung wäre die Option, die gesamte Wertschöpfungskette zu öffnen, einschließlich der verwendeten Werkzeuge s. [218, p. 293]. Ansätze wie bspw. RISC-V (offenes Prozessor-Design) sowie sichere offene Betriebssysteme gibt es bereits s. [218, p. 293]. Dabei können „Regierungen … [die] Arbeit an Design verlässlicher, offener Soft- und Hardware und von offenen Werkzeugen zur Hardwareentwicklung zur prototypischen Produktion von Lösungen fördern.“ [218, p. 293].

Als Beispiel hat die Firma Intel allein zwei Jahre gebraucht, um einen lückenlosen Nachweis ihrer Produktionskette zu ermöglichen s. [220]. Damit soll das Risiko gefälschter elektronischer Teile durch signierte Plattformzertifikate und Rückverfolgbarkeit in der Lieferkette für Hardware, Firmware und Systemkomponenten gemindert werden, welches derzeit nur für Geschäftskunden vorgesehen ist s. [221]. Die Firma Intel selbst ändert durch die Fortentwicklung alle paar Jahre das Chipdesign - hier Grundarchitektur -, so dass allein dadurch neue Sicherheitsrisiken durch die Neuentwicklung entstehen können. Darüber hinaus wird „die Chipentwicklung immer komplexer, da Halbleiterprodukte zunehmend disaggregiert aufgebaut und entsprechend entwickelt werden“ [222], was die Komplexität im Gegensatz zu monolithischen Strukturen erhöht s. [222]. Obwohl mehrere tausend Mitarbeiter nur für die Sicherheit bei Intel beschäftigt sind, kommen dennoch Sicherheitslücken zustande. Die beiden CPU Schwachstellen „Meltdown“ [223] und „Spectre“ [223] waren u.a. durch das Google Project Zero und der Technischen Universität in Graz Österreich entdeckt worden s. [223]. Um diese Art von Sicherheitslücken entdecken zu können, braucht es spezialisiertes Personal, die nicht in einem ausreichenden Maß derzeit weltweit zur Verfügung steht.

Alphabet selbst zeigt vor, wie es sogar fast absolut digital souverän agieren kann. Erstens entwickelt das Unternehmen eigene Chips, betreibt zweitens eigene Rechenzentren und trainiert drittens die selbstentwickelte eigene KI mithilfe von selbst erhobenen Daten, der zu den größten weltweit zählt s. [57, pp. 220-221].

3.7.2 Cloud-Anbieter setzen Standards durch die weitgehende Nutzung dieser Services

Bei der Auswahl der Cloud Architektur muss der Blickwinkel dahingehend erweitert betrachtet werden, dass bei Nutzung automatisch eine dauerhafte Abhängigkeit geschaffen wird. Laut c't sind „US-Clouds beliebt trotz Risiken" [224, pp. 12-13], denn „die Sorge vor unberechtigtem Zugriff auf Daten treibt die Entscheider demnach um" [224, pp. 12-13]. Selbst wenn Kunden sich für ausschließlich in europäischen Raum betriebene Rechenzentren von Google, Amazon oder Microsoft entscheiden, dürfen laut US Recht die US-Behörden auch dann auf die Daten von EU-Bürgern zugreifen s. [224, pp. 12-13]. Verschärft wird dies durch die Möglichkeit, dass der jeweils amtierende US-Präsident immer die Möglichkeit hat, den jeweiligen Onlinedienst in Form eines Handelskrieges - wie es zuletzt in Venezuela fast geschah - einstellen zu lassen s. [224, pp. 12-13]. Amazon, Microsoft und Google führen nicht nur weltweit und in Europa den Cloud Markt an, sondern auch in Deutschland s. [224, pp. 12-13]. Die Telekom ist vergleichsweise nur auf Rang vier s. [224, pp. 12-13].

Als Beispiel hat die größte Bank Deutschlands - hier die Deutsche Bank - entschieden, dass diese ihre IT-Architektur mit Google neu ausrichten will, was ein weiterer Schritt zur dauerhaften Abhängigkeit sein wird s. [224, pp. 12-13]. Nicht umsonst wurde darauf hingewiesen, dass die Bank „seine Daten künftig nicht mehr allein kontrollieren [würde], sondern darauf angewiesen sein, dass der Partner sich an die Regeln hält." [224, pp. 12-13]. Selbst Volkswagen hat seine „Industrial Cloud" [224, pp. 12-13] bei Amazon und die sog. „Automotive Cloud" [224, pp. 12-13] für vernetzte Fahrzeuge wird von Microsoft mitverantwortet s. [224, pp. 12-13]. Hier zeigt sich, dass die Wirtschaft im Gegensatz zum Staat bei der digitalen Souveränität anders agiert s. [224, pp. 12-13]. Dies ist eine der Gründe, warum die im Jahr 2016 von der Telekom betriebene sog. „Microsoft Cloud Deutschland" [224, pp. 12-13] letztlich scheiterte, da diese im Gegensatz zum Original von Microsoft teurer war und gleichzeitig - auch aus Datenschutzgründen - weniger Funktionen angeboten hatte s. [224, pp. 12-13]. Die amerikanischen Anbieter sind u.a. deshalb so dominant, da diese Gesamtpakete anbieten können, wie beispielsweise Entwicklungsumgebungen und Anwendungen wie Datenanalysen oder Sprach- und Bilderkennung s. [224, pp. 12-13]. Dies ist aus strategischer Sicht für die amerikanischen Anbieter von Vorteil, da dadurch Lock-Ins geschaffen werden können, so dass ein Wechsel durch die jeweilige plattformspezifische Anpassung aufwändiger und teuer wird s. [224, pp. 12-13]. Um die Abhängigkeit weiter auszubauen wird weiter massiv in Big Data und KI entwickelt, so dass u.a. europäische Unternehmen gezwungen sind, diese zu nutzen, um den Anschluss nicht zu verlieren s. [224, pp. 12-13].

Als exemplarisches Beispiel wird das Vorgehen der staatlichen Sberbank aufgeführt, die die digitale Souveränität der Bürger in Russland nachhaltig einschränkt. In Russland ist die staatliche Sberbank dabei, die ursprünglich nur Bankengeschäfte tätigte und das größte Geldinstitut des Landes ist, eine führende Rolle in der Internetökonomie zu spielen s. [225]. Die Sberbank - jetzt „Sber“ [225] - bietet „Online-Dienstleistungen für das alltägliche Leben und das Geschäft“ [225] an, was u.a. Essenszustellung, Telemedizin, Paket- und Warentransport, Taxi und Carsharing bis hin zu Immobilien- und Jobportalen, Cloud-Services, Zahlungsdienstleistung und Musik-Streaming umfasst s. [225]. Dies verdeutlicht umso mehr die Machtfülle von einem einzigen Konzern - die zudem dem Staat gehört -, da dieser über einen Einblick in alle Daten, die bei der Nutzung der o.g. Angebotspalette entstehen, verfügt. Dort wird dieser Konzern als „expansiver Krake“ [225] bezeichnet.

Russland agiert ähnlich wie China, in der Techkonzerne aufgrund der Marktgröße wachsen konnten und einen starken Hang zur Autonomie vorweisen, d.h. letztere soll die Übernahme durch ausländische Technikkonzerne erschweren s. [225].

3.7.3 Verringerung der Abhängigkeit von Software Herstellern

Eine Option, die Abhängigkeiten der öffentlichen Verwaltung zu verringern, ist die Bereitstellung der Open Source Plattform für die öffentliche Verwaltung s. [226]. Selbst die Bundesregierung gesteht ein, dass „[i]n der öffentlichen Verwaltung bestehen teils kritische Abhängigkeiten von einzelnen Software-Herstellern.“ [227, p. 43], was die Gefahr nach sich zieht, „die Kontrolle über die eigene IT und somit Handlungsfähigkeit im digitalen Raum zu verlieren.“ [227, p. 43]. Daher haben Bund, Länder und Kommunen im IT-Planungsrat sich das Ziel vorgenommen, „die Digitale Souveränität der Öffentlichen Verwaltung zu stärken“ [227, p. 43], wozu „u.a. der verstärkte Einsatz von Open Source Software (OSS)“ [227, p. 43] zählt s. [227, p. 43]. Die Plattform soll „im Einsatz befindlichen Open-Source-Lösungen …, zur strukturierten Ablage von Softwareprojekten und Verwaltung von offenen Quellcode … sowie zur Kollaboration … bieten.“ [227, p. 43]. Denn die bisherige Abhängigkeit Deutschlands sowie der anderen EU-Staaten von Microsoft „verursacht stetig steigende Kosten und blockiert den technischen Fortschritt in den staatlichen Behörden; untergräbt systematisch das europäische Beschaffungs- und Wettbewerbsrecht; geht einher mit einem erdrückenden politischen Einfluss für den Konzern; und setzt die staatlichen IT-Systeme samt den Daten ihrer Bürger einem hohen technischen und politischen Sicherheitsrisiko aus.“ [228]. Gerade letzteres ist durch die Veröffentlichung von Snowden bekannt geworden, dass die NSA gemeinsam mit dem Government Communications Headquarters (GHCQ) durch eine Sicherheitslücke in Windows u.a. die EU-Kommission abgehört hat s. [228].

Wie die Abhängigkeit allein in der Bundesregierung gestiegen ist, ist an den steigenden Kosten für Berater zu erkennen, deren Gesellschaften seit 2017 insgesamt mindestens eine Milliarde EUR verdient haben s. [229].

3.7.4 Sichere IT ohne Schwachstellen und Hintertüren

In einer aktuellen Studie zur sicheren IT ohne Schwachstellen und Hintertüren wird aufgeführt, dass Schwachstellen in Software und Hardware ein zentrales Problem sind s. [230, p. 1]. Durch die zunehmende Abhängigkeit und der Vernetzung der IT-Systeme muss als Gegenmaßnahme höhere Safety - und Security-Anforderungen gestellt werden s. [230, p. 1]. Dies gilt sowohl für die funktionelle Verlässlichkeit (Safety) als auch für die Informationssicherheit (Verfügbarkeit, Vertraulichkeit, Integrität). Die gegenwärtigen IT-Systeme können den Sicherheits-Anforderungen derzeit nicht gerecht werden, da es Schwachstellen sowohl in der Hardware als auch Software gibt s. [230, p. 1]. Beispiele sind u.a. der Heartbleed-Bug, welches Bestandteil der SSL Verschlüsselung war; die Erpressersoftware Wannacry, deren Schwachstelle im Betriebssystem den Geheimdiensten bekannt war ohne den Hersteller darüber zu informieren; Hardwaretrojaner in elektronischen Haltleiterbauelementen; Angriffe auf IT-Lieferketten wie Solarwinds s. [230, p. 1], [231]. Zum Hardwaretrojaner ist an dieser Stelle festzuhalten, dass diese Art von Trojanern nicht wie sonst durch Änderungen am Metall, der Polysiliciumschicht oder der aktiven Fläche durch optische Inspektion erkannt werden kann s. [231, p. 17]. Der sog. „dopant Trojans“ [231, p. 17] ist nicht nur in der Lage, jeden Zufallszahlengenerator (RNG) generierten Schlüssel zu brechen, sondern darüber hinaus auch noch Schutzmaßnahmen zur Erkennung von Trojanern wie z.B. der Funktionstest als auch Trojaner-Erkennungsmechanismen zu umgehen s. [231, p. 17]. Hier wird deutlich, dass die besten Verschlüsselungstechniken nicht vor dieser Art von Angriffen schützen, da sie unbemerkt durch einen Seitenkanal den geheimen Schlüssel ausleiten. Trotz der Entwicklung der IT-Systeme kann kein signifikanter Fortschritt bei der Informationssicherheit festgestellt werden wie es die u.g. Übersicht von Mitre aufzeigt. Die Common Weakness Enumeration (CWE) von Mitre zeigt für das Jahr 2021 folgende Top 25 der meist gefährlichsten Schwachstellen auf:

Rank	ID	Name	Score
[1]	CWE-787	Out-of-bounds Write	65.93
[2]	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	46.84
[3]	CWE-125	Out-of-bounds Read	24.9
[4]	CWE-20	Improper Input Validation	20.47
[5]	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19.55
[6]	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19.54
[7]	CWE-416	Use After Free	16.83
[8]	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14.69
[9]	CWE-352	Cross-Site Request Forgery (CSRF)	14.46
[10]	CWE-434	Unrestricted Upload of File with Dangerous Type	8.45
[11]	CWE-306	Missing Authentication for Critical Function	7.93
[12]	CWE-190	Integer Overflow or Wraparound	7.12
[13]	CWE-502	Deserialization of Untrusted Data	6.71
[14]	CWE-287	Improper Authentication	6.58
[15]	CWE-476	NULL Pointer Dereference	6.54
[16]	CWE-798	Use of Hard-coded Credentials	6.27
[17]	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	5.84
[18]	CWE-862	Missing Authorization	5.47
[19]	CWE-276	Incorrect Default Permissions	5.09
[20]	CWE-200	Exposure of Sensitive Information to an Unauthorized Actor	4.74
[21]	CWE-522	Insufficiently Protected Credentials	4.21
[22]	CWE-732	Incorrect Permission Assignment for Critical Resource	4.2
[23]	CWE-611	Improper Restriction of XML External Entity Reference	4.02
[24]	CWE-918	Server-Side Request Forgery (SSRF)	3.78
[25]	CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	3.58

Bild 10: Top 25 der gefährlichsten Schwachstellen 2021 [232]

Nach Mitre gibt es derzeit insgesamt 168.330 Schwachstellen s. [233]. Durch die Snowden-Veröffentlichungen wurde auch bekannt, dass der Geheimdienst NSA Schwachstellen gezielt herstellt bzw. ankauft s. [230, p. 2]. Diese gezielt eingebauten Hintertüren sind nun von Kriminellen genutzt worden, was durch WannaCry nachgewiesen ist s. [230, p. 2]. Die Vielzahl der Schwachstellen reicht von Fehlern in der Programmierung bis zur Ausnutzung von Seiteneffekten spekulativer Programmausführung in der Hardware - hier Spectre und Meltdown - s. [230, p. 2]. Selbst die aktive Einschleusung von Schwachstellen durch die verwendeten Entwicklungswerkzeuge ist nicht ausgeschlossen s. [230, p. 2]. Die Herausforderung ist die arbeitsteilige Entwicklung von IT-Systemen über Ländergrenzen hinweg, so dass selbst für industrielle Kunden die Details von Implementierungen nicht transparent sind s. [230, p. 2]. Dies gilt sowohl für Softwaremodule als auch Hardwarekomponenten, was die Vielfalt von Angriffsvektoren erhöht s. [230, p. 2]. Vor diesem Hintergrund ist es nicht ausreichend, das Risiko ausschließlich mit Methoden des Risikomanagements und (Sicherheits-)Updates zu behandeln s. [230, p. 2]. Soft- und Hardware sind zu komplex geworden, verifizierte Lösungen sind ungleich teurer und schützen selbst dann nicht vor gezielten wie auch ungezielten Angriffen, da eine einhundertprozentige Sicherheit es nicht gibt s. [230, p. 2]. Selbst das Testen und Patching reichen hierzu nicht aus, denn neue Systemschichten oder Updates verhindern Angriffe nicht s. [230, p. 2]. Dies gilt auch für zusätzlich eingeführte Kontrollkomponenten, da diese

selbst für Angriffe ausgenutzt oder umgangen werden können oder als - Worst Case - selbst mit unterminiertem Werkzeug entwickelt worden sein s. [230, p. 2]. Mit einer Zertifizierung kann allenfalls die Software - im besten Fall - komplett geprüft werden, was bei der darunter liegenden Hardware nicht mehr der Fall ist s. [230, p. 2]. Denn bei einer Design- bzw. Produktionsprozessänderung bleiben die Hardware-Schwächen weiterhin bestehen. Dies gilt vor allem dann, wenn einzelne Hardwarekomponenten aus unterschiedlichen Gründen geheim gehalten werden und somit ist an diesem Punkt keine - komplette - unabhängige Prüfung mehr möglich s. [230, p. 2]. Hinzu kommt, dass die Zertifizierung - je nach Zertifizierungsstufe - unterschiedlich lange andauert und kostenintensiv ist, so dass die Produkte aufgrund der Schnelllebigkeit des Marktes wieder veraltet sein könnten [230, p. 2]. Nutzer können in der Regel das Produkt nicht selbst beurteilen s. [230, p. 2]. Eine Option ist es, die gesamte Wertschöpfungskette in nationaler Hand zu bekommen bzw. zu halten, was für China und für die USA im Prinzip bereits jetzt schon möglich ist s. [230, p. 3]. Eine vollständige Autonomie kann durch die arbeitsteilige Produktion für den Weltmarkt, in dem Komponenten anderer Anbieter bezogen werden, nicht erreicht werden s. [230, p. 3]. Denn bei den Komponenten können Designschwächen oder absichtlich eingebaute Hintertüren enthalten sein, mit der jedes IT-System beeinflusst werden kann s. [230, p. 3]. Daher sind offene Produktion, verifizierte Soft- und Hardware und sichere Lieferkette eine mögliche Option s. [230, p. 3]. Denn offene Systeme sind gegenüber geschlossenen Systemen im Vorteil, da diese vollständig überprüft werden können s. [230, p. 3]. Allerdings schließt Open Source Fehlerfreiheit nicht aus, bspw. blieb der Heartbleed-Bug jahrelang unentdeckt, obwohl es ein Teil der wichtigsten Kommunikationsverschlüsselung ist (SSL) [230, p. 3]. Selbst systematisches und intensives Testen von Open-Source-Komponenten schließt unentdeckte Fehler nicht aus s. [230, p. 3]. Selbst bei kritischen Komponenten wie CPU-Komponenten nimmt die Schwierigkeit für Korrektheitsbeweise mit der Anzahl der Transistoren, Prozessorkerne etc. zu s. [230, p. 3]. Die Lieferkette für IT-Systeme „kann an nahezu jedem Punkt erfolgreich angegriffen werden - Modifikation des Designs und Beeinflussung des Produktionsprozesses sind ebenso möglich wie die Subversion von Test- und Validierungsverfahren oder Austausch von Systemelementen während der Auslieferung.“ [230, p. 4]. Daher ist eine Sicherung möglichst großer Teile der Lieferkette vorzunehmen, um die Angriffsvektoren so klein wie möglich zu halten s. [230, p. 4]. Selbst wenn für eine Realisierung eines offenen Ansatzes entschieden wird, ist es eine Frage der Finanzierbarkeit. Wegen des Aufwands auf der einen Seite und der mangelnden Flexibilität bei der Weiterentwicklung auf der anderen Seite werden selten formale Spezifikationen oder Verifikationen eingesetzt s. [230, p. 4]. Daher besteht „Forschungs- und Handlungsbedarf, um formale Beweise leichter und kostengünstiger durchführen zu können“ [230, p. 4]. Die Anzahl von Schwachstellen, Fehlern und Hintertüren müssen durch noch zu entwickelnde Mechanismen nachweislich reduzieren, so dass es im Idealfall zu „Secure IT statt IT security“ [230, p. 5] kommt s. [230, p. 5].

Im Vorfeld zur Anhörung des Ausschusses Digitale Agenda zum Thema „IT-Sicherheit von Hard- und Software als Voraussetzung für Digitale Souveränität“, welches am 11. Dezember 2019 stattfand, hat eine Forscherin des Digital Society Institute Berlin folgende

Stellungnahme abgegeben: „Erstens steigt derzeit Deutschlands und Europas Abhängigkeit von ausländischen Technologieanbietern, wobei die Beherrschbarkeit von Schlüsselkompetenzen und -Technologien eher sinkt.“ [234, p. 2]. Dies wurde u.a. damit begründet, dass europäische IT-Anwender „insbesondere in den Bereichen Cloud- und Dateninfrastruktur und Software bzw. bei mobilen oder Desktop-Betriebssystemen“ [234, p. 2] abhängig sind. Außerdem „werden Technologien zunehmend komplexer und mit Hinblick auf die IT-Sicherheit weniger beherrschbar“ [234, p. 3], was mit der globalen Lieferkette begründet wurde, in der die meisten Komponenten in IT-Systemen intransparent für Anwender sind s. [234, p. 3]. Vier Jahre später sieht das Fazit nicht anders aus. Im Gegenteil, es ist eine Verschlechterung der Cybersicherheit und beim Schutz der Privatsphäre eingetreten s. [47, p. 1]. Weder Deutschland noch Europa verfügen über die digitale Souveränität, geschweige denn die Fähigkeit, die Sicherheitseigenschaften von Schlüsseltechnologien selbst beurteilen zu können [47, p. 1]. Eine der Gründe ist die Digitalisierung aller Lebensbereiche, d.h. „[a]lles Physische wird digitalisiert und mit allem vernetzt“ [47, p. 2]. Daraus ergeben sich fast unendliche Angriffsrisiken, was mit einer Erhöhung der Schutzanforderungen einhergeht s. [47, p. 2]. Vor diesem Hintergrund wurden sieben Thesen formuliert, wobei hier auf drei wesentliche Thesen eingegangen wird:

1. Mindeststandards und Produkthaftung: „Berechtigtes Vertrauen in Informationstechnologie entsteht, wenn adäquate Mindeststandards für Sicherheit und Privatsphärenschutz und Testierung nachgewiesen und über Beschaffungsregeln eingefordert werden. Die Verantwortung über Sorgfaltspflichten … verbindliche und schnelle Behandlung sicherheitsrelevanter Schwachstellen und Haftungsregeln von Produkten und Dienstleistungen müssen festgelegt werden.“ [47, p. 3].

2. Stärkung von Grundrechten: „Grundrechte und Werte können durch Informationstechnologie gestärkt werden. Dies gelingt aber nur, wenn auch der gesellschaftliche Interessensausgleich gelingt. … Der Schutz der Grundrechte aller Bürger - in Deutschland wie im Ausland - sollte dabei Vorrang haben vor dem Wunsch, datenbasierte Geschäftsmodelle oder die Überwachung von Verdächtigen zu vereinfachen. Insbesondere sollte es keine Einschränkungen der Kryptographie geben, weder im Inland noch - durch Exportkontrolle - im Ausland.“ [47, p. 3].

3. Aus- und Weiterbildung: „Deutschland und Europa brauchen mehr Fachkräfte, die im Bereich Cybersicherheit qualifiziert sind. Mindestbewusstsein von Cybersicherheit sollte in schulischer Ausbildung und beruflicher Weiterbildung fest verankert sein.“ [47, p. 3].

3.7.5 Zwischenfazit

Digitale Souveränität ist selbst für den deutschen Staat bzw. innerhalb der EU nicht vollkommen realisierbar, wenn dann nur in Teilbereichen möglich. Vor diesem Hintergrund kann von einer digitalen Souveränität eines Nutzers nicht gesprochen werden, da dieser i.d.R. weder das Fachwissen noch die Möglichkeit hat, IT-Systeme selbst umfassend zu kontrollieren bzw. zu prüfen, geschweige diese selbst zu entwickeln. An dieser Stelle ist

zu fragen, ob die Digitalisierung in der Form so weitergeführt werden kann, wenn zumindest auf EU-Ebene nicht die grundlegenden Voraussetzungen für eine digitale Souveränität bislang erfüllt sind, um im Falle eines Falles unabhängig agieren zu können.

3.8 Rechtliche Rahmenbedingungen

Gesetze bzw. Verordnungen können in das Art. 2 Abs 1 i.V.m. Art. 1 Abs. 1 Grundgesetz (GG) abgeleitete Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme - „IT-Grundrecht“ eingreifen, d.h. die Schutzziele Vertraulichkeit und Integrität können rechtlich eingeschränkt werden. Konkret ist jede systematische Erhebung und Speicherung personenbezogener Daten sowohl - mit offenen Mitteln der Informationsbeschaffung als auch mit nachrichtendienstlichen Mitteln - ein Grundrechtseingriff. Darüber hinaus wurden weitere Risiken in diesem Zusammenhang identifiziert, wie beispielsweise die Nichtkenntnisnahme der Nutzungs- bzw. Datenschutzbestimmung durch den Nutzer. Im Rahmen dieser Masterarbeit sind alle Bundesgesetze sowie das Landesrecht der Hauptstadt Berlin, die in das IT-Grundrecht - sowohl direkt als auch indirekt eingreifen - wie folgt aufgelistet und zum Teil - je nach Tragweite - entsprechend kommentiert. Darüber hinaus wird abschließend exemplarisch auf zwei US-amerikanische Gesetze aufmerksam gemacht, die ebenfalls in das IT-Grundrecht eingreifen.

Eingriffe in das IT-Grundrecht durch Bundesgesetze:

3.8.1 Strafprozessordnung (StPO)

§ 94 StPO erlaubt u.a. „die Sicherstellung und Beschlagnahmung von auf dem Server des Providers gespeicherten Daten“ [235].

Der § 95 a StPO ist ein schwerer Eingriff in die Grundrechte sowohl für die Beschuldigten als auch dritte Personen, die von den Maßnahmen betroffen sind. Denn nach Absatz 6 sollen dritte Personen die Beschuldigten von der Unterrichtung einer Maßnahme - hier Beschlagnahme von „E-Mails oder Chat-Inhalte, Inhalte von Nutzerkonten sozialer Netzwerke oder in Clouds gespeicherte Daten.“ [236, p. 4] nicht informieren [236, p. 4]. In diesem Zusammenhang ist auch zu erwähnen, dass der Entwurf des Gesetzes „durch Heimlichkeit [sich] aus[zeichnet]“ [236, p. 4], da im Vorfeld der relevante Paragraph nicht Bestandteil des Referentenentwurfs war und erst später gesondert eingefügt wurde s. [236, p. 4]. Der Paragraph ist nicht auf schwere Kriminalität beschränkt, sondern kann auch auf Delikte angewendet werden, die niedrigschwelliger liegen. Als Beispiel gilt „[e]in Diebstahl im Supermarkt oder das unerlaubte Entfernen vom Unfallort … reicht … für die Durchführung der Beschlagnahme aus.“ [237]. Dies ist besonders schwerwiegend, da der Eingriff das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme erheblich beeinträchtigt s. [236, p. 6]. Denn die „Durchsuchung und Beschlagnahme bei Dritten in einem Umfang an höchstpersönliche Daten einer beschuldigten Person zu gelangen, der noch vor Kurzem undenkbar erschien“ [236,

p. 6] und „mit einem solchen Zugriff ggf. Jahrzehnte eines persönlichen Kommunikationsverhalten nachvollziehen lassen“ [236, p. 6] zeigt beispielhaft die Tragweite des Eingriffs auf.

§ 100a Telekommunikationsüberwachung Strafprozeßordnung (StPO)

Bei diesem Gesetz darf der „kleine Staatstrojaner“ [238] - auch als „Quellen-TKÜ plus“ bezeichnet - eingesetzt werden, um mit dessen Hilfe die laufende Kommunikation auszuleiten, was Juristen und Sachverständige „als „schlicht verfassungswidrig“ [238] bezeichnen s. [238]. Beim „großen“ Staatstrojaner hingegen können „sämtliche Daten des Geräts“ [238] durchsucht und ausgeleitet werden s. [238].

§ 100b Online-Durchsuchung Strafprozeßordnung (StPO)

Hier ist bei § 100b StPO der Absatz 1 hervorzuheben: „Auch ohne Wissen des Betroffenen darf mit technischen Mitteln in ein von dem Betroffenen genutztes informationstechnisches System eingegriffen und dürfen Daten daraus erhoben werden (Online-Durchsuchung)“. Dritte können auch betroffen werden, wie es in § 100b StPO Absatz 3 enthalten ist: „Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.“

§ 100i Technische Ermittlungsmaßnahmen bei Mobilfunkendgeräten (StPO)

Mit dem o.g. Gesetz dürfen sog. mobile Funkvorrichtungen eingesetzt werden, um damit den Telekommunikationsverkehr der Zielperson abfangen zu können. Bei dieser Maßnahme sind auch Unbeteiligte betroffen, da es technisch nicht möglich ist, die Überwachung auf eine einzige Person zu reduzieren.

§ 100k Erhebung von Nutzungsdaten bei Telemediendiensten Strafprozeßordnung (StPO)

Mit diesem Paragraphen ist es u.a. möglich, den Aufenthaltsort eines Verdächtigten zu orten mit Hilfe von sog. Standortdaten.

§ 104 Durchsuchung von Räumen zur Nachtzeit Strafprozessordnung (StPO)

Hier ist vor allem der Abs. 1 Abs. 3 StPO ein schwerer Eingriff in das IT-Grundrecht, denn dieser ermöglicht es, ggf. auf entschlüsselte Daten zugreifen zu können, sofern das IT-System zu diesem Zeitpunkt betriebsbereit ist.

§ 163g Automatische Kennzeichenerfassung Strafprozeßordnung (StPO)

Mit Hilfe dieses Paragraphen ist es durch die Erfassung von Kennzeichen in IT-Systemen möglich, u.a. Bewegungsprofile von Autofahrern zu erstellen und die erhobenen Daten zu anderen Zwecken zu missbrauchen.

Weitere einschränkende Gesetze aus der Strafprozessordnung sind:

§ 98a, 100c, 100g, 100j, 110, 161, 163, 163 StPO.

3.8.2 Telekommunikationsgesetz (TKG)

§ 174 Manuelles Auskunftsverfahren TKG

Mit Hilfe dieses Paragraphen „darf die größte Polizei Deutschlands Staatstrojaner gegen Personen einsetzen, die noch gar keine Straftat begangen haben. Die Bundespolizei erhält die Befugnis zur präventiven Telekommunikationsüberwachung, auch mittels Schadsoftware auf Endgeräten. Der Einsatz soll „sich gegen Personen richten, gegen die noch kein Tatverdacht begründet ist und daher noch keine strafprozessuale [Telekommunikationsüberwachung] angeordnet werden kann““ [238]. Daher ist dieses Gesetz in seiner Eingriffstiefe sehr weitreichend, da u.a. der „Staatstrojaner … sich mit Gesetzen nicht kontrollieren“ [238] lässt.

§ 176 Pflichten zur Speicherung von Verkehrsdaten TMG

Dieser Paragraf verpflichtet die Betreiber von Telekommunikationsdienstleistungen Daten für zehn Wochen zu speichern und Standortdaten für vier Wochen auf Vorrat zu halten. Die anlasslose Datenerhebung wird weiterhin grundrechtswidrig bleiben, wie es die bisherige Rechtsprechung aufgezeigt hat s. [239]. Darüber hinaus entsteht durch die Speicherung ein Missbrauchsrisiko durch Innentäter, durch ausländische Geheimdienste sowie durch Cyberkriminelle s. [239]. Laut dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) sind „Verkehrsdaten … Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden und lassen zum Beispiel erkennen, wer mit wem telefoniert, SMS oder E-Mails austauscht.“ [240]. Mehrmals ist die Regierungskoalition in der Vergangenheit mit ihrem Vorhaben zur Vorratsdatenspeicherung gescheitert, da diese nach dem Urteil des Bundesverfassungsgerichts nicht den verfassungsrechtlichen Anforderungen genügen s. [241]. Bis heute fehlen wissenschaftlich nachvollziehbare Argumente für eine Vorratsspeicherung. [8]

Weitere einschränkende Gesetze aus dem Telekommunikationsgesetz (TKG) sind:

§§ 170, 171, 172, 173 TKG.

Anhand der „Technische[n] Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation, Erteilung von Auskünften (TR TKÜV)“ [242] kann sehr gut Einblick genommen werden, wie umfangreich die technischen Anforderungen für die Überwachung der Telekommunikation geworden sind (165 Seiten) s. [242].

[8] „Insgesamt muss konstatiert werden, dass eine exakte Bewertung der einzelnen Datenkategorien im Hinblick auf ihre Bedeutung für die Gewährleistung der Sicherheit daran scheitert, dass verlässliche Zahlen darüber bis heute fehlen, welche Daten, mit welchem zeitlichen Bezug, für welche Zwecke, abgerufen wurden und wie hoch ihre Bedeutung im jeweiligen Verfahren war.“ [391, p. 268]. Auch wenn die Aussage von 2013 ist, fehlt bis heute ein wissenschaftlicher Nachweis, dass die Vorratsdatenspeicherung der Polizei bzw. Staatsanwaltschaft bei ihren Ermittlungen hilft.

3.8.3 Telemediengesetz (TMG)

§ 8 Durchleitung von Informationen TMG

Nach 8 § TMG Absatz 4 gibt es für die Behörde die Möglichkeit, an Identifikationsdaten sowie an Passwörtern heranzukommen, „wenn ein Diensteanbieter auf freiwilliger Basis die Nutzer identifiziert, eine Passworteingabe verlangt oder andere freiwillige Maßnahmen ergreift."

§ 15b Auskunftsverfahren bei Passwörtern und anderen Zugangsdaten TMG

Das weitreichendste Gesetz ist § 15b TMG. Darin wird das Auskunftsverfahren bei Passwörtern und anderen Zugangsdaten geregelt. Hier können Behörden zu Passwörtern und anderen Zugangsdaten von Betreibern verlangen. Dieser Eingriff ist erheblich, da ein Missbrauch durch die Betreiber oder den Behörden nicht ausgeschlossen werden kann. Zudem können mildere Maßnahmen in Betracht gezogen werden, wie bspw. eine Kontosperrung durchzuführen.

Weitere einschränkende Gesetze aus dem Telemediengesetz (TMG) sind:

§§ 2c, 14, 14a, 15, 15a, 15c TMG.

Weitere einschränkende Bundesgesetze, die als Anhang D jeweils mit konkret einschränkenden Gesetzen einschließlich z.T. mit Erläuterungen aufgeführt sind, sind wie folgt:

Gesetz über den Bundesnachrichtendienst (BND-Gesetz - BNDG), Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz - G 10), Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (Kontrollgremiumgesetz - PKGrG), Bundeskriminalamtgesetz (BKAG), Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz - BVerfSchG), Gesetz über die Bundespolizei (Bundespolizeigesetz - BPolG), Gesetz über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681* (Fluggastdatengesetz - FlugDaG), Gesetz über das Zollkriminalamt und die Zollfahndungsämter (Zollfahndungsdienstgesetz - ZFdG), Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz - ATDG), Abgabenordnung (AO), Kreditwesengesetz (KWG), Netzwerkdurchsetzungsgesetz (NetzDG), Bundesmeldegesetz (BMG), Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz - PAuswG), Paßgesetz (PaßG), Straßenverkehrsgesetz (StVG). Beim Landesrecht wird als Beispiel Berlin herangezogen, hier wäre das Allgemeines Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung in Berlin (Allgemeines Sicherheits- und Ordnungsgesetz - ASOG Bln) zu nennen.

3.8.4 Risiko Zweckentfremdung der Datenerhebung

Aus der Steuer-Identifikationsnummer wird eine eindeutige Bürgernummer geschaffen. Dazu wurde im März 2021 das Gesetz zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz - RegMoG) erschaffen. Vor dem Hintergrund der Geschichte der Deutschen Demokratischen Republik (DDR), wo die Personenkennzahl als Kontrollinstrument genutzt wurde, ist es ein schwerwiegender Eingriff in das Grundrecht auf die informationelle Selbstbestimmung, wenn die Bürgernummer mit der eindeutigen Steuer-Identifikationsnummer verknüpft wird s. [243]. Damit ist eine Profilbildung möglich s. [243]. Dieses Beispiel zeigt exemplarisch auf, dass „einmal eingeführte Systeme später zu einer Ausweitung der Überwachung genutzt werden." [243]. Selbst „Politiker der Bundesregierung" [243] teilten im Jahr 2007/2008 mit, „dass es sich bei der Steuer-ID nicht um die Einführung einer Personenkennzahl handele." [243], was nun mit dem Registermodernisierungsgesetz hinfällig ist s. [243]. Ein weiteres Beispiel für den zunehmende Ausweitung der Kontrollbefugnisse seitens des Staates zeigt das Gesetz „Entfristung von Vorschriften zur Terrorismusbekämpfung" vom 3. Dezember 2020. Das Terrorismusbekämpfungsergänzungsgesetz trat damals im Zusammenhang mit den Terroranschlägen am 11.09.2001 in den USA am 09. Januar 2002 in Kraft und beinhaltete u.a. Auskunftspflichten für die Branchen Luftverkehr, Finanzdienstleistungen, Telekommunikation und Telemedien sowie der Einsatz von IMSI-Catcher s. [244]. Im Vorfeld zur Entfristung dieses Gesetzes haben die Sachverständigen im Bundestag einhellig die Entfristung u.a. wegen verfassungsrechtlicher Bedenken abgelehnt, da es bereits mehrere einschlägige Urteile des Bundesverfassungsgerichts gab, die Teile der Befugnisnormen „sturmreif geschossen" [245] haben s. [245].

3.8.5 Risiko Nichtkenntnis von rechtlichen Nutzungsbedingungen bzw. Datenschutzbedingungen

Die Europäische Datenschutzgrundverordnung (DSGVO) erhöht im Kern den Datenschutz der Bürger in der EU. Dennoch liest die überwiegende Mehrheit der Nutzer die Datenschutzrichtlinien fast nie. Die meisten stimmen den Datenschutzrichtlinien formell zu, ohne zu wissen, was mit ihren persönlichen Daten passiert. Dies wird als „Privacy Paradox" bezeichnet, da einerseits die Privatsphäre als wichtig angesehen wird, andererseits nicht entsprechend danach gehandelt wird s. [246]. Von diesem Umstand profitieren Unternehmen, da die meisten Nutzer die Datenschutzrichtlinien nicht lesen bzw. ziehen die eigene Bequemlichkeit dem Datenschutz vor s. [246]. Prinzipiell herrscht hier eine Informationsasymmetrie zwischen Nutzern und dem jeweiligen Dienstanbieter vor. Dies gilt auch im Zusammenhang mit den Datenschutzerklärungen, die helfen sollen, in diesem Bereich zumindest die Informationsasymmetrie für den Nutzer zu verringern, was aber an der „Unfähigkeit" [247] der Nutzer scheitert s. [247]. Erschwerend kommt hinzu, dass die meist voreingestellten maximalen Nutzungsmöglichkeiten der Daten selbst die Allgemeinen Geschäftsbedingungen (AGB) durch den Anbieter vom Nutzer akzeptiert wird und somit den Datenschutz aushebelt. Denn „[e]ine Einwilligungserklärung […] ist

keine Grundlage für Souveränität und *schützt nicht* vor der Erosion der Privatsphäre“ [248, p. 14]. Dies wird sich in Zukunft verstärken, da der Einsatz von Technologien in allen Bereichen des menschlichen Lebens zunimmt und die damit verbundenen Folgen gravierender sein werden s. [248, p. 14].

Einer Studie zufolge kostet allein das Lesen von Datenschutzrichtlinien in Amerika ca. 201 Stunden pro Jahr, dennoch kann es als Orientierungswert für Europa genommen werden s. [249].

3.8.6 Richtlinie des Europäischen Parlaments und des Rates „E-Evidence-Verordnung“

Die Europäische Kommission hat einen finalen Vorschlag zur „Richtlinie des Europäischen Parlaments und des Rates zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren“ [250] - abgekürzt „E-Evidence-Verordnung“ - vorgestellt, in dem Strafverfolgungsbehörden die Möglichkeit gegeben wird, Zugriff auf digitale Daten in anderen Staaten der EU zu ermöglichen „Europäische Herausgabeanordnung“ [251, p. 2] und Beweismittel zu sichern „Europäische Sicherungsanordnung“ [251, p. 2]. Dabei werden zwei rechtliche Instrumente definiert, die bei Anwendung - ohne dabei die Behörden des betroffenen Staates zu informieren - folgendes ermöglichen sollen:

1. European Production Order (EPO)

„Mit Hilfe einer EPO werden Diensteanbieter verpflichtet, die von den Behörden geforderten Daten binnen 10 Tagen herauszugeben, in Eilfällen sogar binnen 6 Stunden.“ [251, p. 2].

2. European Preservation Order (EPrO)

„Mit Hilfe der EPrO soll das Löschen oder Überschreiben vorhandener Daten verhindert werden, um ein anschließendes Rechtshilfeersuchten, EIO oder EPO zu ermöglichen.“ [251, p. 2].

Die Bundesrechtsanwaltskammer warnt in ihrer Stellungnahme zur o.g. Verordnung, „dass die von Eingriffen betroffenen Personen (Diensteanbieter, Beschuldigte und drittbetroffene Dateninhaber) in diesem grundrechtsrelevanten Bereich im Vollstreckungsstaat schutzlos gestellt werden.“ Denn es ist nun nur „Aufgabe des jeweiligen Providers, die Berechtigung der anfragenden Behörde zu prüfen.“ [251, p. 2], da keine lokale Behörde der betroffenen Person einbezogen wird s. [252]. Darüber hinaus „wird [dies] dem besonderen Schutzbedürfnis, das personenbezogenen Daten sowohl auf europäischer[1], als auch auf deutscher nationaler Ebene[2] zugebilligt wird, nicht gerecht.“ [251, p. 2]. Die Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat zur E-Evidence-Verordnung hat auf folgenden Sachverhalt aufmerksam gemacht: „Erstmals im Bereich der internationalen Zusammenarbeit in Strafsachen soll die Herausgabe von Daten nicht mehr davon abhängig sein, ob die verfolgte Tat

dort, wo die Daten ersucht werden, überhaupt strafbar ist.“ [253, p. 1], was rechtlich ein Novum darstellt. Als Beispiel wurde „ein in Deutschland erlaubter Schwangerschaftsabbruch sein oder eine politische Meinungsäußerung, wenn diese im ersuchenden Staat strafbewehrt ist.“ [253, p. 1]. In letztem Fall kann exemplarisch auf den Fall Jan Böhmermann verwiesen werden, der durch den türkischen Staatspräsidenten Erdogan verklagt wurde, da dieser aus dessen Sicht den Staatspräsidenten beleidigt habe s. [254].

3.8.7 Gesetzliche Regelungen der US-Behörden

Die Konferenz der Datenschutzbeauftragten hat feststellen lassen, dass den amerikanischen Geheimdienstbehörden bspw. durch die Anwendung von „Section 702 des US-amerikanischen Foreign Intelligence Surveillance Act (FISA)“ [255] rechtlich ohne gerichtlichen Beschluss erlaubt, „Kommunikationsdaten von Nicht-US-Bürgern anzufordern oder direkt selbst abzugreifen“ [256]. Dies ermöglicht es den Geheimdiensten dennoch bspw. an die Daten durch eine EU-Tochtergesellschaft eines US-Unternehmens, welches die Daten ausschließlich in Europa speichert, heranzukommen s. [256]. Dies trotz des rechtlichen Umstands, dass es nach der DSGVO nicht erlaubt ist, muss der US-Mutterkonzern ansonsten eine Strafe zahlen, wenn es der verdeckten Anordnung einer US-Behörde nicht nachkommt s. [256]. Hinzu kommen noch weitere rechtliche Möglichkeiten wie die „Clarifying Lawful Overseas Use of Data Act“ [257], bekannt auch als US-Cloud-Act.

3.8.8 Zwischenfazit

Insgesamt fällt angesichts der Vielzahl der Eingriffe - vor allem in den letzten Legislaturperiode - in das sog. IT-Grundrecht auf, dass der sog. Abbau von Bürgerrechten in den Medien - hier FAZ, Süddeutsche Zeitung, Bild, Handelsblatt - kaum erwähnt - geschweige systematisch untersucht wird - und eher mehr in Fachmedien wie der Heise Verlag, Netzpolitik.org oder Blogs wie blog.fefe.de darüber berichten, wenn auch zu einzelnen Themen und nicht in einem größeren Zusammenhang. Bis zum jetzigen Zeitpunkt wurde keine Überwachungsgesamtrechnung vorgenommen. Im Bundestag wurde zuletzt am 22.02.2021 darüber debattiert und es gab noch keine gemeinsame Lösung dafür, wie eine Überwachungsgesamtrechnung erfolgen soll s. [258]. Hier kann als Anregung das Handbuch zur Evaluation der Anti-Terror-Gesetze in Österreich genommen werden s. [259]. Als exemplarisches Beispiel sei hier das Thema Überwachung seitens des BND beim deutschen Internet-Knoten genannt. DE-CIX, der größte Betreiber des Internet-Knoten in Frankfurt, hat gegen die Verpflichtungsanordnungen des Bundesnachrichtendienstes geklagt. Zur Bundesverwaltungsgerichtsentscheidung haben nur zwei überregionale Zeitungen geschrieben, hier FAZ mit Artikel vom 31.05.2018 und die SZ mit Artikel vom 31.05.2018 s. [260], s. [261]. Auffällig in diesem Zusammenhang ist, dass das Urteil des Bundesverwaltungsgerichts am 30.05.2018 unter Abwesenheit der Parteien stattfand und darüber hinaus um 22:30 Uhr verkündet wurde, was in der Vergangenheit

durch das Bundesverwaltungsgericht relativ selten vorkommt s. [262]. Das gleiche Gericht hat im Jahr 2014 selbst festgestellt, dass der komplette Telekommunikationsverkehr von dem Betreiber an den BND ausgeleitet wird und erst dann wird eine Selektion vorgenommen und nicht umgekehrt s. [263]. Dies trotz der Tatsache, dass potentiell Millionen deutscher Bürger von der Ausleitung und damit der Überwachung durch den BND betroffen sind, ist das angesichts der Tragweite der Entscheidung nicht nachzuvollziehen. Derzeit kommen weitere Einschränkungen seitens auf EU-Ebene hinzu, hier die anlasslose Durchsuchung aller privaten Nachrichten der EU-Bürger nach verdächtigen Inhalten s. [264]. Hier dürfen Anbieter von Chatsystemen flächendeckend „nach Darstellungen sexuellen Missbrauchs Minderjähriger scannen“ [264]. Damit wird eine flächendeckende Überwachung von digitalen Kommunikationskanälen ermöglicht.

3.9 Staatliche einschließlich geheimdienstlicher Rahmenbedingungen

In diesem Kapitel werden wesentliche - nicht abschließende - Aspekte staatlicher und geheimdienstlicher Rahmenbedingungen beleuchtet. Dies fängt über technische Abhörschnittstellen an, geht über die Beschlagnahmung bzw. dem Verlust von IT-Geräten bis hin über den Verfassungsschutzbericht einschließlich der Parlamentarischen Nachrichtenkontrolle und schließt mit der Zusammenarbeit von Dienstleistern mit Geheimdiensten sowie einer Kurzdarstellung von zwei Auslandsgeheimdiensten einschließlich einer Auflistung von Möglichkeiten der NSA für die Manipulation von kryptografischen Systemen ab.

3.9.1 Risiko Lawful Interception

Firmen müssen - insbesondere die Netzbetreiber - Abhörschnittstellen für Behörden schaffen, da diese sonst keine Betriebserlaubnis erhalten. Öffentlich bekannt ist es unter dem Namen Lawful Interception (LI). „Die … technischen Richtlinien für die Aufschaltpunkte sind in den verschiedenen LI-Standards vom European Telecommunications Standards Institute (ETSI), dem Third Generation Partnership Project (3GPP) … spezifiziert.“ [265]. Bspw. ist die Firma Digitask in der Lage, verschlüsselte Skype Telefonate mitzuschneiden, deren Service vom Bayerischen Landeskriminalamt genutzt wird s. [266, p. 1]. Des Weiteren bietet die Firma die Dekodierung von SSL-Verbindungen an, was mit Hilfe eines Man-in-the-Middle-Angriff realisiert werden kann s. [266, p. 6 (Anlage)]. Dort werden „auf dem überwachten Rechner … die Schlüssel und Metadaten über die vorhandene Breitbandüberwachung mit ausgeleitet“ [266, p. 6 (Anlage)]. Selbst Anbieter von Überwachungssoftware wurden gehackt, so dass u.a. das Risiko besteht, dass die dort erhobenen Daten von überwachten Personen in falsche Hände geraten können s. [267]. In einem weiteren Leak wurde bekannt, dass ein Anbieter von Überwachungssoftware auch Tornutzer im Blick hat s. [268].

3.9.2 Risiken durch Beschlagnahmung seitens der Strafverfolgungsbehörden bzw. Geheimdienste

Durch die Digitalisierung in allen Lebensbereichen entstehen u.a. „Standort-, Kommunikations-, Gesundheitsdaten sowie weitere sensible Daten von beschlagnahmten Geräten wie Mobiltelefone, Tablets, IoT-Geräten, Laptops“ [269], USB-Sticks u.v.m. s. [269]. Diese Daten bergen zum Teil erhebliche Datenschutzrisiken, wofür eine Datenschutzfolgenabschätzung notwendig ist s. [269]. Die EU Richtlinie 2016/80 schreibt eine Datenschutzfolgenabschätzung vor, hier Art. 27 [270]. Die Beschlagnahmung führt zu einem Eingriff in die Grundrechte der betroffenen Person. „Mögliche betroffene Personen sind Verurteilte, Verdächtige, Opfer, Zeugen und Dritte, die mit den Ermittlungen nichts zu tun haben oder Personen, die zu Unrecht verdächtigt werden.“ [269]. Des Weiteren enthalten „Informationen aus einem Mobiltelefon unter anderem Foto, Namen, Telefonnummern, E-Mails, Metadaten, Standortdaten, Zahlungsdaten, Videos, Daten über religiöse Vorstellungen oder Gesundheit etc.“ [269]. Durch die Beschlagnahmung gibt es dabei folgende Risiken:

1. Illegitimer Zugriff auf Daten, was zu erheblichen Schäden der betroffenen Person führen kann, wie z.B. Diskriminierung, Rufschädigung, finanzieller Verlust usw. s. [269]. „Einige Hauptbedrohungen, die zu einem unzulässigen Zugriff führen können, sind wie folgt:

I. Verarbeitung / Lesen von Daten für einen falschen Fall.

II. Unverschlüsselte Datenübertragung von Dritten.

III. Unberechtigter Zugriff von Personen auf die forensische Big Data Plattform.

IV. Untersuchungsbericht (Papierform) an den falschen Zielort gesendet.

V. Zugriff auf Daten nach Abschluss des Falls.

VI. Keine systematische Überwachung der Berechtigungen.

VII. Unerlaubter Querverweis von Daten (Internationale Organisation für Normung

[ISO],2017).“ [269].

2. Unerwünschte Änderung von Daten, hier Manipulation von Beweisen, was dazu führen könnte, dass Unschuldige beschuldigt werden.

„Einige Hauptbedrohungen, die zu einer unerwünschten Änderung von Daten führen, sind wie folgt:

I. Fehler bei Updates, Konfiguration oder Wartung (ISO 2017).

II. Einschleusen von bösartigem Code (Commission Nationale de l’Informatique et des Libertés [CNIL], 2017).

III. Ersetzen eines Originaldokuments (Papier) durch eine Fälschung (ISO, 2017)

IV. Ersetzen von Komponenten (ISO, 2017).

V. Nicht erteilte Berechtigungen auf Fallebene.

VI. Keine Sicherstellung der Aufgabentrennung (z. B. zwischen Systemadministratoren, Bedienern und Ermittlern).

VII. Fehler beim Hochladen von beschlagnahmtem digitalem Material.

VIII. Unzureichende Kenntnisse über die Software.“ [269].

3. Der Verlust von Daten hat Auswirkungen auf die Datenverfügbarkeit, was zu Lasten der Ermittlungsdauer geht und zum anderen kann der Verlust von Daten auch zu Fehlfunktionen führen.

„Einige Hauptbedrohungen, die zum Verlust von Daten führen, sind wie folgt:

I. Überlastung der Verarbeitungskapazität (ISO, 2017).

II. Denial-of-Service-Angriff (CNIL, 2017).

III. Alterung der archivierten Dokumente (CNIL, 2017).

IV. Verlust des Verschlüsselungsschlüssels.

V. Einsatz von schlecht geschulten Mitarbeitern.

VI. Nicht ausreichend getestete Software/Hardware-Integration.“ [269].

Das größte Risiko ist die potentielle Manipulation durch Einfügen von kompromittierenden Daten auf beschlagnahmte Datenträger durch Behördenstellen, da der Betroffene im Nachhinein nicht eindeutig beweisen kann, dass diese Daten nicht von demjenigen stammen kann.

3.9.3 Risiken bei gestohlenen bzw. verlorenen IT-Systemen

Falls ein Smartphone verloren oder gestohlen geht, ist ein Missbrauch von darauf befindlichen Daten möglich. Durch die Nutzung über einen längeren Zeitraum fallen bei der Smartphone Nutzung riesige Mengen an Daten an, die zu anderen Zwecken missbraucht werden können. Daher hat SysAdmin, Audit, Networking and Security (SANS) zu den derzeitigen Forensik Möglichkeiten von Smartphone Betriebssystemen in Anlehnung an die anfallenden Datenmengen „The Most Relevant Evidence per Gigabyte“ [271] bezeichnet. Folgende Extraktionen sind möglich:

IOS Cheatsheet	Android Cheatsheet
Geräte Informationen	Geräte Informationen
Passwörter und Konteninformationen	Passwörter und Konteninformationen
Systemeinstellungen - System Kontrolle - Tastatur, Wörterbuch, Logdateien, BT Adressen, etc.	Systemeinstellungen
Systemeinstellungen - Nutzer Kontrolle - Synchronisationseinstellungen, Springboard, etc.	Nutzereinstellungen
Kommunikationen – SMS, Anrufe, E-Mails	Kommunikationen – SMS, Anrufe, E-Mails
Browser Aktivitäten	Multimedia
Multimedia	Browser Aktivitäten
Netzwerkverbindungen	Netzwerkverbindungen
Synchronisationsartefakte	Synchronisationsartefakte
Aufenthaltsartefakte	Aufenthaltsartefakte
Spuren der Zerstörung - Löschen, etc.	Applikations-Nutzungen
	Native Applikationen

Tabelle 1: Forensische Auswertungsmöglichkeiten vom I-Phone und vom Android [271]

Laut BSI Leitfaden Forensik sind insgesamt acht Datentypen extrahierbar, die wie folgt lauten: 1. Hardwaredaten, 2. Rohdateninhalte, 3. Details über Daten, 4. Konfigurationsdaten, 5. Kommunikationsprotokolldaten, 6. Prozessdaten, 7. Sitzungsdaten, 8. Anwenderdaten s. [272, pp. 81-82]. Mit den eben genannten Informationen kann - besonders mit Hilfe von Zugangsdaten - gezielt Schaden für den betroffenen Nutzer genommen werden. Mit Hilfe von Big Data Mechanismen kann ein umfassendes Bild - einschließlich des Persönlichkeitsprofils - des betroffenen Nutzers gewonnen werden.

3.9.4 Massenzugriff auf Kundendaten von Banken

In der Vergangenheit hat die Staatsanwaltschaft Halle auf Grundlage von § 161 a StPO im Fall des Erwerbs von kinderpornografischen Materialien über eine Webseite, die durch die Bezahloption Kreditkarte ermöglicht wurde, daraufhin alle Banken und Kreditkartenanbieter angeschrieben, um mögliche Personen zu identifizieren, die das beschuldigte Material erworben hatten s. [273, p. 20]. Betroffen von dieser Aktion waren in Deutschland fast 22 Mio. Kreditkartenkonten, wovon 322 identifizierte Personen an die Staatsan-

waltschaft Halle übermittelt wurden s. [273, p. 21]. Für dieses Vorgehen war im Gegensatz zur Rasterfahndung nach § 98a StPO kein richterlicher Beschluss notwendig gewesen s. [273, p. 21]. Unter Rasterfahndung ist zu verstehen, dass in „mehreren Schritten eine Datenauswertung aus unterschiedlichen Datenquellen durchgeführt“ [273, p. 24] wird, was hier bei diesem Fall nicht zutrifft, da jeweils eine Abfrage pro Bank erfolgte s. [273, p. 24]. Das Grundrecht auf informationelle Selbstbestimmung wird laut Gericht nicht durch diese Maßnahme unverhältnismäßig eingeschränkt s. [273, p. 25]. Selbst das BVerfG ist der Auffassung, dass § 161 Abs. 1 StPO eine „Generalklausel für Ermittlungsmaßnahmen“ [273, p. 28] sei und damit „auch eine zulässige Ermächtigungsgrundlage für die Ergebung von personenbezogenen Daten“ [273, p. 28], was „auch die Möglichkeit einer entsprechenden Ermittlungsanfrage an privaten Stellen“ [273, p. 28] miteinfließt s. [273, p. 28]. Inzwischen hat die Polizei des Landes Nordrhein-Westfalen 200 Lizenzen für eine Finanzanalyse Software eine halbe Mio. EUR ausgegeben, mit denen Geldströme noch besser verfolgt werden können s. [274].

3.9.5 Risiko fehlerbehaftete Attribution

Laut Kaspersky kann ein Angreifer verschiedene laufende Aktivitäten haben, so dass es schwieriger ist, denselben Ursprung zu identifizieren bzw. der gleichen Bedrohung zuzuordnen s. [275, p. 4]. Staatliche Akteure können leichter direkt die Infrastrukturen und Unternehmen angreifen, in denen sich die eigentlichen Opfer befinden s. [275, p. 4]. Das gilt auch für Internetanbieter, die durch Regularien zur Zusammenarbeit verpflichtet sind s. [275, p. 4]. Eine weitere Möglichkeit die Attribution zu erschweren, ist Aufträge an unterschiedliche Gruppen und Unternehmen zu vergeben, die wiederum unterschiedliche Tools und Techniken einsetzen, so dass die Zuordnung zu den Angreifern noch schwieriger ist, was eine Strafverfolgung und damit eine Bestrafung der tatsächlichen Angreifer erheblich erschwert s. [275, p. 4].

3.9.6 Verfassungsschutzbericht

Das Bundesamt für Verfassungsschutz (BfV) hat bezüglich fremder Nachrichtendienste folgende Aussage getroffen: „Fremde Mächte setzen gegenüber der Bundesrepublik Deutschland ihre Nachrichtendienste und … Mittel und Wege des verdeckten Agierens ein, um so Informationen zu erlangen, Einfluss auszuüben und ihre Interessen zu verfolgen.“ [276, p. 306]. Und weiter: „Die komplexe Bedrohung ist aus Sicht der Spionageabwehr tendenziell ansteigend.“ [276, p. 306]. „Neben Spionage gegen Politik und Verwaltung stehen auch … Unternehmen … im Fokus von Wirtschaftsspionage fremder Nachrichtendienste.“ „Die Ausforschung und Unterwanderung oppositioneller Gruppen aus Drittstaaten durch ausländische Dienste in Deutschland verursacht nicht nur ein Klima der Angst, sie kann auch eine Gefahr für Leib und Leben darstellen.“ [276, p. 306]. Zur Gefährdungsdimension Cyberangriffe stellt das BfV fest, dass es „eine anhaltende Bedrohung für unser Gesellschaft“ [276, p. 307] darstellt, da u.a. „die Angriffsfläche für

Cyberangriffe … global sprunghaft angestiegen“ [276, p. 307] sei. Auch Kritische Infrastrukturen sind „zunehmend der Gefahr durch Cyberangriffe ausgesetzt.“ [276, p. 308]. Im Detail schreibt das BfV, dass mutmaßliche chinesische APT-Gruppierungen ein zunehmendes Aufklärungsinteresse „an weltweiten Telekommunikationsnetzen haben, wovon „personenbezogene Daten (Personally identifiable information, PII) sowie telefonische Verbindungsdaten (Call Data Records, CDR) im Fokus der Angriffe“ [276, p. 325] stehen s. [276, p. 325]. Dort sind die „hochspezialisierten Angreifer in der Lage … derartige Telekommunikationsdaten massenhaft zu erheben und gezielt nach Individuen zu filtern sowie anhaltende Überwachungsmöglichkeiten gegen diese Personen zu etablieren.“ [276, p. 325]. Dabei kommen als „potenzielle Ziele … möglicherweise auch in Deutschland“ [276, p. 325] in Betracht. Diese Daten werden für Spionagezwecke genutzt s. [276, p. 325]. Darüber hinaus berichtet das BfV, dass ausländische Unternehmen mit geschäftlichen Tätigkeiten in China verpflichtet sind, „eine Software zu installieren, um automatisiert steuerliche Abgaben an das zuständige Finanzamt abzuführen sowie Finanztransaktionen abzuwickeln“ [276, p. 325]. Dabei wurde festgestellt, dass „durch die Installation dieser Software die Spionagesoftware GoldenSpy nachgeladen wurde. GoldenSpy könnte einem nicht näher identifizierten Angreifer Zugriff auf die Netzwerke der betroffenen Unternehmen ermöglichen.“ [276, p. 325]. Das Besondere an diesem Vorgehen ist, dass eine legitime chinesische Finanzsteuersoftware, welches aus gesetzlichen Gründen durch die ausländischen Unternehmen in China installiert werden muss, als Ausgangspunkt für Angriffe seitens der chinesischen Angreifer genutzt wird, um das jeweilige Firmennetzwerk infiltrieren zu können. Auch hier ist insgesamt mit den Jahren eine Zunahme aufgrund der zunehmenden Digitalisierung festzustellen. Was der nachgewiesenen Spionage - spätestens bekannt seit Edward Snowden - seitens US-amerikanischer Geheimdienste gegen Deutschland angeht, ist das BfV auffällig zurückhaltend. Hier schreibt das BfV dazu nur: „[B]eim Vorliegen tatsächlicher Anhaltspunkte für nachrichtendienstliche Aktivitäten in Deutschland auch solche Nachrichtendienste in den Fokus geraten, mit denen das BfV in anderen Zusammenhängen vertrauensvoll und partnerschaftlich zusammenarbeitet.“ [276, p. 334]. Hinsichtlich der methodischen Vorgehensweise ausländischer Nachrichtendienste wird seitens des BfV wie folgt festgehalten: „Spionage gegen Deutschland wird sowohl mit technischen als auch mit menschlichen Quellen durchgeführt, die offen oder konspirativ agieren.“ [276, p. 345]. „Fremde Dienste wählen dabei perspektivisch meist arglose Zielpersonen im Hinblick auf deren aktuelle und langfristige Zugangsmöglichkeiten aus. Mit geschickter Gesprächsführung gelingt es oftmals, sensible Informationen zu erlangen oder auch Hinweise auf weitere potenzielle Quellen zu gewinnen.“ [276, p. 346]. „Nachrichtendienste nutzen für Anbahnungsoperationen soziale Netzwerke wie Facebook oder die Karriereplattform LinkedIn. Der Modus Operandi ähnelt sich: Vermeintliche Wissenschaftler oder Jobvermittler nehmen Kontakt zu Personen auf, die für fremde Nachrichtendienste interessant erscheinen.“ [276, p. 347]. „Die weiter voranschreitende Digitalisierung hat der nachrichtendienstlichen Informationsbeschaffung neue Möglichkeiten eröffnet. Informationen, die früher nur durch menschliche Quellen zu erlangen waren, sind heutzutage verhältnismäßig leicht und ohne

größere Risiken auf technischem Weg zu beschaffen. Dazu gehört das Abhören inländischer Kommunikation und der internationalen Kommunikationsverbindungen über Server oder Internetknoten im Ausland.“ [276, p. 347]. „Fernmeldeaufklärungsmaßnahmen ausländischer Nachrichtendienste in Deutschland in Bezug auf relevante Informationen der Bundesregierung werden wegen ihrer günstigen Lage und Exterritorialität besonders von den jeweiligen Botschaftsgebäuden im Zentrum Berlins aus durchgeführt. Insbesondere im Regierungsviertel muss daher bei allen über Funk geführten Kommunikationsverbindungen (z.B. Gespräche mit Mobiltelefonen, WLAN- und Bluetooth-Verbindungen) mit einer Überwachung gerechnet werden. Auch in WLAN-Netzen eingebundene mobile Endgeräte und die darauf gespeicherten Daten könnten so einem unberechtigten Zugriff ausgesetzt sein.“ [276, p. 347]. „Cyberangriffe mit und gegen IT-Infrastrukturen haben sich als wichtige Spionage und Sabotagemethode ausländischer Nachrichtendienste etabliert. Sie umfassen das Ausspähen, Kopieren oder Verändern von Daten, die Übernahme einer fremden elektronischen Identität, den Missbrauch fremder IT-Infrastrukturen sowie die Übernahme computergesteuerter und netzgebundener Produktions- und Steuereinrichtungen. Solche Cyberangriffe können von außen über Computernetzwerke wie das Internet oder durch einen direkten, nicht netzgebundenen Zugriff auf einen Rechner erfolgen (z.B. über manipulierte Hardwarekomponenten wie USB-Sticks).“ [276, pp. 347-348]. „Seit 2005 werden in Deutschland zielgerichtete nachrichtendienstliche Cyberangriffe auf breiter Basis gegen Bundesbehörden, Politik und Wirtschaftsunternehmen festgestellt. … Die Dauer einzelner Angriffsoperationen und die globale Ausrichtung bei der Auswahl von Themen und Opfern weisen deutlich auf ein strategisches Vorgehen hin. Da die Angreifer die eingesetzten Schadprogramme permanent weiterentwickeln, steigt die Effektivität derartiger Angriffe. So werden die Methoden zunehmend komplexer. Zudem ist die Dunkelziffer nicht erkannter Cyberangriffe als hoch einzuschätzen.“ [276, p. 348]. „Einflussnahmeaktivitäten und Desinformation waren und sind gängige Handlungsoptionen von Staaten.“ [276, p. 349]. „Deutschland ist ein gegenüber ausländischen Direktinvestitionen offenes Land. Im Zuge eines Unternehmensaufkaufs kann es aber zu unerwünschten Informationsabflüssen kommen. Neben dieser Gefahr können ausländische Direktinvestitionen insbesondere im Bereich Kritischer Infrastrukturen zu Abhängigkeiten von staatlich kontrollierten ausländischen Investoren und - im äußersten Fall - zu entsprechenden sicherheitsrelevanten Kontrollverlusten führen.“ [276, p. 350].

3.9.7 Parlamentarische Nachrichtenkontrolle

Das Parlamentarische Kontrollgremium (PKGr) im Bundestag besteht aus neun Ordentlichen Mitgliedern, die G10-Kommission aus vier Mitgliedern und das Vertrauensgremium aus zehn Mitgliedern s. [277], s. [278], s. [279]. Zur Kontrollfähigkeit wurde konstatiert, dass „[d]ie Regierung … häufig unvollständig oder gar nicht über grundrechtsrelevante Praktiken der Nachrichtendienste [hier BfV, BND und MAD]“ [280, p. 68] unterrichtet und weiter zur Arbeit der Abgeordneten des PKGr: „[Diese haben] bei der Aufklärung von Vorwurfsfällen regelmäßig nicht die gebotene Sorgfalt walten lassen“ [280, p. 68].

Dies wurde auch durch das Bundesverfassungsgericht bestätigt, dass die bisherige Kontrollpraxis „nicht den Anforderungen an eine ausgebaute unabhängige objektiverechtliche Kontrolle“ [281] genügt. Auch ist festzustellen, dass „ganze Bereiche des exekutiven Handelns von der Kontrolle ausgenommen werden (wie bisher die strategische Auslandsfernmeldeaufklärung), Kontrollerituale weiterhin … nur zeremoniell genutzt werden“ [280, p. 68], was zum folgenden Fazit führt: „[es] fehlt dem Regierungshandeln strenggenommen die Legitimität.“ [280, p. 68]. Beweis hierfür sind u.a. die zahlreichen Untersuchungsausschüsse zu nachrichtendienstlichen Themen bei fast jeder Legislaturperiode s. [280, p. 77]. Diese wären nicht nötig gewesen, wenn „eine effiziente Kontrolle gewährleiste[t]“ [280, p. 77] wäre. Darüber hinaus kommt eine „staatsorganisatorisch bedingte Nähe zwischen Regierung und Parlamentsmehrheit und der durch sie bestimmten Bundestagsverwaltung.“ [282, p. 190]. Daher ist eine unabhängige Kontrollinstanz wie es bspw. der Bundesrechnungshof darstellt, erforderlich s. [282, p. 190]. Vor diesem Hintergrund kann die Bundesregierung „auf diese für sie günstigen Kontrollstrukturen vertrauen“ [282, p. 190], so dass „keine ernsthaften Probleme“ [282, p. 190] zu erwarten sind. Ob die inzwischene angegangene Reform der Nachrichtendienstkontrolle die bisherigen Defizite beseitigt, bleibt abzuwarten.

3.9.8 Risiko Daten von Unternehmen bzw. Nutzung von Dienstleistern durch Geheimdienste

Ein exemplarisches Beispiel ist die Nutzung eines privaten Dienstleisters durch den Secret Service. Der Dienstleister Babel Street ermöglicht mit Hilfe des Tools Locate X dem Secret Service „Bewegungen von Personen ohne Durchsuchungsbefehl zu verfolgen.“ [283]. Locate X versorgt seine Kunden mit geografischen Daten aus mobilen Apps, die ihre Koordinaten oft über Werbung oder vorgefertigten Code, der in die App eingebettet ist, … an unbekannte Dritte weiterzugeben.“ [283]. Die Standortdaten „werden in zahllosen Apps erfasst und zwischen einem … großen und … wachsenden Ökosystem von Ad-Tech-Firmen und Datenmaklern auf der ganzen Welt gekauft, verkauft und ausgetauscht, bis sie schließlich im Besitz von Babel Street landen, das den Suchzugang an Regierungskunden … verkauft.“ [283]. Damit kann u.a. der Secret Service feststellen, „welche Personen sich zu einem bestimmten Zeitpunkt an einem bestimmten Ort aufhielten - und sogar, woher sie kamen und wohin sie in den vorangegangenen Monaten gereist waren.“ [283] und das weltweit. Durch diese Vorgehensweise wird faktisch der Rechtsschutz aufgehoben bzw. sogar noch verschlimmert, da dessen Erkenntnisse aus dem Tool „für die Verwendung in Gerichts- oder Verwaltungsverfahren ungeeignet sei.“ [283], sprich verschwiegen werden soll. Selbst auf eine Anfrage eines Senators, hier Ron Wyden, hat der Dienstleister keine Rückmeldung gegeben s. [283]. Dieser Vorgang ist nur durch eine Informationsfreiheitanfrage an die Öffentlichkeit gelangt s. [283]. Es ist davon auszugehen, dass es eine Vielzahl weiterer Kooperationen gibt, insbesondere im Geheimdienstbereich, was nicht nur auf Amerika beschränkt ist. Allein die Tatsache, dass der Kongress der Vereinigten Staaten von Amerika sich mit dem Thema „[W]ie Datenbroker

Smartphone-Tracking-Informationen an Strafverfolgungsbehörden verkauft“ [284] befasst hat, zeigt auf, wie sensibel dieses Thema ist.

3.9.9 Manipulation der Kryptographie bzw. der Verschlüsselungssysteme

Die NSA hat an das Sicherheitsunternehmen RSA Security 10 Mio. US-Dollar bezahlt, „um den umstrittenen Zufallsgenerator Dual_EC_DRBG als Standard“ [285] einzusetzen. Dieser Zufallsgenerator war mit einer Hintertür ausgestattet gewesen und wurde in „[t]ausenden von kommerziellen Produkten eingesetzt“ [285], u.a. auch in OpenSSL s. [285]. Darüber hinaus wurde bekannt, dass die NSA einen Mitarbeiter im „Kryptographie-Beratungsgremium … des Internet Engineering Task Force“ (IETF) hatte, der sich für ein Projekt einsetzte, was von der Arbeitsgruppe nicht mehr weiterentwickelt wurde [286]. Die beiden Vorgehensweisen weisen ein Muster auf, dass sich mit den Veröffentlichungen durch Edward Snowden abdeckt. Ein internes klassifiziertes Dokument der NSA listet u.a. folgende Methoden auf, um die Kryptographie gezielt zu schwächen:

„“Einfügen von Schwachstellen in kommerzielle Verschlüsselungssysteme, IT-Systeme, Netzwerke und Endpunkt-Kommunikationsgeräte, die von Zielpersonen genutzt werden“ - Sabotage unserer Systeme durch Einfügen von Hintertüren und anderweitige Schwächung, wenn die Möglichkeit besteht, dass eine "Zielperson" diese ebenfalls nutzt.

„Aktive Einbindung US-amerikanischer und ausländischer IT-Industrien zur verdeckten Beeinflussung und/oder offenen Ausnutzung der Designs ihrer kommerziellen Produkte“ - Heimliche Infiltration von Unternehmen, um diese Sabotage durchzuführen, oder Zusammenarbeit mit Unternehmen, um Schwachstellen in ihre Systeme einzubauen oder sie zu zwingen, im Geheimen mitzumachen.

„Gestaltung des weltweiten kommerziellen Kryptographiemarktes, um ihn für die von NSA… entwickelten fortgeschrittenen kryptoanalytischen Fähigkeiten zugänglicher zu machen - Sicherstellen, dass der globale Markt nur kompromittierte Systeme enthält, so dass die Menschen keinen Zugang zur sichersten Technologie haben.

„Diese Konstruktionsänderungen machen die fraglichen Systeme durch Sigint-Sammlungen ausnutzbar ... mit Vorwissen über die Modifikation. Für den Verbraucher und andere Angreifer bleibt die Sicherheit der Systeme jedoch intakt.“ - Sicherstellen, dass niemand weiß, dass die Systeme kompromittiert worden sind.

„Einflussnahme auf Richtlinien, Standards und Spezifikationen für kommerzielle Public-Key-Technologien“ - Sicherstellen, dass die Standards, auf die sich jeder verlässt, Schwachstellen aufweisen, die vor den Benutzern verborgen sind.“ [287], [288].

Ein zusätzliches Risiko ist folgendes Szenario, welches von der NSA praktiziert wird. Die NSA ist in der Lage „bis zu 140 Terrabyte für jede Person in der Welt“ [289, p. Folie 46] [9] zu speichern. Dies schließt auch die Tatsache mit ein, dass diese verschlüsselte

[9] Die Folien zu diesem Video wurden per E-Mail zugesandt.

Nachrichten jetzt speichern kann, um es in Zukunft entschlüsseln zu können, wenn entsprechende Angriffsmöglichkeiten sich eröffnen, wie es bereits - laut GHCQ - realisiert wird s. [290]. Wenn in Zukunft Quantencomputer einsatzfähig sein werden, sind neue Entschlüsselungsmöglichkeiten vorhanden s. [289, p. Folie 46]. Bei Einsatz von Quantencomputern sind u.a. Angriffe auf Signaturen, auf den Schlüsselaustausch sowie auf die Verschlüsselung selbst möglich s. [291]. In diesem Zusammenhang ist zu konstatieren, dass „die [gegenwärtig eingesetzte] Verschlüsselung nicht verlängert werden kann“ [289, p. Folie 46].

Das im Bereich der Kryptographie nicht allein auf zertifizierte Produkte nach Common Criteria (CC) oder nach dem Federal Information Processing Standard vom National Institute of Standards and Technology (NIST FIPS 140-2) gesetzt werden darf, zeigt das Beispiel des vom BSI nach CC EAL 5+ zertifizierten Infineon Security Controller auf s. [292]. Forscher konnten eine Schwachstelle bei der Generierung von RSA-Schlüsseln, die von einer Software-Bibliothek verwendet wird, aufzeigen s. [293]. Diese Schwachstelle ermöglicht es, den privaten Teil des RSA-Schlüssels zu berechnen s. [293]. Die Auswirkungen allein von dieser Schwachstelle sind so groß, dass u.a. elektronische Ausweise betroffen sind - Estland musste die Zertifikate erneuern -, TPM-Chips, die in Laptops verbaut sind, Authentisierungstoken wie Yubikey, die Signierung von Softwarepaketen wie Debian mussten aktualisiert bzw. erneuert werden s. [293], s. [294]. „[E]ine Haftung für Schäden sieht Common Criteria nicht vor“ [295], so dass Firmen auf ihre Kosten durch den Mehraufwand sitzenbleiben. Durch diese Schwachstelle hätten Angreifer die Möglichkeit gehabt, mithilfe des berechneten privaten Schlüssels „Nachrichten zu entschlüsseln, Signaturen zu fälschen … und andere verbundene Angriffe auszuführen“ [293]. Kein Vorbild war das BSI hinsichtlich des Umgangs zu der Zertifizierung des betroffenen Produkts gewesen. Trotz mehrfacher Nachfragen seitens der Presse hat das BSI keine Stellungnahme abgegeben, was angesichts der sehr kritischen Komponente und der Schwere der Auswirkungen nicht vertrauensförderlich ist s. [295].

Ein weiteres exemplarisches Beispiel, an dem der BND sowie die CIA involviert waren, war die Schweizer Firma Crypto AG, die Verschlüsselungsgeräte herstellte und an über einhundert Staaten auslieferte, während die Schwesterfirma Infoguard AG die Verschlüsselungsgeräte an die Privatwirtschaft verkaufte s. [296]. Beide Firmen haben u.a. manipulierte Verschlüsselungsgeräte verkauft, so dass mit Hilfe einer eingebauten Hintertür der BND und die CIA abhören konnten s. [296]. Dies galt nicht für Behörden in der Schweiz, in Deutschland und in Schweden sowie den Geschäftsbanken s. [296]. Damit waren sowohl Bürger direkt als auch indirekt betroffen, sei es durch Polizeimaßnahmen, die die manipulierten Geräte einsetzten oder durch den Kontakt mit Firmen, die ebenfalls diese manipulierten Geräte im Einsatz hatten.

3.9.10 Rufschädigung und Überwachung durch den GHCQ

Der GCHQ hat sich - neben anderen Spionagemethoden - systematisch mit der Rufschädigung über das Internet beschäftigt. Zu den Methoden gehören u.a. wie folgt: „eine Honigfalle aufstellen [eine Sexfalle], die Fotos auf sozialen Netzwerkseiten ändern, E-Mails/Texte im Namen der Zielperson an Kollegen, Nachbarn, Freunde schicken“ [297]. Das gleiche gilt auch für die Diskreditierung von Firmen, hier sind die Methoden wie folgt: „vertrauliche Informationen an Foren weitergeben/ via blogs die Presse informieren, negative Informationen posten auf geeigneten Foren, Deals stoppen/Geschäftsbeziehungen ruinieren“ [297]. Der Einsatz dieser Methoden ist gefährlich und auch rechtlich fragwürdig, da „mit dieser Art von Online-Täuschungstaktiken zur Rufzerstörung und Störung beliebige Personen ins Visier … [genommen werden] können, die nie eines Verbrechens angeklagt, geschweige denn verurteilt worden sind.“ [297]. Das Fazit eines Weltartikels dazu: „Traue niemanden, gebe nie etwas preis“ [298]. Darüber hinaus überwacht der GHCQ das Internet, indem Glasfaserverbindungen „an[ge]zapft und für bis zu 30 Tage zwischengespeichert“ [299] werden. Darunter ist das Überseekabel TAT-14 betroffen, bei der die Deutsche Telekom eines der Betreiber ist. Darüber hinaus kooperiert der GHCQ mit British Telecommunications, Level-3, Viatel, Interoute, Verizon und Vodafone, deren Unternehmen ebenfalls auch in Deutschland tätig sind s. [300].

3.9.11 Der amerikanische Geheimdienst NSA

Durch die Veröffentlichungen von Edward Snowden wurde in Deutschland ein Untersuchungsausschuss zur NSA-Affäre im Bundestag durchgeführt s. [301]. Vernommen wurde u.a. Herr Andreas Könen, der damals Vizepräsident (VP) des BSI war s. [302]. Selbst als Experte, der vormals für den BND im Leitungsstab zuletzt gearbeitet hatte, war er vom Ausmaß der Überwachung überrascht gewesen: „Die Aktivitäten der NSA in dieser Hinsicht überraschen allerdings hinsichtlich des mengenmäßigen Ausmaßes der Erfassung und hinsichtlich der Dichte der weltweit existierenden Erfassungspunkte. Die durch die strategische Aufklärung gewonnenen Daten werden mittels verschiedener Analysetools ausgewertet und relevante Inhalte herausgefiltert. Hier ist die enge und weitgehende Verknüpfung von Metadaten, also Verkehrsdaten, über viele verschiedene NSA-Programme hinweg auffallend. Die Ergebnisse werden offenbar gerade auch bei der Durchführung von individualisierten Angriffen weiter genutzt. Dies geschieht beispielsweise durch das direkte Abhören von Kommunikation; dort, wo Netzwerke etwa über Funkstrecken geführt werden, zum Beispiel WLAN, Richtfunk bei Mobilkommunikation oder Satellitenverkehre, sind Daten den klassischen Abhörangriffen ausgesetzt.“ [302, pp. 10,12]. Hier sprach er von zwei Merkmalen, einerseits die Massenüberwachung und andererseits wird eben durch die Massenüberwachung ermöglicht, individuelle Angriffe durchzuführen. Desweiteren sprach er von der Abteilung „Tailored Access Operations“ (TAO), die u.g. gezielt Endgeräte kompromittiert mit „Advanced Network Technology“ (ANT), womit die Endgeräte manipuliert werden s. [302, p. 10]. Selbst hier war er ebenfalls vom Ausmaß überrascht gewesen: „Man muss … konstatieren, dass viele dieser An-

griffsvarianten von uns und anderen Fachleuten bisher jedoch als unpraktikabel angesehen wurden. Hier haben uns die Veröffentlichungen verdeutlicht, dass wir in nachrichtendienstlichem Umfeld jederzeit mit unüblichen, teuren und vermeintlich unpraktikablen Vorgehensweisen rechnen müssen.“ [302, p. 10]. Zudem muss berücksichtigt werden, dass allein die NSA über 46.000 Mitarbeiter (MA) verfügt und vergleichsweise für den Cyberbereich der BND, das BSI und der Verfassungsschutz zusammen nur 1.300 MA vorweisen kann s. [303, p. 8]. Allein die Personalstärke der deutschen Behörden zeigt auf, dass bei weitem nicht die Fähigkeiten und Kapazitäten wie bei der NSA bestehen. Noch größer wird der Abstand durch die Zusammenarbeit der NSA mit den Five-Eyes - hier GHCQ, Australischer -, Neuseeländischer - und Kanadischer Geheimdienst -, so dass noch mehr Möglichkeiten zur Verfügung stehen. Was dabei bislang nicht im Fokus stand, ist die Zusammenarbeit der Geheimdienste in den USA mit Privatfirmen. Allein die fünf größten Privatunternehmen (Leidos, Booz Allen Hamilton, CSRA, SAIC, CACI) verdienten zusammen im Jahr 2015 16 Mrd. Dollar mit IT-Aufträgen und rund 45.000 externe MA arbeiten für die NSA, der CIA und weiteren Behörden s. [304]. Dies veranlasste den Autor zu diesem Thema zur folgenden Aussage: „Diese nicht rechenschaftspflichtige Oligarchie von Spionen kontrolliert die Informationen, die unsere militärischen und zivilen Führungskräfte leiten.“ [304], was demokratisch nicht abgedeckt ist und zuletzt im Jahr 2014 im US-Kongress besprochen wurde s. [304]. Vor diesem Hintergrund wurde in einer Studie festgehalten, dass „die wirtschaftlichen Interessen des Landes nicht angemessen vor Spionage geschützt werden“ [303, p. 8] kann, zumal die Dienstleister für die Geheimdienste auch eigene Interessen verfolgen, was selbst ein Risiko darstellt, da ein Missbrauch der erhobenen Daten zu anderen Zwecken nicht ausgeschlossen werden kann.

Hinsichtlich über Schutzmaßnahmen äußerte er sich wie folgt: „Ein Schutz vor strategischer Aufklärung kann vor allem durch einen umsichtigen Umgang mit persönlichen und beruflichen Daten erreicht werden. Insbesondere durch konsequente oder Ende-zu Ende-Verschlüsselung kann die Vertraulichkeit von Kommunikationsinhalten erreicht werden, durch konsequente Verschlüsselungen von gesamten Kommunikationsstrecken auch ein weitgehender Schutz von Verkehrsdaten.“ [302, p. 10]. Was Daten angeht, die einer hohen Vertraulichkeit unterliegen fordert er: „Zur Absicherung von Daten mit sehr hohem Schutzbedarf … werden von uns durch die Entwicklung und den Schutz eigener Algorithmen bzw. eigener Parameter zu bekannten Verfahren zusätzliche Sicherungsebenen eingebaut.“ [302, p. 11].
Der ehemalige IT-Direkter des BMI, Martin Schallbruch, hat im gleichen Ausschuss u.a. ausgesagt, dass „dass die Qualität der Informationstechnik sich über die letzten 10, 15 Jahre nicht wirklich gebessert hat, also die Qualität der Software- und Hardwareprodukte, dass die Abhängigkeit von Staat, Gesellschaft, Wirtschaft von Informationstechnik im gleichen Zeitraum immens zugenommen hat, dass sich eine komplexe Bedrohungslage entwickelt hat, in der viele Player aus dem Bereich der Kriminalität - Konkurrenzausspähung usw. usf. -, auch nachrichtendienstliche Akteure, militärische Akteure das Thema IT- und Cyberangriffe für sich entdeckt haben.“ [302, p. 77]. Als Fazit teilt er mit: „Die Verantwortung für IT-Sicherheit kann kein Akteur allein herstellen, weder Hersteller von

Systemen noch Nutzer noch der Staat. Die Lösung der Probleme der IT-Sicherheit erfordert immer ein Zusammenwirken unterschiedlichster Akteure.“ [302, p. 77].

Hinsichtlich des Umfangs der Datendimension wurden die Stasi-Aktenschränke (48.000 Aktenschränke ergibt ein Bedarf für 0,19 km²) mit dem von der NSA verglichen s. [305]. Wenn 5 Zettabytes ausgedruckt würden, wären das 42 Billionen Aktenschränke, was von der Fläche her über 1 1/2 mal so groß von Europa einnehmen würde (etwa 17 Mio. km² von 10,5 Mio. km²) s. [305], s. [306].

3.9.12 Zwischenfazit

Der Bürger ist verpflichtet seine Identitätsdaten (u.a. Unterschrift, Passfoto) an die Einwohnermeldestelle zu liefern, an dem eine Vielzahl weiterer Organisationen digital Zugriff hat. Dadurch bestehen hier zwei prinzipielle Risiken, in der mind. das Schutzziel Vertraulichkeit betroffen ist. Zum einen das direkte Risiko durch Innentäter. Bspw. hat eine Mitarbeiterin einer Magdeburger Klinik unbefugt die Einwohnermeldedaten in 182 Fällen abgerufen, um diese an Linksextremisten weiterzugeben, damit Personen aus der rechten Szene geschädigt werden s. [307]. Auch häufige Missbräuche polizeilicher Informationssysteme - hier durch Berliner Polizisten - ist von der Berliner Datenschutzbeauftragten festgestellt worden s. [308]. Allein die Berliner Polizei kann auf über 130 Datenbanken einschließlich der Datenbanken des BKA zugreifen s. [309]. Insgesamt bleibt die Dunkelziffer von Innentätern in Behörden - wie es in Unternehmen ebenfalls der Fall ist - hoch, zumal die Forschungsbeiträge auf diesem Gebiet marginal sind s. [310]. Zum anderen das indirekte Risiko durch schlecht geschützte IT-Systeme der öffentlichen Verwaltung, hier insbesondere auf kommunaler Ebene s. [311]. Es besteht deswegen ein hohes Risiko zu einem Datenabfluss bzw. dass durch Angriffe bspw. durch Ransomware keine Arbeitsfähigkeit gegeben ist, womit zusätzlich das Schutzziel Verfügbarkeit betroffen wäre. Auch Fehler bei der Vernichtung von scheinbar gelöschten Speichermedien kommen häufig vor, so dass u.a. vertrauliche Meldedaten einschließlich Passfotos und Originalunterschriften auf eBay ersteigert wurden s. [312]. Dies gilt nicht nur für Meldedaten, sondern auch analog u.a. für Führerscheinstellen, Finanzämter sowie Rentenversicherungsanstalten. Gerade die letzten beiden öffentlichen Stellen verfügen über den umfangreichsten Datensatz an Bürgern.

Vor diesem Hintergrund muss zukünftig einerseits eine persönliche Haftung für die politische Leitungsebene erfolgen, wenn die Mindeststandards zur Informationssicherheit in den jeweiligen Behörden grob fahrlässig vernachlässigt wurden. Andererseits muss sowohl der interne als auch externe Datenschutzbeauftragte regelmäßig Stichproben durchführen, ob Zugriffe immer protokolliert werden und ob diese berechtigt waren. Denn eine stichprobenartige rein interne Datenschutzprüfung reicht nicht immer aus, wie der Datenschutzskandal bei der Bremer Polizei aufzeigt. Trotz einschlägiger Gesetze wurden personenbezogene Daten weiterhin jahrelang aufbewahrt, anstatt diese fristgerecht zu löschen s. [313]. Auch wenn die Polizeibehörde in Bremen einen eigenen Datenschutzbe-

auftragten hat, ist nicht sichergestellt, dass dieser seiner Kontrollpflicht umfassend nachkommt s. [314]. Wenn die Bürger einerseits gesetzlich gezwungen sind, ihre Daten an Behörden abzugeben, muss adäquat andererseits hier Transparenz vorherrschen, ob die jeweilige Behörde die Mindeststandards der Informationssicherheit einhält. Die Überprüfung hat mind. einmal jährlich von Rechnungshofsprüfern zu erfolgen und der Bericht als Zusammenfassung ist zu veröffentlichen anstatt es - wie bisher - unter Verschluss zu halten.

Was die Kontrolle der Geheimdienste angeht, so scheitert die Parlamentarische Kontrolle allein aufgrund mangelnder Ressourcen einschließlich des fachlichen Personals auf Seiten der Abgeordneten. Darüber hinaus muss konstatiert werden, dass dem BND vormals illegale Tätigkeiten im Nachhinein legalisiert wurden, d.h. deren Befugnisse wurden sogar erweitert anstatt die Kontrollen nachhaltig zu verschärfen und eine Evaluation vorzunehmen, ob die bereits bestehenden Befugnisse noch notwendig bzw. zweckmäßig sind.

4. Gesamtwürdigung und Erweiterung des Begriffs Informationssicherheit

Die Digitalisierung durchdringt auf der einen Seite immer mehr Lebensbereiche, so dass auf der anderen Seite zugleich die Abhängigkeit und damit die Vulnerabilität für die Gesellschaft insgesamt erhöht wird. Dies schließt auch das zunehmende Überwachungspotential sowohl seitens der Unternehmen als auch der Staaten mit ein. Der neuralgische Punkt für die IT-Systeme ist die Stromversorgung. Ohne diese funktionieren die IT-Systeme nicht mehr bzw. nur noch für einen bestimmten Zeitraum u.a. in Rechenzentren oder Mobilfunkanlagen. Durch die Digitalisierung entstehen darüber hinaus Netzwerk- bzw. Sogeffekte, so dass inzwischen bspw. Gebühren - auf das Bundesland Berlin bezogen - für einen Personalausweis nicht mehr in bar bezahlt werden können, obwohl laut § 14 Bundesbankgesetz die Barzahlung gesetzlich vorgegeben ist. Auch die sog. Freiwilligkeit ist kritisch zu betrachten, da es auf langer Sicht zum Zwang kommen kann. Bereits heute sind bzw. waren Zugänge zu Organisationen z.T. nur möglich, wenn die Luca-App installiert war. Für Bürger, die nicht die unsichere Luca-App nutzen wollen bzw. keinen Smartphone besitzen, wird es daher schwieriger - trotz Vorhandenseins eines Impfausweises - sich an gesellschaftlichen Aktivitäten zu beteiligen s. [315], s. [316]. Diese Art des Vorgehens ermöglicht u.a. die Gefahr der Ausgrenzung. Darüber hinaus zeigt die aktuelle Lage auf, dass Bürger in Russland u.a. Amazon Pay sowie Paypal nicht nutzen können, so dass hier eindrucksvoll vorgeführt wird, dass die digitale Bezahlung mit erheblichen Risiken verbunden ist, erst recht, wenn mit dieser Art von Bezahlung langfristig dauerhafte Abhängigkeiten geschaffen werden s. [214]. Unabhängig davon gibt es das Risiko des dauerhaften Datenabflusses bei den jeweiligen Anbietern. Auch zeigt dieser Fall exemplarisch auf, dass hier geostrategische Interessen ebenfalls eine Rolle spielen und dadurch die Abhängigkeit von IT-Systemen auch von diesem Blickwinkel betrachtet werden müssen, um vor allem das Schutzziel Verfügbarkeit nicht zu gefährden. Eine Lebensführung ohne Einsatz von IT-Systemen wird immer aufwendiger, so dass der Handlungsspielraum des Bürgers sich zunehmend verkleinert. Mit wachsender Anzahl von IT-Systemen steigt der Aufwand zur Wartung und gleichzeitig wächst der Informationsfluss sowie der Strombedarf. Da IT-Systeme von der Stromversorgung abhängig sind, muss hinsichtlich der Versorgungssicherheit konstatiert werden, dass diese mittelfristig nicht vollständig gewährleistet ist, wenn Deutschland durch einen erhöhten Zukauf vom Strom aus dem Ausland dadurch noch größer abhängig wird. Verschärft wird diese Lage, weil in Deutschland mehrere Kraftwerke zum Jahresende 2022 bzw. bis Ende 2030 abgeschaltet werden s. [317].

Das Risiko eines Datenabflusses steigt mit zunehmender Nutzeranzahl von Onlineanbietern wie bspw. Alphabet oder Meta, Banken oder öffentlichen Institutionen. Je mehr Daten vorliegen, desto attraktiver wird es für private wie auch staatlich organisierte Angreifer. Besonders die Plattformen amerikanischer Anbieter sind aufgrund ihrer Datenmacht sehr kritisch zu betrachten. Dies gilt analog auch für chinesische Anbieter, die für den deutschen Nutzer jedoch eine marginale Rolle spielen. Daher ist jedwede Form „einer

zentralisierten Kontrolle über Informationen, ob staatlich [hier Geheimdienste] oder privat, mit der Freiheit unvereinbar.“ [304]. Das bisherige Instrumentarium des europäischen Kartellrechts reicht nicht aus, um die Plattformen bzw. Datenhändler nachhaltig Einhalt zu gebieten bzw. ggf. als ultima ratio zu zerschlagen.

Zwar ist einerseits in der DSGVO das Prinzip der Datensparsamkeit (Privacy-by-Design, Privacy-by-default) enthalten, andererseits herrscht „ein erhebliches Vollzugsdefizit“ [318, p. 13], insbesondere ggü. den Plattformen durch die Datenschutzaufsichtsbehörden. In diesem Zusammenhang ist weiterhin offen, „wie diese Regeln für [außereuropäische] Unternehmen“ [318, p. 13] durchgesetzt werden können. Auch fehlt bislang die rechtliche Möglichkeit, ein „Datenschutz-Verbandsklage“ [318, p. 13] durchzuführen, da der Einzelne i.d.R. nicht die finanziellen Möglichkeiten hat, mit spezialisierten Rechtsanwälten gegen Verstöße vorzugehen.

Die Ausübung des Grundrechts auf informationelle Selbstbestimmung des einzelnen Nutzers ist aufgrund der zunehmenden Anzahl von Onlinediensten sowie der Vernetzung der IT-Systeme erheblich aufwändiger und komplexer geworden. Besonders bei den Onlineanbietern ist das Nutzungsdesign meist so gestaltet, dass die Ausübung der Selbstbestimmung über die Preisgabe sowie Verwendung der persönlichen Daten bewusst erschwert wird. Letzten Endes liegt eine Tendenz zur Fremdbestimmung vor, in dem die Anbieter selbst über die Daten der Nutzer verfügen. Jede Nutzung von Apps ist prinzipiell sowohl ein Sicherheits- als auch ein Datenschutzrisiko. Denn sobald eine App installiert ist, ist kein effektiver Schutz mehr möglich. Markant wurde es vom ehemaligen NSA Chef Michael Hayden wie folgt formuliert: „Vierhunderttausend Apps bedeuten 400,000 Möglichkeiten für Attacken.“ [319] einschließlich der Tatsache, dass u.a. GHCQ auch die Daten von Drittanbietern - hier bspw. die Firma Dataflurry - abgreifen kann s. [320, p. Folie 45], s. [321]. Desweiteren wurde festgestellt, dass selbst bei über 1/3 aller Bezahlapps dennoch die gleichen sensitive Daten an Drittparteien übermittelt werden wie bei den kostenfreien Apps s. [322]. Daher bieten „bezahlte Apps ebenfalls keine Garantie dafür, dass es mehr Privatsphäre oder Anonymität für den Verbraucher gibt“ [322]. Im Gegenteil: „[W]eder Plattformen noch Apps [bieten] einen Mechanismus, um Verbraucher über die Verhaltensunterschiede zwischen kostenpflichtigen und kostenlosen Versionen der gleichen App zu informieren“ [322]. Darüber hinaus wurde festgestellt, dass „40 % der noch verfügbaren Apps keinen Link zu ihren Datenschutzrichtlinien im Google Play Store haben“ [322]. Dies gilt insbesondere für Apps, die erhöhte Risiken aufweisen, wie bspw. Medizinische Apps, Partnerschafts-Apps, Menstruations-Apps etc.. Darüber hinaus speichern amerikanische Unternehmen die Daten viel länger, aus dem Grund, dass durch zukünftige neue Big-Data-Verfahren - verbunden mit KI - neue Analysemöglichkeiten für die bestehenden Datensammlungen geben wird und damit verbunden neue Auswertungsverfahren, die noch tiefere Erkenntnisse über die einzelnen Nutzer bzw. Nutzergruppen zu Tage befördern kann - sei es im Bereich Interessen oder neue Ansatzpunkte für Kaufanreize zu schaffen etc.-.

Um sich langfristig schützen zu können, muss die Politik - mindestens auf der europäischen Ebene - den Datenhandel über persönliche Daten, einschließlich der Sammlung von Metadaten der (EU-)Bürger verbieten und eine grundsätzliche Datensparsamkeit aufseiten der Hersteller sowie Anbietern von Onlinediensten anordnen. Daher ist wieder ein „Verbot der Protokollierung des Surfverhaltens im Netz durch Internet- und Medienkonzerne“ [318, p. 13] einzuführen. Konkret sollen Daten beim Besuch von Webseiten nicht mehr gespeichert werden - mit Ausnahme von Protokollen zur Gewährleistung der Betriebssicherheit auf Seiten der Anbieter. Trackingdienste jedweder Art sind gesetzlich zu untersagen, da diese u.a. eine Profilbildung ermöglichen und u.a. von Geheimdiensten genutzt werden, worüber der Nutzer auf lange Sicht keine Einflussmöglichkeit hat. Dies schließt auch ein Verbot des Einsatzes von sog. Dark Pattern mit ein. Ein Verbot ist unumgänglich, da selbst eine datenschutzfreundliche Umstellung nicht genügen würde, solange das Geschäftsmodell so attraktiv ist, dass auch eine Umgehung in Kauf genommen wird, wie es bereits jetzt praktiziert wird. Allein die Trackingdienste von Facebook werden bereits von drei Viertel aller deutschen Nachrichtenseiten und Verlagsangebote (Gesamt: 130) genutzt, bei dem die Nutzerdaten an Facebook gesendet werden s. [323]. Ein Test bei der Webseite Süddeutschen Zeitung (SZ) ergab insgesamt 27 Treffer, wobei nicht alle Trackingdienste damit erfasst werden können s. [324]. Tatsächlich nutzt die SZ laut Richard Gutjahr insgesamt 470 Tracker s. [325]. Daher können solche Analysen nur als Hinweis genommen werden, ob eine Webseite Trackingdienste einsetzt oder nicht. Insgesamt nutzen sowohl öffentliche als auch private Nachrichtenseiten einschließlich Blogging Seiten besonders viele Tracker, was kritisch zu betrachten ist, da u.a. die politische Einstellung des Nutzers herausgefunden werden kann, was laut der DSGVO zu den besonderen Kategorien personenbezogener Daten zählt. Die Möglichkeit, einen Blog ohne Trackingdienste zu betreiben, zeigt bspw. der Blog des Informationssicherheitsexperten Felix von Leitner - blog.fefe.de - (Stand: 25.03.2022) auf.

Der Einsatz von KI ist für Nutzer besonders kritisch zu betrachten, da dieser kaum nachvollziehen kann, wie Entscheidungen getroffen wurden und zum anderen ist dieser bereits systemisch im Nachteil ggü. der jeweiligen Organisation, die KI anwendet. Hinzu kommt die Herausforderung, dass es bislang kein einheitliches Rahmenwerk zum sicheren Umgang mit KI gibt. Dies gilt erst recht für die ganzheitliche Betrachtung, in dem u.a. die potentiellen Auswirkungen auf die Gesellschaft mitbetrachtet werden müssen.

Hinsichtlich der sozialen Medien ist von einer Nutzung abzuraten, da nicht nur das Schutzziel Vertraulichkeit gefährdet ist, sondern auch potentielle Folgen von meist zweckentfremdeten Analysen und Auswertungen personenbezogener Daten durch die sozialen Anbieter als auch auf Seiten der Behörden einschließlich der Geheimdienste beinhaltet.

Vor diesem Hintergrund sind IT-Systeme einerseits so zu gestalten, dass diese eine sichere Nutzung durch den Nutzer gewährleisten können. Zum anderen sind IT-Systeme so zu entwickeln, dass von Anfang eine Komplettverschlüsselung nach Stand der Technik implementiert ist, dies betrifft nicht nur die automatisierte Verschlüsselung von lokalen

Daten sowohl auf Seiten des Nutzers als auch auf Seiten des jeweiligen Anbieters, sondern insbesondere eine durchgehende Ende-zu-Ende-Verschlüsselung einschließlich Transportverschlüsselung bei Onlinenutzung. Die Transportverschlüsselung dient vor allem dazu, die Metadaten zu ändern, so dass nicht mehr ersichtlich wird, wer mit wem direkt kommuniziert. Als Druckmittel kann auf Seiten der Politik angeregt werden, dass die Provider bzw. Backboneanbieter - mit einer gewissen Vorlaufzeit - keine unverschlüsselten Daten mehr übertragen dürfen, so dass hier insbesondere die IoT-Hersteller in der Pflicht sind, bereits bei der Entwicklung Mindestvorgaben wie Security by Design und Privacy by Design sowie Privacy by Default umzusetzen. Bei Nichtanwendung dieser Mindestvorgaben haften weltweit die Hersteller bzw. Anbieter von Onlinediensten. Der größte Anteil an Sicherheitslücken in der Software beruht darauf, dass diese von mangelhafter (Sicherheits-)Qualität sind, daher sind zukünftig Softwareentwickler zur Berücksichtigung von Mindeststandards zur sicheren Softwareentwicklung - bspw. vom BSI: „CON.8: Software-Entwicklung“ - zu verpflichten. Vor Freigabe von Software-Produkten sind vor allem neben der sicherheitsfördernden Nutzerfreundlichkeit auch „[s]ystematische Security Tests der wichtigsten Anwendungen zur Identifizierung von bislang nicht erkannten Sicherheitslücken (Zero-Day-Vulnerabilities), Covert Functions und Back Doors“ [326] durchzuführen.

Falls die Mindeststandards von einem Softwareentwickler nicht umgesetzt werden sollten, hat ein Berufsverbot zu erfolgen, da durch die zunehmende Vernetzung u.a. Kaskadeneffekte entstehen können, die u.U. Leben gefährden kann. Gerade wegen der potentiellen Auswirkungen muss es die Möglichkeit eines Berufsverbotes weltweit geben. Nur so kann langfristig und nachhaltig die Informationssicherheit erhöht werden. Zudem muss Informationssicherheit - insbesondere für Softwareentwickler - bereits beim Studium weltweit integraler Bestandteil sein, ohne einen entsprechenden Prüfungsnachweis kann ein Abschluss nicht erfolgen. Bis heute gibt es für den Nutzer keine bekannten Kennzeichen, woran dieser vor dem Kauf erkennen kann, ob das jeweilige Software- bzw. Hardwareprodukt Mindeststandards sowohl auf Seiten der Informationssicherheit als auch des Datenschutzes erfüllt. Das freiwillige Sicherheitskennzeichen des BSI ist als unzureichend abzulehnen, da es zum einen freiwillig ist und zum anderen prüft das BSI beim Sicherheitskennzeichen im Gegensatz zum Common-Criteria-Prüfsiegel (CC) nicht standardmäßig, sondern nur anlassbezogen. Am ehesten könnte das CC als Kennzeichen für den Nutzer der breiten Öffentlichkeit bekannt gemacht werden, da CC bereits ein internationaler Standard ist und auf diesem Fundament können weitere Anforderungen wie bspw. die Datenminimierung aufgebaut werden. Clouddienste sind prinzipiell aufgrund der Komplexität der IT-Landschaft unsicher, selbst wenn eine Ende-zu-Ende-Verschlüsselung, die Schlüssel zur Verschlüsselung ausschließlich beim Nutzer generiert werden können und darüber hinaus sogar die Verschleierung von Metadaten ermöglicht wird, kann nicht ausgeschlossen werden, dass unrechtmäßig verschlüsselte Daten kopiert werden, um diese später zu knacken wie es bspw. nachweislich die NSA praktiziert. Edward Snowden hat folgende Aussage zur NSA getätigt: „[W]as die NSA in Wirklichkeit will ist die Fähigkeit, rückwirkend zu ermitteln. Sie wollen eine vollständige Aufzeichnung Ihres Lebens der letzten fünf Jahre, so dass sie alles über Sie wissen können, wenn Sie in

ihr Blickfeld geraten.“ [327]. Vor diesem Hintergrund sind nur Daten, die nicht gespeichert werden und nicht mit dem Internet verbunden sind, sicher. Verschärfend kommt der Trend der Analyse von verschlüsselten Daten zu. Einem israelischen Forschungsteam ist es gelungen, aus verschlüsseltem Internetverkehr einzelne Anwendungen wie bspw. Facebook, Skype oder Vimeo zu identifizieren und weitere Erkenntnisse sind in naher Zukunft nicht auszuschließen s. [328].

Der Unterschied einer Wohnungsdurchsuchung und einer Onlinedurchsuchung ist erheblich. Denn bei ersterem bekommt der Betroffene wenigstens einen Hinweis mit Ausnahme geheimdienstlicher Aktionen und ist i.d.R. eine einmalige Angelegenheit. Bei einer Onlinedurchsuchung hingegen laufen diese i.d.R über einen längeren Zeitraum verdeckt ab und die abgefangene Datenmenge ist so umfangreich, dass nicht nur auf die Lebensweise des Nutzers sowie dessen soziales Umfeld geschlossen werden kann, sondern aufgrund der verfügbaren Analysemöglichkeiten auch die Art und Weise wie dieser Nutzer denkt. Daher ist die Eingriffsintensität wesentlich tiefer als bei einer Wohnungsdurchsuchung zu betrachten. Insgesamt ist zu konstatieren, dass in letzter Zeit mehr Befugnisse bei den Behörden eingeräumt wurden, ohne dabei bislang eine Überwachungsgesamtrechnung vorzunehmen. Dieser Trend birgt Gefahren, da hinsichtlich der politischen Entwicklung festzustellen ist, dass in Europa die bisherigen Volksparteien mittelbis langfristig in die Bedeutungslosigkeit versinken und zugleich es Tendenzen zur Radikalisierung gibt. Vor diesem Hinblick ist es eine gefährliche Entwicklung, weil u.U. Radikale auf die Regierungsseite wechseln können und somit Zugriff auf eine schlüsselfertige Überwachungsstruktur bekommen. Gerade die Geheimdienste verfügen über umfangreiche Zugriffe auf die Daten privater Anbieter sowohl im Inland als auch im Ausland und besitzen darüber hinaus auch eigene Datenzentren. Hier besteht aufgrund der neuen politischen Ausrichtung die Gefahr des Missbrauchs der erhobenen Daten durch den Staat. Beispielhaft sei an dieser Stelle die Übernahme der Macht durch die Taliban in Afghanistan genannt, die dann mithilfe von erhobenen Biometriedaten seitens der US-Streitkräfte “Verräter“ eindeutig identifizieren können, was u.U. den Tod nach sich ziehen kann [329].

Hinsichtlich der Entwicklung der Datenvielfalt und des -umfangs sowie die Zunahme des unterschiedlichsten Aufbaus von IT-Systemen ist es nicht mehr zielführend, die bisherigen Begriffe Informationssicherheit und Datenschutz getrennt zu betrachten bzw. zu behandeln. Inzwischen ist es vielmehr eine Kombination aus Gefährdungen bzw. Gefahren, die beide - hier Informationssicherheit und Datenschutz - betreffen. Als Beispiel sei die folgende Fallkonstellation genannt: Durch ein Konfigurationsfehler eines Datenbankservers - was der Informationssicherheit zuzuordnen ist - war es möglich gewesen, unbefugt aus dem Internet personenbezogene Daten - was dem Datenschutz zuzuordnen ist - aus der Datenbank abzurufen. Wenn der Datenbankserver nicht nur korrekt aufgesetzt worden wäre, sondern von Anfang an Verschlüsselung genutzt hätte - was in diesem Fall sowohl eine Anforderung der Informationssicherheit als auch des Datenschutzes ist - und darüber hinaus auch die Datenminimierung beachtet worden wäre - eine Anforderung aus dem Datenschutz -, dann wäre es nicht zu diesem schwerwiegenden Vorfall gekommen.

Wenn hinsichtlich der Datenminimierung die Datenbanksoftware automatisch nach einer gewissen Zeit Löschungen durchführt, die vorher für einen bestimmten Zeitraum manuell festgelegt worden wären, dann wäre beim Datenabfluss auch die Datenmenge nicht so groß gewesen. Deswegen sind die Anforderungen der Informationssicherheit (security by design) und des Datenschutzes (privacy by design und privacy by default) konsequenterweise zusammenzuführen, so dass ein ganzheitliche Informationssicherheit - einschließlich von Teilaspekten des Datenschutzes - hergestellt werden kann. Der Begriff „ganzheitliche Informationssicherheit“ erlaubt bislang getrennte Anforderungen zu einer zusammenzufassen, so dass bereits bei der Entwicklung von Soft- und Hardware-Produkten die möglichen Auswirkungen von Gefährdungen bzw. Schwachstellen sowie Risiken von vorneherein minimiert werden können. Von Anfang an implementierte Informationssicherheit ist systembedingt immer besser als nachträglich aufgesetzte Schutzmaßnahmen, wobei letztere noch überwiegend der Regelfall ist.

In Bezug auf dem Nutzer ist die derzeitig mittel- bis langfristig einzige wirksame Schutzmöglichkeit, ausschließlich lokale IT-Systeme zu nutzen, deren Daten vollumfänglich verschlüsselt sind und nicht an das Internet angebunden sind. Nur diese Option erlaubt die maximale Kontrolle und würde damit am ehesten die Ausübung der digitalen Souveränität ermöglichen. Dabei sind nur erforderliche IT-Systeme zu nutzen. IoT Geräte einschließlich des Smart-TV sind nicht zu nutzen, da hier u.a. die Daten unverschlüsselt vorliegen und daher forensische Möglichkeiten nutzbar sind. Auch vom Einsatz von Handys sowie Smartphones ist abzuraten, da es systembedingt u.a. keine Schutzmaßnahme gegen Ortung gibt. Falls eine Onlineverbindung notwendig ist, ist diese ausschließlich an einem extra eingerichteten IT-System zu erfolgen, auf dem das Betriebssystem Tails ausschließlich über einen nicht beschreibbaren USB-Stick läuft und die Verbindung ins Internet ausschließlich über Tor erfolgt. Dabei wird Tor nur zum Anschauen von Webseiten benutzt und keine Login-Verfahren jedweder Art von Onlinediensten angewendet, um eine eindeutige Identifizierbarkeit nicht nur durch die Trackingdienste zu erschweren. Diese Vorgehensweise ermöglicht kurz- bis mittelfristig die maximale Schutzmöglichkeit hinsichtlich der drei Schutzwerte Vertraulichkeit, Integrität und Verfügbarkeit einschließlich der Anforderung Datenminimierung und kommt somit der ganzheitlichen Informationssicherheit am nächsten, was dem unmittelbaren Einflussbereich des Nutzers betrifft. Sofern das Risikobewusstsein des Nutzers entsprechend geschärft ist, können auch Login-Verfahren genutzt werden. In diesem Fall sind datensparsame Firmen wie bspw. E-Mailanbieter wie mailbox.org zu bevorzugen anstatt gmx.de. Allerdings fallen durch die Verbindung Daten an, die eine Identifikation des Nutzers ermöglichen. Bei einem entsprechenden Risikobewusstsein versteht der Nutzer u.a. den Unterschied zwischen Anbietern, die dauerhaft und umfangreich Daten - einschließlich der Nutzung von Drittparteien - generieren wie es beim Besuch von gmx.de der Fall ist, wo hingegen bei mailbox.org keine Datenerhebung stattfindet - da eine Registrierung ohne Bankkonto und echtem Namen möglich ist - und auch beim Login keine Drittparteien genutzt werden.

5. Handlungsoptionen

Die Bedrohungslage ändert sich ständig wie die diversen Jahresberichte des BSI aufzeigen. Vor diesem Hintergrund können die folgenden Schutzmaßnahmen nur den jetzigen Stand entsprechen und garantieren daher nicht den dauerhaften Schutz beim Umgang mit IT-Systemen. Der einzig vollständige Schutz ist nur durch die Nichtnutzung von IT-Systemen einschließlich der Nichtnutzung jedweder digitalen Dienste bzw. Service möglich. Zudem ist Informationssicherheit wegen der technischen Fortentwicklung kein statischer Zustand, sondern ein fortlaufender Prozess. Vieles in der Informationssicherheit ist an Risiken bekannt, noch mehr aber ist unbekannt, was ein größeres Risiko darstellt.

Wenn IT-Grundlagenwissen fehlen, können Sicherheitshinweise nicht korrekt umgesetzt werden. Ein Beispiel ist das Kriterium, möglichst lange Passwörter einzusetzen wie das BSI es auf seiner Webseite darstellt s. [330]. Die besten Passwörter schützen nicht bei Keyloggern oder wenn auf Seiten des Anbieters die Passwörter nicht verschlüsselt werden, was selbst bei einem Konzern wie Facebook jahrelang der Fall war s. [331]. Hier fehlt das Verständnis von weiteren Faktoren, die auf die Passwortsicherheit einwirken. Daher sind die gut gemeinten Hinweise des BSI nicht zielführend, weil zum einen der falsche Eindruck erweckt wird, dass mit der Berücksichtigung der Passworthinweise der Nutzer sich in falscher Sicherheit wiegen kann und zum anderen sind die Hinweise nicht vollständig, hier fehlt bspw. der Hinweis mit dem Keylogger völlig, um ein „ganzes“ Bild zu bekommen. Es fehlt zudem hier die Einordnung, warum Passwörter wichtig sind, welche Konsequenzen aus der Nichtbeachtung folgen können. Daher ist ein gewisses Grundverständnis für IT der Nutzer eine wichtige Voraussetzung, da sonst keine nachhaltige Informationssicherheit praktiziert werden kann. Deswegen muss vorab eine Prüfung durch einen Informationssicherheitsexperten erfolgen, wieviel IT-Grundlagenwissen der Nutzer hat, damit passgenau die Sensibilisierung erfolgen kann. Das Hauptaugenmerk wird auf ein bewusstes und damit sicheres Verhalten beim Umgang mit IT-Systemen gelegt. Der Nutzer soll mind. einmal durch einen Informationssicherheitsexperten vor Ort erfahren, wie einerseits unsicheres Verhalten aussieht und welche sicheren Verhaltensweisen gegen welche Gefahren bzw. Gefährdungen schützt. Dem Nutzer ist aufzuzeigen, dass die IT-Systemlandschaft nicht sicher ist und daher dieser seinen eigenen Beitrag leisten muss, um einen sicheren Umgang zu ermöglichen. Dies fängt mit der Auflistung der Phasen des Cyber-Angriffes an (s. Kapitel 2), damit dieser zum einen ein Gefühl bekommt, welche Gefahren dabei bestehen und zum anderen das Wissen erhält, wie zahllos die Angriffsmöglichkeiten sind. Dabei darf kein Blaming beim Nutzer erfolgen, d.h. ihm ist aufzuzeigen, dass die “Schuld“ nicht primär beim Nutzer liegt, sondern bei den Herstellern von i.d.R. unsicher produzierten Hard- bzw. Softwareprodukten (einschließlich Firmware und Betriebssysteme).

Je mehr IT-Systeme eingesetzt werden, desto aufwändiger sind die entsprechenden Prüfschritte, um ein ganzheitliches Schutzkonzept zu ermöglichen. Unabhängig davon steigt mit zunehmender Anzahl der IT-Systeme auch der Update-Prozess und damit der Pflegeaufwand, was bei IoT-Geräten in der Regel nicht möglich ist. Zugleich fließen bei mehr IT-Systemen, die permanent mit dem Internet verbunden sind, mehr Daten ab, was mind. das Schutzziel Vertraulichkeit gefährdet. Damit der Nutzer die Dimension der unberechtigten Datenabflüsse und Hacks vor Augen geführt bekommt, wird ihm diese Webseite aufgezeigt:

https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ (Stand: 25.03.2022).

Vor diesem Hintergrund ist der einzige effektive Schutz, dem Nutzer in erster Linie Datensparsamkeit nahe zu bringen, nach Möglichkeit lokale Datenspeicherung zu praktizieren anstatt Clouddienste in Anspruch zu nehmen sowie die konsequente Vollverschlüsselung aller gespeicherten Daten. Eine Onlineverbindung ist konsequent nur über Tor zu erfolgen. Darüber hinaus wird dem Nutzer empfohlen, so wenig wie nötig Geräte zu benutzen und unnötige Software auf dem IT-System zu deinstallieren, um die Angriffsflächen so niedrig wie möglich zu halten. D.h. es sind idealerweise keine IoT Geräte einschließlich Smart-TV in Betrieb. Daher ist eine Auflistung aller vernetzten Geräte im Haushalt erforderlich. Während die Grundprinzipien noch erklärbar sind, ist es spätestens beim Zusammenspiel aller Geräte nicht mehr möglich. „Das Zusammenspiel von Geräten, Programmen, Netzen und Cloud-Diensten ist wegen der unterschiedlichen Hersteller, Geschäftsmodelle und Technologien … nicht kontrollierbar“ [332, p. 189]. Wenn zusätzlich noch die KI eingesetzt wird, ist eine Kontrolle so gut wie gar nicht mehr möglich s. [332, p. 189]. Spätestens dann, wenn Hard- und Software i.d.R. dabei Schwachstellen aufweisen, ist der Kontrollverlust im schlimmsten Fall am höchsten. Hinzu kommt, dass die Schutzmaßnahmen nicht für Geheimdienste gelten, da diese entweder über den Schlüssel von Zertifikatsanbietern verfügen - u.a. über Browserhersteller - oder durch eingebaute Hintertüren an die Daten gelangen. Desweiteren muss dem Nutzer aufgezeigt werden, dass u.a. die NSA gezielt Tornutzer überwacht bzw. der sog. Five Eyes Club das Internet kolonialisiert hat, in dem „[j]edes Gerät ein Ziel“ [333] darstellt s. [333], s. [334]. Denn „[d]er Gefahr, nichts ahnend Opfer eines Datenangriffs zu werden, ist jeder Internetnutzer ausgesetzt. … Spione können routinemäßig fast jede Firewall knacken; auf manchen Rechnern herrscht ein munteres Kommen und Gehen diverser Eindringlinge; auch … wird eingebrochen und kopiert mithilfe von Programmen … und zum Abtransport brisanter Daten können die Mobiltelefone Unbeteiligter missbraucht werden.“ [335]. „In diesem Guerilla-Krieg um Informationen wird … kaum zwischen zivil und militärisch unterschieden. Jeder Nutzer des Internets kann mit seinen Daten und seinem Rechner einen Kollateralschaden erleiden.“ [335]. Das Motto des Remote Operations Center (ROC) der NSA, „dem Zentrum für ferngesteuerte Einsätze … [lautet:] „Deine Daten sind unsere Daten, deine Geräte sind unsere Geräte."“ [335]. Treffender kann es nicht bezeichnet werden. Vor diesem Hintergrund muss dem Nutzer klar aufgezeigt werden, dass hier als einzige Schutzmaßnahme gegen Geheimdienste nur die lokal verschlüsselten

Daten schützen können, sofern das IT-System niemals an das Internet angeschlossen wird. Daher wird dem Nutzer die Bedeutung eines Stand-Alone-Computers nähergebracht.

Der Nutzer muss wissen, dass (Sicherheits-)Zertifikate jedweder Art keine Aussage zur tatsächlichen Sicherheit eines Produktes bzw. eines Onlinedienstes treffen können. Selbst wenn Mindeststandards nach dem BSI und die Common Criteria berücksichtigt wurden, kann nicht ausgeschlossen werden, dass ein Softwareprodukt „im Code nach wie vor Qualitäts- und Sicherheitsmängel“ [336, p. 33] aufweist.

E-Mail-Dienste mit Verschlüsselung sind nach Möglichkeit zu meiden, eher sind Messengerdienste zu nutzen wie Briar oder Signal, falls es für den Nutzer zu schwierig zu nutzen ist. Dabei ist eine Nutzung von PGP nicht zu empfehlen, da diese nicht nur abgegriffen werden kann, sondern auch anhand der Metadaten eine genaue Zuordnung des jeweiligen Senders und Empfängers ermöglicht wird, so dass es in Beziehungsgraphen darstellbar ist s. [337], s. [338]. Zudem besteht die technische Möglichkeit der NSA, den Computer zu hacken und den privaten Schlüssel zu stehlen, so dass damit im Nachhinein verschlüsselte Nachrichten wieder entschlüsselt werden können s. [337]. Deswegen ist der private Schlüssel nicht auf dem PC direkt aufzubewahren. Ein weiterer Vorteil bei Nutzung von Messengerdiensten ist, dass hier neben der konsequenten Verschlüsselung die wenigsten Metadaten anfallen. Vor diesem Hintergrund ist der Betrieb des Messengerdienstes über einen eigenen Server ideal, was die max. Kontrollmöglichkeit erlaubt.

Texte jedweder Art sind nach Möglichkeit nicht über das Internet (einschließlich Bloggen und Posten) zu veröffentlichen, da inzwischen mithilfe der forensischen Textanalyse die Möglichkeit besteht, u.a. „Themen, Stimmungen oder Schreibstilen zu klassifizieren“ [339]. Dies schließt auch die Möglichkeit mit ein, den Urheber eines Textes zu identifizieren, falls dies anonym bzw. unter einem anderen Namen erfolgte. Letztere ist nur möglich, wenn keine weiteren Texte öffentlich abrufbar sind, um einen Vergleich durchführen zu können. Daher sind ausschließlich Texte als .txt Format zu veröffentlichen, um die anfallenden Metadaten so klein wie möglich zu halten. Bislang gibt es noch keine Schutztechniken, die sowohl die Inhalts- sowie die Stilebene von Textdaten als auch die Metadaten anonymisieren kann s. [340].

Eine Cloud Nutzung wird dem Nutzer nicht empfohlen, da diese nicht in dessen Eigentum steht und daher nicht kontrollierbar ist. Wenn dann, ist ein sog. Sealed-Cloud-Dienst zu bevorzugen, da dieser neben der Verschlüsselung von Inhaltsdaten auch die Metadaten verschleiert. Denn mit Hilfe von Metadaten kann u.a. herausgefunden werden, „wer mit wem, wann und wie lange kommuniziert.“ [341]. Zudem darf nicht außer Acht gelassen werden, dass der Cloudanbieter auch aufgekauft werden oder in Insolvenz gehen kann.

Was den Bereich E-Kommerz angeht, so wird dem Nutzer aufgezeigt, dass Amazon nicht nur ein „Allesverkäufer“ [342, p. 35] ist, sondern auch ein „Allesspeicher-Geschäft“ [342, p. 35], da selbst die „kleinsten Datenmengen über seine Kunden und Produkte“ [342, p. 35] gespeichert werden. Es gibt bereits über 500 persönliche Attribute pro Nutzer (Stand: 2017), deren Weiterentwicklung noch nicht berücksichtigt worden sind s. [342, p. 36].

Von einer Nutzung dieser Dienstleistungsart von Amazon bzw. des E-Kommerz ist eher abzuraten.

Beim Umgang mit medizinischen Daten - einschließlich Apps - ist Datensparsamkeit unter Einhaltung entsprechender Informationssicherheitsmaßnahmen erforderlich. Selbst das BSI hat die IT-Sicherheit bei den Gesundheits-Apps geprüft und kommt zum Schluss, „dass keiner der App-Anbieter eine vollständige Umsetzung der Sicherheitsmaßnahmen nach dem Stand der Technik bieten kann. … Aus Sicht der technischen IT-Sicherheit muss das Ergebnis mindestens als kritisch bewertet werden.“ [343, p. 44]. Solange dies der Fall ist von der Nutzung von Gesundheits-Apps dringend abzuraten. Eine Weitergabe medizinischer Daten durch behandelnde Ärzte in anonymisierter Form - auch zu Forschungszwecken - ist solange nicht zu befürworten, wenn es Methoden gibt, diese Daten wieder zu deanonymisieren. Solange es keine Anonymisierungsmethoden gibt, die keine Rückschlüsse erlauben, ist eine Weitergabe nicht zu empfehlen, dies gilt erst recht für Pseudonymisierung. Denn letzteres ermöglicht mit Hilfe von Big Data Mechanismen wieder eine Re-Identifikation und sollte daher nach heutigen Maßstäben als inzwischen veraltete Schutzmaßnahme nicht mehr erlaubt sein. Dies schließt auch sog. Zyklus-Apps ein. Diese sind prinzipiell nicht zu verwenden, da es zum einen nicht sicher gestaltet ist und zum anderen die erhobenen Daten mit vielen Drittanbietern geteilt werden, u.a. an Facebook wie eine Studie der NGO Privacy International nachwies s. [344].

Eine sehr anschauliche Übersicht, wie weit die Datenerfassungs- und Analysemöglichkeiten von Facebook ist, wird dem Nutzer mit dieser Webseite aufgezeigt: https://labs.rs/en/facebook-algorithmic-factory-immaterial-labour-and-data-harvesting/ (Stand: 21.08.2016). Damit soll der Nutzer ein Gefühl für die Möglichkeiten der Datenerfassungs- und Analysemöglichkeiten - nicht nur von Facebook - bekommen.

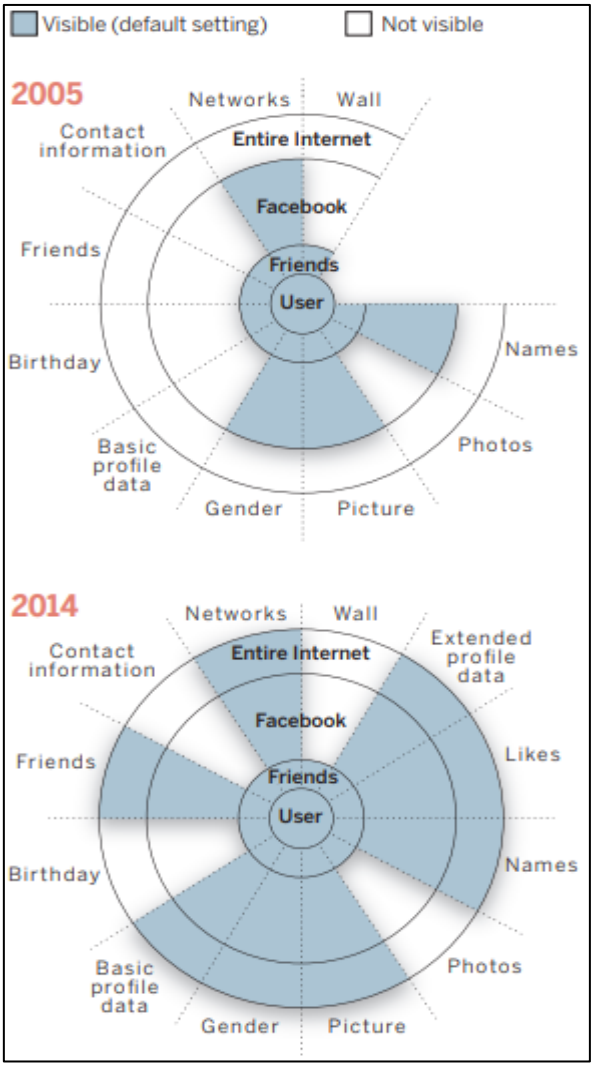


Bild 11: Darstellung der Privatsphäreneinstellung für die Jahre 2005 und 2014 [345, p. 513]

Mit diesem Schaubild soll dem Nutzer anschaulich dargelegt werden, wie am Beispiel Facebook die Standardeinstellungen zum Schutz der Privatsphäre im Laufe der Zeit immer mehr aufgeweicht wurden, so dass bei jetziger Nutzung de facto eine fast automatische Preisgabe privater Informationen erfolgt. Warum ebenfalls die Nutzung von Instagram nicht zu empfehlen ist, dass anhand der Datenspuren - die ein Nutzer dort hinterlässt - unter Einsatz des maschinellen Lernens frühzeitig Depressionen feststellbar sind und das vergleichsweise sogar zuverlässiger diagnostiziert als von Ärzten s. [346]. Diese Entwicklung kann zukünftig auf weitere Krankheitsbilder ausgebaut werden. Warum ebenfalls die Nutzung von beruflichen Karrierenetzwerken wie LinkedIn oder Xing nicht zu empfehlen sind, zeigt bspw. die Vorgehensweise der Firma Hiqlabs auf. Diese Firma hat alle Profildaten von LinkedIn ausgelesen und es mit weiteren Daten angereichert, so dass die Firma in der Lage ist, mit Big Data-Mechanismen u.a. die Kündigungswahrscheinlichkeit von Beschäftigten zu ermitteln s. [347, p. 123]. Dieser Fall zeigt exemplarisch auf, dass Daten zu ganz anderen Zwecken eingesetzt werden, was nach der DSGVO für die EU-Bürger nicht erlaubt ist, aber dennoch durch die US-Firma praktiziert wird.

Dem Nutzer werden die Unterschiede beim Datenschutz in Europa und den USA aufgezeigt, wie es Herr Spitzer in dessen Buch Cyberkrank! plastisch gegenübergestellt hat:

Tabelle 2: „Datenschutzunterschiede zwischen Europa und den USA“ [348, p. 135]

Europa	**USA**
Das Sammeln von personenbezogenen Daten ist prinzipiell verboten.	Das Sammeln von personenbezogenen Daten ist prinzipiell erlaubt.
Die Daten gehören der Person, die durch sie beschrieben wird.	Die Daten gehören demjenigen, der sie sammelt.
Die Daten müssen gelöscht werden, sobald sie nicht mehr benötigt werden.	Die Daten können beliebig lange gespeichert werden.
Daten sollten grundsätzlich so schnell wie möglich anonymisiert werden.	Solche Einschränkungen gibt es nicht.

Darüber hinaus wird kurz auf die Bedrohungen durch Tracking eingegangen:

- „Bedrohung durch Erhebung von Daten (IoT, Internet der Dienste, Eingeschränkte Abwehr und neue Trackingmethoden, Ressourcenverbrauch)“ [349, p. 10].

- „Bedrohung durch Verarbeitung von Daten (Kombinierbarkeit von Daten und Big Data, Verknüpfbarkeit mit echten Identitäten, Rückschlüsse aus sozialen Beziehungen)“ [349, pp. 10-11].

- „Bedrohung durch Verwertung von Daten und dem Markt (Weitergabe von Daten und Datenhandel, Reichweite von Trackern, Neue Geschäftsmodelle, Irreführung von Verbrauchern)“ [349, p. 11].

- „Bedrohung durch Verhalten von Nutzern (Fehlendes Nutzerwissen und Intransparenz, Änderung von Vertrauensbeziehungen, Durchsetzung der Löschung von Daten)“ [349, p. 12].

Das Fraunhofer-SIT hat Tracking mit Stalking verglichen, da Nutzer „bei jedem Schritt von einer ganzen Herde von Dritten verfolgt werden, die jeden dieser Schritte aufzeichnen und auswerten.“ [349, p. 11].

Wie hoch der Wert der eigenen Daten ist, kann dem Nutzer auf der folgenden Webseite gezeigt werden - zur Sensibilisierung -:

https://www.invisibly.com/learn-blog/how-much-is-data-worth (Stand: 13.07.2021).

Hinsichtlich der Gefahren von Dark Pattern werden dem Nutzer diese beiden Webseiten empfohlen: https://www.darkpatterns.org/ (Stand: 25.03.2022) und https://termsandconditions.game/ (Stand: 25.03.2022). In diesem Zusammenhang wird auch die Bedeutung der Persönlichkeitspsychologie - hier Big Five Modell - aufgezeigt. Dazu gibt es eine bildhafte Übersicht, welche Erkenntnisse vorhanden und wie die Wohnung der jeweiligen Persönlichkeitsmerkmale ausgestattet sind: https://big5.visualdna.com/ (Stand: 25.03.2022).

Dem Nutzer soll die Bedeutung von Positionsdaten aufgezeigt werden. Ein Forscher und Mitgründer der Firma Sense Networks analysiert diese Daten und hat dazu bereits 2009 die folgende Aussage getroffen: „Mit der Beobachtung von Signalen kann man ganze Firmen, ganze Städte, eine ganze Gesellschaft röntgen“ [350]. Gegen die Lokalisierung und damit der Erstellung von Bewegungsprofilen gibt es bislang keinen technischen Schutz s. [351]. Ein anschauliches Beispiel, wie viele Erkenntnisse aus den Handydaten gewonnen werden können, zeigt diese Webseite auf: https://www.zeit.de/datenschutz/malte-spitz-vorratsdaten (Stand: 31.08.2009).

Ein exemplarisches Beispiel, wie weit Rückschlüsse aus den Daten gezogen werden können und die nichts mit dem eigentlichen Geschäftsmodell zu tun hat, zeigt der Fahrdienst Uber auf. Uber kann bereits seit 2012 feststellen, ob jemand zu einem One-Night-Stand hinfährt oder nicht. An dieser Stelle stellt sich die Frage, zu welchem Zweck diese “Erkenntnisse“ weiterhin erhoben werden s. [352]. Welche Erkenntnisse andere Anbieter, die über noch umfassendere Datensilos wie bspw. Alphabet oder Meta verfügen, bleibt verborgen. All die gesammelten Daten - auch im Zusammenhang mit Big Data - können zu anderen Zwecken als ursprünglich gedacht, genutzt werden. Der ehemalige Chefwissenschaftler von Amazon sagte dazu folgendes: „Meine Hauptsorge ist, dass Fotos, Videos, Audiofiles oder auch Texte und Chats in einen Kontext gestellt werden können, der mich in Schwierigkeiten bringen könnte.“ [353]. Solange Plattformen, Datenunternehmen einschließlich der Datenhändler intransparenz gegenüber dem Nutzer handeln, ist von einer Nutzung dieser Dienste abzuraten. Dies gilt auch für die Nutzung von Start-Ups, da diese i.d.R. von marktbeherrschenden Internetunternehmen aufgekauft werden und die erhobenen Daten ebenfalls in deren Datensilos landen würden. Aufgrund der mangelnden Transparenz auf Seiten der Onlineanbieter kann kein vollständiges Risikobild bei Nutzung derer Dienste hergestellt werden. Denn jede Onlineaktivität hinterlässt eine Datenspur, eine digitale Aufnahme von den Aktivitäten, die nicht verhindert werden kann.

Die Ausführung des Onlinebankings ist nur auf das Notwendige zu reduzieren. Von einer Nutzung einer Banking-App ist dem Nutzer nicht nur aus IT-sicherheitstechnischen Gründen abzuraten, sondern auch wegen der zunehmenden Anzahl an Drittanbietern. Den derzeitigen Spitzenreiter bildet die Banking-App N26, die nicht nur 11 Tracker nutzt, sondern bis zu 27 Berechtigungen benötigt, was in diesem sensiblen Bereich als sehr fragwürdig anzusehen ist s. [354]. Eine Prüfung auf Berechtigungen sowie auf Trackingdienste kann auf dieser Seite erfolgen: https://reports.exodus-privacy.eu.org/de/ (Stand: 25.03.2022).

Von einer Onlinespielnutzung ist abzuraten, da auch dieser Bereich Auswertungen über Spieler vornimmt. Allein nur aus dem Onlinespiel sind folgende Erkenntnisse möglich: angefangen von den Registrierungsdaten des Spielers über „ihr Verhalten, ihre Verbindungen zu anderen Menschen, ihre Vorlieben, wirtschaftlichen Möglichkeiten und viele weitere Details ihres realen Lebens [inklusive] … Rückschlüsse über soziale Netze, Beziehungsgeflecht u. dgl. ableiten, Lebensumstände bis hin zu Gesundheitsdaten und politischen Einstellungen“ [355, p. 55].

Dem Nutzer wird darauf aufmerksam gemacht, dass - wenn überhaupt - Nacktfotos nur durch eine Kamera getätigt werden, in dem dann die Aufnahmen ausschließlich verschlüsselt auf dem USB-Stick abgespeichert werden. Ansonsten passiert das, was u.a. Jennifer Lawrence durch die Nutzung von ihrem I-Phone passiert ist und als „The Fappening“ [356] bekannt wurde.

Dem Nutzer ist von einer Kreditkartennutzung abzuraten, da Kreditkarten-Transaktionsdaten von Mastercard bspw. von Datensammlern wie Google aufgekauft wurden s. [357]. Daher ist bei Erhalt der Kreditkarte umgehend ein Opt-out durchzuführen und diese so wenig wie möglich zu nutzen. Darüber hinaus ist Mastercard wie Visa ein US-Unternehmen, wo amerikanische Behörden sich direkt Zugang verschaffen können.

Dem Nutzer wird darauf aufmerksam gemacht, dass keine Wartezimmersoftware wie bspw. Doctolib genutzt werden soll, da sensible Daten nicht geschützt sind. Dies gilt auch für Anrufe bei Call-Centern, da es u.a. möglich ist, die Stimme des Anrufers auszuwerten. Zudem besteht das Risiko einer unerlaubten Sprachaufzeichnung.

Vermittelte Übernachtungen durch Airbnb können Risiken bergen, wenn diese IoT Geräte einschließlich - versteckte - Kameras aufweisen s. [358]. Bei Übernachtungen außerhalb der eigenen Wohnung ist darauf zu achten, dass IoT Geräte einschließlich Smart-TV ausgeschaltet sind (per Stromkabel gezogen).

Solange die menschliche Onlinekommunikation kommerziell ausgebeutet wird und u.U. zum Staat gelangen, ist dem Nutzer von einer Nutzung von Chat- / E-Mail-Diensten abzuraten.

Dem Nutzer ist aufzuzeigen, dass Blackboxes im Auto nicht akzeptiert werden sollen, auch wenn es billiger ist. Nicht umsonst wurde bereits im Jahr 2008 festgestellt: „Nur noch Vermögende können sich eine Privatsphäre leisten. Die Gesellschaft spaltet sich in anonym bleibende Wohlhabende und vollständig überwachte ärmere Schichten - Datenschutz wird damit zum Luxusgut.“ [359, p. 14]. Darüber hinaus wird mit diesem Schritt auch die Solidargemeinschaft gefährdet, wovon letzten Endes nur der Versicherer profitieren würde.

Updates bei Betriebssystemen wie Microsoft, Android und Apple bergen u.a. die Gefahr, dass ohne Kenntnisnahme des Nutzers, die datenschutzfreundlichen Einstellungen wieder rückgängig gemacht werden. Nicht umsonst ist bspw. Google durch den Bundesstaat Arizona u.a. dafür verklagt worden, dass „Google Automatically Changes the State of Permissions Without Notifying Users“ [360, pp. -i-]. Die Vorwürfe gehen sogar weiter,

dass „Google Collects Location Data Even When Users Turn Their Device Location Off“ [360, pp. -i-]. Auch können bei „verdächtigen“ Personen modifizierte Updates erfolgen, die das Betriebssystem bzw. Software mit Schadcode ausstatten.

Insgesamt sind alle in dieser Arbeit aufgeführten Informationen über Vorfälle nur die Spitze des Eisbergs. Informationstechnik - jedweder Art - ist Risikotechnologie, d.h. es gibt keine 100 % Sicherheit. Es gibt sowohl auf Hardware- als auch auf Softwareseite (inklusive Betriebssystem) immer Sicherheitsrisiken in Form von Hintertüren (mit Absicht oder unbeabsichtigt), Trojaner, Viren, (auch unbeabsichtigte) Fernsteuerungen u.v.m.. Wie schwer schon die Rückverfolgbarkeit nur der Materialien von Zulieferern bei der Herstellung einer Computermaus ist, kann an dem Schaubild rausgelesen werden: https://www.nager-it.de/static/pdf/lieferkette.pdf (Stand: Dezember 2021). Dieses Schaubild steht exemplarisch für alle anderen (informations-)technische Komponenten. Vor diesem Hintergrund ist Verschlüsselung für den Fall des Falles eine der wichtigsten Maßnahmen überhaupt. Der Kryptographie Experte Bruce Schneier hat es auf den Punkt gebracht: „Die Verschlüsselung ist dein Freund“ [361]. Auf absehbarer Zeit könnten aber alle derzeitigen asymmetrischen Verschlüsselungsmethoden unsicher werden, wenn Quantenrechner Realität werden.

Es ist eine stufenweise Herangehensweise nach Grad des entsprechenden (Risiko-)Bewusstseins beim Umgang mit IT-Systemen zu empfehlen. Damit wird einerseits sichergestellt, dass keine Überforderung stattfindet und zum anderen kann durch diese Vorgehensweise eine Überprüfung vorgenommen werden, ob die jeweilige Stufe „gemeistert“ wurde, bevor die nächsthöhere Stufe, die mit mehr Gefährdungen bzw. Risiken und damit einer höheren Komplexität einhergeht, erreicht werden kann. Wenn dies auch noch „spielerisch“ eingebettet ist, hat es höhere Chancen auf eine dauerhafte Umsetzung der gewonnenen Erkenntnisse für einen sicheren und damit professionellen Umgang mit IT-Systemen. Als Ausgangspunkt wird Tails eingesetzt. Dieses Betriebssystem wird ausgiebig offline solange getestet, bis ein Verständnis dafür entwickelt wurde. Darüber hinaus entstehen durch die Offlinenutzung nur Metadaten, die innerhalb des Rechners verbleiben und somit im eigenen Kontrollbereich befinden. Erst mit zunehmenden Verständnis- und Risikobewusstseins wird online ausschließlich Tor mit der höchsten Sicherheitseinstellung benutzt. Tor ist daher zu nutzen, weil selbst Schutzsysteme wie bspw. uMatrix nicht vor verhaltensbasiertes Tracking schützen kann s. [362]. Dies schließt insbesondere die nicht sichtbaren Pixel mit ein sowie Weiterleitungsprozesse s. [362]. Bei Nutzung von Onlinediensten wird dafür ein Zweitgerät verwendet, auf dem sich keine Daten befinden, auch wenn ein Übergriff vom geschützten Betriebssystem auf dem Gastsystem fast ausgeschlossen ist. Der Transfer zwischen den beiden Rechner erfolgt über einen USB-Stick. Die Vorgehensweise hat den Vorteil, dass erstens die Konzentration auf jeweils einen Punkt gegeben ist und eine mentale Überforderung durch das schrittweise Ausprobieren verringert wird.

1. Stufe: Tails offline kennenlernen und solange probieren, bis es beherrscht wird.

2. Stufe: Online nur mit TOR und dabei Webseiten nur anschauen.

3. Stufe: Kommentieren ohne dabei Loginverfahren zu nutzen.

4. Stufe: Daten herunterladen und nach Möglichkeit kein Loginverfahren nutzen.

Mit dieser Vorgehensweise wird dabei die Selbstwirksamkeit mit jeder erfolgreich abgelegten Stufe erhöht.

Das IT-System ist prinzipiell nur über das Kabel (Local Area Network - LAN) verbunden, da WLAN einige Risiken beinhaltet. Je mehr Programme, desto höher der Updateaufwand. Daher wird dem Nutzer empfohlen, so wenig wie nötig Programme zu nutzen. Wenn Updates manuell getätigt werden, dann immer nur direkt beim Hersteller die Updates holen und nicht über Drittseiten, da in der Vergangenheit darüber Schadcodes verteilt wurden. Hacker kommen meist leicht über ungepatchte Systeme rein. Selbst wenn alle Sicherheitsmaßnahmen seitens des Nutzers umgesetzt worden sind, kann von unerwarteter Seite der Netzwerkverkehr ungeschützt sein, was ein erhebliches Sicherheitsrisiko ist. Hier ein exemplarisches Beispiel, welche Risiken entstehen können, wenn der Provider seine Hausaufgaben nicht gemacht hat: https://www.heise.de/security/meldung/Luecken-in-Provider-Routern-entdeckt-4099449.html (Stand: 04.07.2018). Darüber hinaus hat die Regierung durch eine sog. technische Spezifikation mit der Bezeichnung "TR-069“ zugelassen, dass darüber es „dem Provider [erlaubt], automatische Aktualisierungen unbemerkt und ohne Zustimmung des Benutzers in DSL-Router einzuspielen“ [363]. Einerseits ist diese Option wichtig, um sicherzustellen, dass notwendige Updates installiert werden können, aber andererseits kann diese Funktion dazu missbraucht werden, um den sog. Bundestrojaner auf diesem Wege heimlich einzuschleusen. Leider kann allein nur durch den Einbau dieser Möglichkeit nicht nur die organisierte Kriminalität, sondern auch Geheimdienste für ihre Zwecke missbrauchen.

Der Nutzer soll das Verständnis entwickeln, wie wenig Webseiten ohne JavaScript auskommen können und warum JavaScript gefährlich ist. Falls Webseiten Chaptas verlangen, sind diese zu meiden, da i.d.R. Daten an Drittanbieter - meist Google - gesendet werden. Die scheinbare Einschränkung bei der Auswahl von Webseiten verhilft dem Nutzer zur besseren Konzentration und schafft ihm ein Bewusstsein dafür, wie groß die Verführung zur Nutzung von datenintensiven Services ist. Die Webseite https://schemeflood.com/ (Stand: 25.03.2022) verhilft plastisch vor Augen zu führen, dass es möglich ist, nur anhand von installierten Anwendungen einen einzigartigen Fingerabdruck zu generieren. Der Nutzer kann über folgende Webseiten erfahren, ob dessen Browser wiedererkennbar ist: https://coveryourtracks.eff.org/learn (Stand: 25.03.2022) oder über https://amiunique.org/ (Stand: 25.03.2022) bzw. https://www.deviceinfo.me/ (Stand: 25.03.2022). Darüber hinaus gibt es beispielhaft visuelle Informationen über Geschäfte mit Daten (von Arte betrieben): https://blog.donottrack-doc.com/de/ (Stand: 25.03.2022). Das ermöglicht dem Nutzer mit allgemeinverständlichen Worten den In-

dustriezweig Tracking und die damit verbundene Auswertungsmöglichkeiten nahezulegen. Wie kreativ dieser Industriezweig beim Umgehen von Trackingschutzmaßnahmen vorgeht, zeigt eine Studie auf, die nachgewiesen hat, dass die Browserfunktion Favicons ebenfalls für einen Fingerprinting missbraucht werden kann s. [364]. Diese noch junge Trackingmethode wurde zum Zeitpunkt der Studie bereits realisiert, was aufzeigt, dass auf diesem Feld immer neue Konstellationen für Trackingmethoden entstehen. Dem Nutzer soll damit aufgezeigt werden, dass die Trackingindustrie sehr kreativ ist, Nutzer - auch geräteübergreifend - zu tracken. Auch soll dem Nutzer bewusst gemacht werden, dass der Einsatz von Adblockern nicht das Tracking unterbindet, was genauso für Tracker-Blocker gilt, die ebenfalls nicht immer die Werbung unterbinden können. Wenn dann helfen nach dem gegenwärtigen Stand sog. Filtersysteme wie bspw. der eBlocker (https://eblocker.org/ Stand: 25.03.2022), die auf einem Raspberry Pi laufen und vor der LAN-Buchse angeschlossen werden.

Dem Nutzer wird das Bewusstsein dafür geschärft, dass es ein Unterschied ist, wenn mit einem Menschen direkt austauscht, dann bleibt dies i.d.R. vertraulich und ist auf einem Ort begrenzt. Dies ist bei einem Austausch über IT-Systeme nicht mehr der Fall, da die Daten weltweit verteilt werden. Selbst wenn keine sensiblen Themen darüber ausgetauscht werden, entstehen dabei Metadaten, die systemseitig nicht unterbunden werden kann. Darüber hinaus muss berücksichtigt werden, dass der andere Kommunikationspartner nicht das gleiche Sicherheitsniveau aufweisen muss, wie der Absender. D.h. über diesen Weg können auch Daten abhandenkommen, sowohl auf der Übertragungsstrecke als auch auf dem Endgerät des Empfängers. Es unterliegt somit nicht mehr der Kontrolle des Absenders, was mit dessen Informationen geschieht.

Dem Nutzer muss aufgezeigt werden, dass nur Open-Source-Verschlüsselung einzusetzen ist und keine kommerzielle Verschlüsselungssoftware, insbesondere außerhalb von Europa, da diese i.d.R. Hintertüren für staatliche Angreifer aufweisen s. [365]. Darüber hinaus ist Verschlüsselung allein nicht sicher, auch die korrekte Implementierung und Anwendung muss beachtet werden. Was die Veröffentlichung von Daten einschließlich von Texten im Internet angeht, so ist die Empfehlung nichts veröffentlichen, da eine vollständige Löschung im Internet systembedingt nicht realisierbar ist.

Synchronisierung ist auf den ersten Blick praktisch, ist dennoch aber ein Kontrollmechanismus. Denn diese Funktion ermöglicht Onlineanbietern auf ihrer eigenen Cloud unbemerkt die Daten der Nutzer zu durchsuchen und ggf. unbemerkt zu kopieren, daher ist diese Option zwingend zu deaktivieren. Selbst bei der “datenschutzfreundlichen“ Firma Apple ist die iCloud-Funktion zu deaktivieren, da dort die Daten letzten Endes unverschlüsselt liegen, weil die Firma Apple einen Schlüssel zum Entschlüsseln verfügt. Dieser Weg wird übrigens zur Überwachung von Apple-Nutzern eingeschlagen, wie unlängst aus einer heimlichen Tonaufnahme einer Besprechung von US-Sicherheitsbehörden hervorgeht s. [366]. Für die Durchsuchung von Apple-Nutzern von einer Privatfirma wird oft nicht einmal eine Durchsuchungsanordnung von der Firma Apple verlangt, was rechtlich als fragwürdig einzustufen ist s. [366]. Auch der Vorstoß des Konzerns, ein iPhone-

Scanning auf kinderpornografisches Material einzuführen, ist mit erheblichen Implikationen und Risiken verbunden s. [367].

Dem Nutzer wird aufgezeigt, dass Konsum und Überwachung zwei Seiten einer Medaille sind. Mit Konsum ist nicht nur das E-Shopping im klassischen Sinne gemeint, sondern auch der Konsum nach Informationen.

Selbst im Flugzeug ist die Nutzung eines IT-Systems nicht zu empfehlen, da bspw. der GHCQ auch dieses Feld zum Abhören nutzt und bereits 2013 in der Lage war, u.a. die PIN von Blackberrys herauszulesen s. [207, p. 236].

Es ist hilfreich, dem Nutzer flankierende Maßnahmen durch wiederkehrende Wiederholungen als Routine aufzuzeigen, in dem bspw. jeden zweiten Montag, ein Backup angefertigt wird, jeden Dienstag ein komplettes Update vorgenommen wird, jeden dritten Mittwoch vorhandene Konten auf Datendiebstahl geprüft wird, um sicheres Verhalten beim Umgang mit IT-Systemen zu praktizieren bzw. zu festigen.

6. Ganzheitliches Schutzkonzept für den Bürger

Das folgende Sicherheitskonzept ist auf die wichtigsten Punkte beschränkt und bewusst in einfacher Sprache gehalten. Alle darin genannten Links haben den Stand vom 25.03.2022, sofern kein anderes Datum vermerkt wurde. Als Format wurde die Checklistenform gewählt, damit zum einen schnell ein Überblick verschafft werden kann und zum anderen wurde es mit einem freien Termin- und Umsetzungsfeld versehen, um eine höhere Verbindlichkeit zur Umsetzung der Schutzmaßnahmen herzustellen. Vor Nutzung dieser Checkliste ist eine Einführung durch einen Informationssicherheitsexperten notwendig, um einerseits den Nutzer abzuholen und andererseits sicheres Verhalten beim Umgang mit IT-Systemen gleich zu trainieren. Bspw. wird die Nutzung von Veracrypt so lange geübt, bis der Nutzer weiß, wie er damit umzugehen hat und sich bei evtl. Problemen sich selbst zu helfen weiß.

Folgender Vortext zur eigentlichen Checkliste wurde bewusst anfangs positiv formuliert, um den Nutzer nicht „abzuschrecken“:

Dieses Ticket bringt Sie zur digitalen Sonnenseite. Je mehr Punkte Sie umsetzen, desto mehr können Sie langfristig die digitale Sonnenseite genießen. Ein Hinweis vorab: Betrachten Sie die folgenden Schutzvorkehrungen, die als Mindestmaßnahmen anzusehen sind, nicht als abschließend an. Überprüfen Sie daher bitte in regelmäßigen Abständen, ob die vorgeschlagenen Mindestmaßnahmen ggf. angepasst werden müssen. Zur schnellen Orientierung habe ich die Checkliste in einzelne Themenbereiche zusammengefasst:

Sofortmaßnahmen

Passwörter

Maßnahme	**Termin**	**Umgesetzt**
Passwort Alle Passwörter sind mind. 15 Zeichen lang und enthalten Buchstaben und Zahlen, mind. ein Groß- bzw. Kleinbuchstaben sowie mind. ein Sonderzeichen. Besser ist es, eine Zwei-Faktor-Authentifizierung (2FA) zu nutzen. Jedes Konto hat ein eigenes Passwort. Niemals bei zwei Konten das gleiche Passwort nutzen. Gilt analog auch für verschlüsselte Daten. Keinesfalls sind dabei biometrische Daten wie Fingerabdruck zu verwenden. Es gibt Passwort-Apps, wobei hier Vorsicht zu walten ist. Hinweis: Das beste Passwort schützt nicht, wenn der Onlineanbieter die Passwörter bei sich im Klartext speichert oder wenn eine Tastaturaufzeichnung (Keylogger) bei Ihnen vorhanden ist und alle Zugangsdaten mitloggt. Letzteres wird durch den Einsatz der 2FA verhindert.		
Router		

Das WLAN-Passwort (Herstellerpasswort) sowie das Gerätepasswort des Routers sind umzuändern. Dabei sind o.g. Rahmenvorgaben einzuhalten. Das WLAN-Passwort ist hierbei mind. 20 Zeichen lang. Darüber hinaus ist ggf. ein Gastnetz einzurichten. Es ist sehr wichtig, dass der Router immer den neuesten Stand an Updates hat. Darüber hinaus sind alle nicht notwendigen Funktionen wie WPS, UPnP, Multimedia-Dienste, FTP etc. zu deaktivieren, da diese sonst Einfallstore sind. Ein Netzwerkcheck ist wie folgt durchzuführen: https://www.heise.de/security/dienste/port-scan/test/go.shtml?scanart=1 Der Status der Fritz-Produktunterstützung kann hier erfragt werden: https://avm.de/service/status-der-produktunterstuetzung/fritzbox		
Filtersystem zum Blocken von Schadcode und Werbung Mit folgender Maßnahme wird zum großen Teil Schadcode sowie Werbung geblockt Eine preisgünstige Variante ist die Nutzung von Raspberry Pi https://www.raspberrypi.com/ und Pi-hole https://pi-hole.net/ Eine Anleitung dazu: https://www.heise.de/tipps-tricks/Pi-Hole-auf-dem-Raspberry-Pi-einrichten-so-geht-s-4358553.html oder https://eblocker.org/. Eine fertige Lösung bietet diese Fa. an: https://buyzero.de/products/anonymebox-anonym-frei-einfach oder umfassender: https://trutzbox.de/shop/.		
Löschung Löschung der Passwortspeicher in allen Browsern einschließlich beim Smartphone.		
Autovervollständigung Autofillfunktion deaktivieren (in Browser/Smartphones).		
Passwortsafe Für den Fall der Nutzung eines Passwortsafe ist KeepassXC https://keepassxc.org/download/ zu bevorzugen. Falls dazu eine Synchronisierung erwünscht wird, ist am ehesten das zu nutzen: https://syncthing.net/.		
Änderungsrhythmus des Passworts		

Spätestens alle drei Monate sind die Passwörter zu ändern, bei sensiblen Daten ist ein monatlicher Rhythmus angezeigt. Bitte entsprechend im Kalender notieren. Es sei denn, es ist ein sehr gutes Passwort (mind. 15 Zeichen), dann kann es länger genutzt werden.		
Wurde Ihr Konto gehackt (als Kontrollmöglichkeit)? Diesen Vorgang regelmäßig jeden Monat immer überprüfen: https://sec.hpi.de/ilc/ (Hasso-Plattner-Institut)		

Konten/Mitgliedschaften/Bonusprogramme/Newsletter – Gilt auch für Ihren Partner/Ihren Familienangehörigen

Maßnahme	**Termin**	**Umgesetzt**
Datenauskunft Bevor unten genannter Schritt (Löschen bzw. Kündigen) durchgeführt wird, wird dringend empfohlen jeweils eine Selbstauskunft bei den jeweiligen Anbietern durchzuführen, sofern dort ein Konto vorhanden ist: https://takeout.google.com/settings/takeout https://de-de.facebook.com/ https://faq.whatsapp.com/general/account-and-profile/how-to-request-your-account-information/?lang=de https://www.linkedin.com/help/linkedin/answer/50276/auf-ihre-kontodaten-zugreifen?lang=de https://www.help.tinder.com/hc/de/articles/115005626726-Wie-beantrage-ich-eine-Kopie-meiner-pers%C3%B6nlichen-Daten- https://help.twitter.com/de/managing-your-account/accessing-your-twitter-data https://www.amazon.de/gp/help/customer/display.html?ref_=hp_left_v4_sib&nodeId=GXPU3YPMBZQRWZK2 usw.		
Löschen bzw. Kündigen Alle nicht mehr benötigten Bonusprogramme/Konten/Mitgliedschaften sind zu löschen bzw. zu kündigen. Beispiele an Konten		

bzw. Mitgliedschaften: Facebook (nicht mehr “Liken” gehört auch dazu), Twitter, LinkedIn, Paypal, Payback, eBay usw..		
Alle nicht mehr notwendigen Newsletter sind abzubestellen.		
Regelmäßig ein Mal pro Jahr sind alle Konten dahingehend zu prüfen, ob eine weitere Mitgliedschaft notwendig ist. Empfehlung ist hier, eine Liste anzufertigen, welche Konten genutzt werden.		

Langfristige Maßnahmen

Spurenarm surfen und suchen (Ziel: Reduzierung des digitalen Fingerabdrucks)

Maßnahme	**Termin**	**Umgesetzt**
Zwei Rechner Strategie Ein Rechner bleibt immer offline, an dem sensible Daten wie persönliche Bilder, Dokumente, Steuerangelegenheiten bearbeitet werden. Die gesamte Festplatte ist dabei verschlüsselt. Der zweite Rechner wird ausschließlich für die Onlineverbindung genutzt, dabei werden - mit Ausnahme von heruntergeladenen Dateien, die direkt auf dem USB-Stick gespeichert werden - keine Dateien gespeichert. Der Rechner bzw. das Notebook hat mindestens folgende Anforderungen umzusetzen, wie es bspw. anhand des NitroPC mit Qubes als Betriebssystem https://shop.nitrokey.com/de_DE/shop/product/nitropc-132 sowie als Laptop ebenfalls mit Qubes https://shop.nitrokey.com/de_DE/shop/product/nitropad-t430-119 umgesetzt worden ist. In Eigenregie kann es günstiger mit Raspberry Pi 4 https://www.raspberrypi.com/products/raspberry-pi-4-model-b/ als Grundlage erworben werden.		
Betriebssystem - Die Nr. 1 ist am ehesten zu bevorzugen. Die Betriebssysteme sind unter dem Aspekt der Informationssicherheit und Datensparsamkeit in der folgenden Reihenfolge empfohlen: 1. Das Open-Source-Betriebssystem Linux ist zu bevorzugen. Darunter gehört bspw. Ubuntu. Am sichersten ist die Nutzung von Tails. Tails ist idealerweise in einer öffentlichen Einrichtung (z.B. Bibliothek) auf einem USB-Stick herunterzuladen und offline zu installieren: https://tails.boum.org/index.de.html. Eine Schritt-für-Schritt-Anleitung ist hierüber zu finden: https://capulcu.blackblogs.org/wp-content/uploads/sites/54/2021/04/Tails-2021-04-12.pdf (Stand: 12.04.2021).		

2. Macintosh 3. Das Windows Betriebssystem ist nicht zu nutzen, da keine vollständige Kontrolle über die eigenen Daten sowie des Betriebs möglich sind. Zudem geht der Trend in Richtung Cloudnutzung.		
Festplattenverschlüsselung Die gesamte Festplatte ist zu verschlüsseln. Linux Systeme bieten diese Option an. Bei Macintosh bzw. Windows ist mind. die kostenfreie Version Veracrypt zu nutzen: https://www.veracrypt.fr/en/Home.html. Die windowseigene Verschlüsselung Bitlocker ist nicht einzusetzen, da diese unsicher ist.		
Zwei-Faktor-Authentifizierung (2FA) Es ist nach Möglichkeit immer die 2FA zu nutzen. Eine Quelle bspw. ist Nitrokey: https://www.nitrokey.com/ oder tanJack deluxe: https://shop.reiner-sct.com/tan-generatoren-fuer-sicheres-online-banking/tanjack-deluxe. Dabei ist die PIN zu aktivieren.		
Tor installieren: https://www.torproject.org/ Sicherheitseinstellungen im Torbrowser mind. auf „Sicherer“ setzen. Eine Schritt-für-Schritt-Anleitung ist hierüber zu finden: https://www.privacy-handbuch.de/download/privacy-handbuch.pdf (im Kapitel 10.3.2, Anonym Surfen mit dem TorBrowserBundle, S. 259 ff.). Nur die Nutzung von Tor gewährleistet derzeit den höchsten Stand, was datensparsames Surfen angeht. Die nächstniedrige Option wäre das unsichtbare Internet Projekt: https://geti2p.net/en/.		
Ggf. Mozilla Firefox installieren: https://www.mozilla.org/de/ Mindestens folgende Add-ons sind zu installieren: https Everywhere, uMatrix, Privacy Badger, uBlock Origin, I don’t care about cookies, Firefox Multi-Account Containers, Temporary Containers. Weitere Erweiterungen sind kritisch zu sehen, da diese auch ein Einfallstor darstellen. Darüber hinaus ist dieses Tool zu installieren: https://tools.google.com/dlpage/gaoptout?hl=de Mozilla Firefox ist immer im Inkognito-Modus zu starten und die Browserhistorie ist deaktiviert. Darüber hinaus sind keine Synchronisationsdiese zu nutzen. Eine Schritt-für-Schritt-Anleitung zur Installation hierüber zu finden: https://www.privacy-handbuch.de/download/privacy-handbuch.pdf (im Kapitel 4.1, Auswahl des Webbrowsers, S. 73 ff.). Alternativ kann auch Brave installiert werden: https://brave.com/de/.		
Browsertest, um zu sehen, wie gut Ihr Browser geschützt ist bzw. welche Mechanismen zur Erkennung es gibt:		

https://coveryourtracks.eff.org/, https://webkay.robinlinus.com/, https://fingerprintjs.com/demo/, https://browserleaks.com/.		
VPN Von einer Nutzung durch VPN-Anbieter ist abzuraten, da diese über die Zugangsdaten der Kunden verfügen und daher jedweden Internetverkehr im Klartext lesen können. Wenn dann, ist TOR die erste Wahl.		
Updates (Patch) Es ist absolut wichtig alle Systeme immer auf den neuesten Stand zu halten. Updates sind - nach Möglichkeit - immer manuell herunterzuladen, da in manchen Updates noch unnötiges wie bspw. Toolbar etc. mitinstalliert wird.		
Backup Mindestens einmal im Monat ist ein Backup sämtlicher Datenträger durchzuführen. Bei häufiger Änderung dann öfter. Hierfür ist eine externe Festplatte oder noch besser eine sog. Network Attached Storage (NAS) zu nutzen. Bei wenigen Daten reicht auch ein mind. 64 GB großer USB-Stick aus, der aber verschlüsselt sein muss. Die Backup-Daten sind zu verschlüsseln. Eine gute Verschlüsselungssoftware ist diese hier: https://www.veracrypt.fr/en/Home.html Mindestens ein Backup ist verschlüsselt außerhalb des Büros bzw. der Wohnung aufzubewahren (u.a. wegen Einbruchsgefahr oder möglichem Wohnungsbrand). Zudem muss alle zwei Monate ein Test vorgenommen werden, ob die Daten noch lesbar sind.		
Drucker Die Software „Deda Toolkit“ ist unter https://dfd.inf.tu-dresden.de/tools/deda.tar.gz herunterzuladen und zu installieren (um farbige Druckerzeugnisse zu anonymisieren).		
Bildschirmsperre Bei Inaktivität oder kurzfristiges Verlassen des Rechners Bildschirmsperre aktivieren bzw. Sicherheits-USB-Stick abziehen, damit das IT-System gesperrt ist**.**		
Kamera Abdeckung / Mikrofon Blocker		

Die Kamera ist abzudecken und ein Mikrofon Blocker schützt vor Audio Hacks. Eine Bezugsquelle zum Mikrofon Blocker: https://privise.io/products/mikrofon-blocker.		
Beim Surfen immer auf https-Verschlüsselung achten Bei Nutzung von kritischen Diensten wie Onlinebanking etc. ist darauf zu achten, dass immer die https Verschlüsselung aktiv ist und das Zertifikat tatsächlich dem Betreiber der Webseite gehört und nicht abgelaufen ist. Darüber hinaus ist im Hinterkopf zu behalten, dass selbst eine https-Verschlüsselung nicht sicher ist, wenn der Angreifer das Zertifikat des eigentlichen Inhabers gehackt bzw. unberechtigt Zertifikate erhalten hat. Dadurch ist es - meist staatlichen - Angreifern möglich, die Inhalte der verschlüsselten Verbindung auszulesen.		
Suchmaschine Folgende datenschutzfreundliche Suchmaschinen sind bevorzugt zu nutzen: https://www.startpage.com/, https://swisscows.ch/, https://metager.de/, https://duckduckgo.com/. Bitte Suchvorschläge im Browser deaktivieren.		
Verschlüsselt kommunizieren (Alternative zu Skype) https://jitsi.org/ (mit Video), https://otr.im/downloads.html		
AGB bzw. Datenschutzbestimmungen Vor Nutzung von jedweden Onlinedienstanbietern sind die AGB bzw. Datenschutzbestimmungen zu lesen. Als Orientierung: Je verklausulierter und länger diese sind, ist eher davon Abstand zu nehmen. Außereuropäische Onlinedienstanbieter sind besonders kritisch zu prüfen bzw. zu hinterfragen und ggf. nicht zu nutzen.		
Keine sozialen Dienste einschließlich Partnerbörsen sowie Onlinespiele nutzen Soziale Dienste jedweder Art sind zu meiden, einschließlich Partnerbörsen sowie berufliche Netzwerke wie bspw. LinkedIn oder Xing. Dies gilt auch für jedwede Art von Onlinespielen.		
Fernwartungstools Fernwartungstools (Ideal: TeamViewer) sind nur bei Notfällen - was wiederum nur gegen Passworteingabe möglich sein darf		

(mind. 8 Zeichen) - zu nutzen und danach wieder zu deinstallieren.		
Welche Google Dienste gibt es? https://www.kuketz-blog.de/das-kranke-www-stop-using-google-web-services/ **Tipp:** Generell wird empfohlen, keine Onlinedienste zu nutzen, die dauerhaft Datenströme generieren. **Wie kann man sich vor Google schützen?** https://www.kuketz-blog.de/tschuess-datenkrake-ein-leben-ohne-google/		
OpenStreetMap statt Google Map https://www.openstreetmap.org/		
LAN-Kabel Bitte bei Kabelnutzung WLAN beim Laptop/Tablet/Smartphone deaktivieren. Einer Kabelverbindung ist vorzuziehen und gilt als Prävention für die Gesundheit (Stichwort: Strahlenbelastung). **Sonderlösung Datenabfluss über das Stromnetz** Der Einsatz dieser Box verhindert den Datenabfluss über das Stromnetz und ist vom BSI geprüft worden: https://heinen-elektronik.de/it-hardwareschutz/nospy-box/.		
Vernichtung von IT-Systemen Bei Aussonderung von IT-Systemen ist - sofern möglich - der Speicher auszubauen und zu vernichten. Wenn dies nicht möglich sein sollte, ist vor Ort bei einer spezialisierten Firma die Vernichtung vornehmen zu lassen.		
Ratgeber Internetkriminalität Aktuelle Hinweise zum Bereich Cybercrime kann hier nachgesehen werden: https://www.polizei-praevention.de/		

Handy/Smartphone

Maßnahme	Termin	Umgesetzt
Smartphone allgemein Zu empfehlen ist, das Smartphone nicht mehr zu benutzen und stattdessen ein Handy zu nehmen, da bei langfristiger Nutzung die Nachteile bei weitem überwiegen. Fall diese weiterhin genutzt wird, sind alle nicht mehr genutzten bzw. nicht genutzten Apps umgehend zu deinstallieren. Alle Schnittstellen wie WLAN/Bluetooth (zum Öffnen des Autos - Stichwort Keyless Systeme siehe http://www.bundpol.de/oeffnungstechnik/qkey-deutsch.htm) sind bei Nichtbenutzung zu deaktivieren. Das gilt auch für Ortungsdienste. Generell ist bei den Einstellungen des Smartphones prinzipiell so wenig wie nötig Rechte einzuräumen, dies schließt auch die Nichtnutzung von Clouddiensten ein wie bspw. iCloud. Sprachassistenten jedweder Art sind keinesfalls zu nutzen. Bitte die weiteren Hinweise im Bereich Handy beachten (siehe übernächste Zeile). Weitere Infos sind hierüber zu finden: https://mobilsicher.de/		
Smartphone mit Betriebssystem Android Bei Android ist das folgende Betriebssystem zu bevorzugen: https://grapheneos.org/. Danach kann F-Droid https://f-droid.org/ installiert werden. Zum Surfen ist Orfox zu empfehlen (nutzt Tor als Grundlage). Als Schutz ist zusätzlich Blokada zu installieren: https://blokada.org/?lang=de. Wer dies schlüsselfertig beziehen möchte, kann diese unter https://shop.nitro-key.com/de_DE/shop/product/nitrophone-2-pro-245 oder unter https://www.cryptophone.de/ bestellen. Verschlüsselte Kommunikation über https://briarproject.org/, https://jitsi.org/ oder https://www.linphone.org/. Eine Übersicht über sichere Apps ist hier zu beziehen: https://myshadow.org/resources. Mind. 8 Zeichen muss das PIN vorweisen. Die Kamera des Smartphones auf der Innenseite ist abzudecken. Eine Blickschutzfolie ist zu empfehlen.		
Handy Kein internetfähiges Handy ist zu nutzen, d.h. das Handy ist nur zum Telefonieren und für die (seltene) SMS-Nutzung da. Das Handy ist ausschließlich mit unterdrückter Rufnummer zu nutzen, da nicht gesichert werden kann, dass über dem Gegenüber bspw. die Handynr. bei Facebook landet (Zugriff auf Kontaktdaten durch WhatsApp). Beim Festnetz ist ebenfalls mit unterdrückter Rufnummer zu telefonieren. Handytelefonate max. 20 Min. am		

Tag im Freien durchführen. Ansonsten im ausgeschalteten Zustand bei sich tragen bzw. im angeschalteten Zustand mind. zwei Meter von Ihnen entfernt liegen lassen, um die Strahlenbelastung so gering wie möglich zu halten.		
Schutzhülle Unterwegs ist die Schutzhülle u.a. wegen Strahlungsreduzierung empfehlenswert, die hierüber zu beziehen ist: https://www.e-wall.eu/		
Beim **Handyanbieter** sich nicht tracken zu lassen (Bewegungsdaten): **Telekom**:https://www.optout-service.telekom-dienste.de/public/anmeldung.jsp? **O2**: https://www.telefonica.de/dap/selbst-entscheiden.html bzw. bei anderen Handybetreibern nachfragen!		
Ggf. Schnurgebundenes Telefon beschaffen Unter den schnurgebundenen Telefonen sind welche mit der sog. Piezo-Technik vorzuziehen (strahlungsfrei und magnetfrei): http://www.umweltanalytik.com/analoge_piezotelefone.htm Falls auf das Schnurlostelefon nicht verzichtet werden kann, dann bitte darauf achten, dass mind. das sog. „ECO Modus plus“, „Full ECO Mode“ und „fulleco“ bzw. DECT „zero“ im Standby eingestellt ist. Welche Telefonhersteller hierfür geeignet sind, ist der folgenden Liste zu entnehmen: https://baubiologie-virnich.de/wp-content/uploads/2018/05/DECT_zero.pdf		

E-Mail

Maßnahme	**Termin**	**Umgesetzt**
Umzug Ihres E-Mailaccounts von Gmail/Yahoo/Msn etc. (von allen amerikanischen bzw. außereuropäischen Anbietern) auf https://posteo.de/de oder https://mailbox.org/. Eine Alternative ist eine eigene Domain (info@meinname.de), was die größte Kontrolle ermöglicht, aber nicht unbedingt die Sicherheit erhöht (das hängt vom Domainbetreiber ab) wie z.B. Deutsche Telekom oder 1 und 1. Hier bitte darauf achten, dass die persönliche E-Mailanschrift nur einem kleinen Kreis bekannt wird (meinname@meinname.de) und für Bestellungen oder Newsletter		

sind sog. Funktionspostfächer zu nutzen (Bsp.: bestellung@meinname.de). Warum Funktionspostfach? Das hat den Vorteil die E-Mailanschrift jederzeit ändern zu können, falls dort zu viel Spam erscheint. „Privatbestellungen“ sollten nicht über Ihre eigene Domain laufen, hier ist dann über eine „öffentliche“ E-Mailanschrift bei https://posteo.de/de (bestellung@posteo.de) zu nutzen. Auch sollte es eine weitere E-Mailanschrift nur für Social Media geben, falls diese genutzt wird. Ein starkes Passwort ist hier sehr wichtig, da durch das E-Mailkonto diverse Konten zurückgesetzt werden können. Falls Sie eine unerwartete Nachricht zur Passwortänderung erhalten, ist dies ein Indikator dafür, dass ein Angriff auf Ihren Account stattfand.		
2-Faktor-Authentifizierung und E-Mailverschlüsselung Es ist eine 2-Faktor-Authentifizierung beim E-Mailaccount zu nutzen. Damit Ihre E-Mails nicht öffentlich einsehbar sind, sind diese zu verschlüsseln. Eine Schritt-für-Schritt-Anleitung ist hierüber zu finden: https://www.privacy-handbuch.de/download/privacy-handbuch.pdf (im Kapitel 8, E-Mails verschlüsseln, S. 189 ff.). Eine einfache Variante ist diese E-Mail Verschlüsselung: https://delta.chat/de/ oder über https://encrypt.to/.		
Vorschaufenster auf TXT-Format umstellen Sofern Sie ein Vorschaufenster (Lesebereich) nutzen, ist diese von HTML-Format auf TXT-Format umzustellen. Ihr E-Mailkonto ist prinzipiell auf TXT-Format bei Nachrichtenerstellung und -empfang eingestellt. Nur hier werden alle Links von Absendern in Klartext angezeigt, um ggf. manipulierte Links zu erkennen.		
Vorsicht vor Links und Anhängen Vorsicht bei jedweder Art von Links und jedweder Art von Anhängen (PDF, Worddatei, EXE-Dateien etc.), da diese Schadcodes enthalten können.		
De-Mail / Besonderes elektronisches Anwaltspostfach (beA) Das De-Mail-Angebot ist nicht zu nutzen, da diese nicht sicher ist. Dies gilt auch für das besondere elektronische Anwaltspostfach. Hier ist der Schriftverkehr am besten persönlich zu übergeben.		
Backups Mindestens einmal im Monat ist ein Backup aller E-Mails von allen E-Mailkonten auf einem USB-Stick bzw. einer externen Festplatte anzulegen, die dort verschlüsselt abgelegt sind.		

Bearbeitung von E-Mails Die Betreffzeile ist immer offen zu lassen, da dies u.a. auch Rückschlüsse auf den verschlüsselten Inhalt der E-Mail zulässt. Aus Effektivitäts-, Konzentrations- sowie aus ergonomischen Gründen ist die Bearbeitung von E-Mails vornehmlich kabelgebunden am Laptop/Rechner mit einem mind. 15 Zoll großen Bildschirm bei ruhiger Umgebung am gleichen Platz vorzunehmen. Das Smartphone bzw. das Tablett sollte dafür nicht genutzt werden, da das Risiko höher ist. Die o.g. Faktoren sind analog auch für andere Arbeiten am Laptop/Rechner zu beachten, insbesondere für eine längere Bearbeitungszeit.		

Office Nutzung

Maßnahme	**Termin**	**Umgesetzt**
Es sind nur Open Source Produkte zu empfehlen wie bspw. OpenOffice https://www.openoffice.de/ oder LibreOffice https://de.libreoffice.org/ . Bei Nutzung sind Makros zu deaktivieren. Idealerweise ist als Format die Textdatei (*.txt) zu bevorzugen, da keine Metadaten enthalten sind. Bei allen anderen Formaten muss vor Weitergabe eine Bereinigung von Metadaten vorgenommen werden, um es anschließend als PDF-Dokument zu konvertieren, um nachträgliche Änderungen zu vermeiden.		

Onlinebanking

Maßnahme	**Termin**	**Umgesetzt**
Die sicherste Überweisung ist über das Terminal vor Ort in der Bank. Beim Onlinebanking ist mind. die folgende Authentifizierungsmethode zu nutzen: https://www.kobil.com/driver/manuals/toc_handbuch_20110429_de.pdf (einmalig für ca. 10 EUR). Die sicherste Onlinebankingmethode ist zur Zeit HBCI: https://www.wikibanking.net/onlinebanking/verfahren/hbci/ Der dazugehörige Chipkartenleser: https://shop.reiner-sct.com/chipkartenleser-fuer-die-sicherheitsklasse-3/cyberjack-rfid-komfort-usb Ausschließlich am eigenen Laptop/Rechner ist Onlinebanking per Favorit gespeicherten Direktlink auf der Onlinebanking Webseite der Bank durchzuführen, dabei ist die Transaktion vor Freigabe immer zu prüfen. Keinesfalls über das Smartphone, da entsprechende Apps - inklusive Bezahl-Apps - nicht risikofrei sind!		
Kreditkartenanbieter		

Damit die Kreditkartendaten nicht ausgewertet werden, ist ein Opt-Out Verfahren durchzuführen: **Visa**: https://marketingreportoptout.visa.com/OPTOUT/request.do **Mastercard**: https://www.mastercard.de/de-de/datenschutz/datenanalyse-abmeldung.html Kreditkarten sind sparsam zu verwenden, da nicht nur Banken Auswertungen vornehmen.		
Paypal Die Nutzung von Paypal ist nicht zu empfehlen, da die Fa. besonders viele Daten sammelt und mit Drittanbietern teilt. Eine Kurzübersicht über Drittanbieter ist hier ersichtlich: https://rebecca-ricks.com/paypal-data/		

Clouds

Maßnahme	**Termin**	**Umgesetzt**
Clouds sind nicht zu nutzen, da diese prinzipiell unsicher sind (Stromausfall bzw. Nichterreichbarkeit des Anbieters bzw. Internetausfalls, insbesondere im Ausland). Als Alternative kann bspw. die NextBox https://shop.nitrokey.com/de_DE/shop/product/nextbox-116 genutzt werden, um eine private Cloud zu betreiben. Falls eine Cloud dennoch gewünscht wird, ist am ehesten diese Cloud zu empfehlen: https://www.idgard.de/. Wenn dann nur in Verbindung mit einer Smartcard.		

Alternative zu Skype / Webkonferenzen

Maßnahme	**Termin**	**Umgesetzt**
Eine Alternative zu Skype sind diese sicheren Varianten: https://jitsi.org/ oder https://element.io/ (beides kostenfrei).		
Webkonferenzen		

https://jitsi.org/jitsi-meet/ ist die kostenfreie und sichere Variante sowie weitere Alternativen sind: https://bigbluebutton.org/ oder https://nextcloud.com/talk/ Eine kostenpflichtige Variante ist https://wire.com/de/, die nur dann zu empfehlen ist, wenn es dabei auf einem eigenen Server läuft. Zoom ist nicht zu empfehlen, wenn dann nur mit Tor und ohne Videoansicht und unter einer Alias-E-Mailanschrift sowie Alias-Namen mitnutzen.		

Online sicher unterwegs

Maßnahme	**Termin**	**Umgesetzt**
Handy/Laptop etc. nicht unbeaufsichtigt liegen lassen Die eigenen Geräte sind unterwegs immer bei sich zu führen und niemals unbeaufsichtigt liegen zu lassen, da u.a. ein Spionage-App/Programm installiert werden kann. Gilt auch für das PKW.		
Blickschutzfolie (für unterwegs) Eine Blickschutzfolie ist für den Laptop zu benutzen. Hier ist 3M Marktführer. Bitte vor Ort testen, ob die Qualität gut ist.		
Unbeobachtete Passworteingabe beim Login Es ist darauf zu achten, dass beim Login eine Beobachtung der Eingabe von Passwörtern durch fremde Personen nicht ermöglicht wird. Dies gilt analog auch für Überwachungskameras, wie es bspw. in Zügen vorkommt.		
Keine Bluetooth-Geräte nutzen Bluetooth Geräte wie bspw. Kopfhörer sind unsicher, daher sind schnurgebundene Kopfhörer zu bevorzugen.		
Internetcafés / Keine fremden PCs nutzen Fremde PCs können Keylogger enthalten, daher sind ausschließlich eigene Geräte zu bevorzugen.		
Keine öffentlichen WLAN‘s oder Hotspots nutzen Es ist ausschließlich die eigene Mobilfunkverbindung zu nutzen.		

Einkauf in der digitalen Welt und in der realen Welt

Maßnahme	Termin	Umgesetzt
Einkauf in der digitalen Welt Vorsicht bei Bezahlung in der digitalen Welt, denn hier ist u.a. die Gefahr eines Identitätsdiebstahls am höchsten! Nach Möglichkeit fast immer in bar vor Ort zu bezahlen. Sonst die Rechnung bzw. - sofern dem Anbieter vertraut wird - die Vorkasse vorzuziehen als EC-Zahlung. Kreditkarte - nach Möglichkeit - nur bei Autovermietung (wegen Kaution) nutzen. Das sogenannte „kontaktlose Bezahlen“ ist zu deaktivieren. Ansonsten siehe Punkt Schutzhülle bei Handy/Smartphone. **Tipp:** Nicht direkt bei Amazon bestellen, sondern über den Anbieter. Meist ist der Anbieter (Marketplace) mit seinem vollen Namen hinterlegt, so dass dessen persönliche Webseite aufgerufen werden kann und dort bestellt wird - je nach Vertrauenswürdigkeit des Anbieters-. Bei der Bestellung prinzipiell als Gast bestellen. Keine Bestellung bei unverschlüsselten Seiten ausführen. Wenn Sie unsicher sind, ob die Webseite wirklich sicher verschlüsselt ist, können Sie es hier kostenfrei überprüfen: https://www.ssllabs.com/ssltest/ oder https://ssl-trust.com/SSL-Zertifikate/check		
Beim Einkauf Bei Einkäufen ist eine öffentliche E-Mailanschrift zu verwenden bzw. eine temporäre E-Mailanschrift, falls es eine einmalige Bestellung sein sollte. Eine temporäre E-Mailanschrift ist dieser Link: https://ulm-dsl.de/.		
(Sicherheits-)Zertifikate Wenn ein Anbieter auf der Webseite ein sog. (Sicherheits-)Zertifikat vorweist, so ist darauf zu achten, dass es „echte“ Logos sind und ob der Anbieter „vollumfänglich“ geprüft wurde. Hier kann man überprüfen, ob der Anbieter darunter gehört: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/7148_pdf.pdf?__blob=publicationFile&v=6 Dazu gehören u.a. TÜV-Siegel und Trusted Shops – SSL verschlüsselt. Auch Zertifizierungen garantieren keine Sicherheit!		
Einkauf in der realen Welt Nicht über WLAN im Café/Einkaufszentrum etc. einloggen, da diese genutzt werden, um Sie zu tracken. Auch ist das Smartphone vor dem Einkauf auf Flugmodus zu stellen bzw. besser auszuschalten, da neuerdings auch ohne Einloggen getrackt wird. Es wird prinzipiell in bar bezahlt.		

Eigene Webseite

Maßnahme	Termin	Umgesetzt
https-Verschlüsselung und Prüfung Logfiles Ihre eigene Webseite muss eine https-Verschlüsselung aufweisen können. Ob die Verschlüsselung dabei sauber ist, können Sie hier kostenfrei überprüfen lassen: https://www.ssllabs.com/ (über Auswahl Server). Zudem ist eine Zwei-Faktor-Authentifizierung zu bevorzugen. Darüber hinaus sind regelmäßig die Logfiles zu überprüfen. Es ist der kostenfreie Dienst SIWECOS https://siwecos.de/ zu nutzen, denn dieser scannt nach Sicherheitslücken auf der Webseite.		
Veröffentlichungen Die Veröffentlichungen sollten idealerweise über die eigene Domain durchgeführt werden. Die beste Variante ist die normale Textform innerhalb der Webseite. Danach als PDF-Dokument in Form einer Verlinkung oder als Downloadvariante. Bei Objekten jedweder Art (Worddatei, PDF-Dokument, Bilder etc.) ist darauf zu achten, dass die Metadaten „sauber" sind. Entsprechende Webseiten zum Entfernen der Metadaten sind hier zu finden: https://websetnet.net/de/how-to-completely-delete-personal-metadata-from-microsoft-office-documents/ bzw. https://www.heise.de/download/product/exiftool-35845		
Öffentlicher Kalender Öffentliche Kalender sind nach Möglichkeit nicht zu nutzen, da potentielle Diebe sonst sehen können, ob jemand anwesend ist oder nicht.		
Impressum Ein Impressum darf nicht fehlen. Eine gute Webseite ist diese hier: https://www.e-recht24.de/impressum-generator.html.		

Sicher Reisen

Maßnahme (größtenteils aus der BSI Webseite entnommen: [368])	**Termin**	**Umgesetzt**
Vorbereitung der Reise		

Onlinebuchungen sind nur auf offiziellen und TLS/SSL-verschlüsselten Seiten vorzunehmen. Ein Backup von wichtigen Dokumenten sowie digitale Reisedokumente sind verschlüsselt auf USB-Stick anzulegen. Sicherheitsfunktionen der mobilen Geräte sind zu aktualisieren und aktivieren - dazu ist ein Backup vorher anzulegen! Idealerweise sollte hier ein gesondertes mobiles Gerät genutzt werden, welches nur für Reisen im Ausland genutzt wird. Die mobilen Geräte sind mit mind. 8 Zeichen - sofern möglich - zu sichern. Dazu gehört auch die Einrichtung der Passwortabfrage auf jedem Gerät und bei jeder Anwendung. Vor Hinreise ist das heimische WLAN zu deaktivieren. Für die Reise nach Amerika gibt es ein ausführliches Dokument von der EFF, wie die Privatsphäre vor der Einreise optimal geschützt werden kann: https://www.eff.org/files/2018/01/11/digital-privacy-border-12-2017.pdf (52 Seiten, Stand: Dezember 2017)		
Während der Reise Keine sensiblen Daten über öffentliche WLAN - inklusive Übernachtungsstätte - versenden. Die drahtlosen Schnittstellen (NFC, Bluetooth und WLAN) sind nur bei Gebrauch zu aktivieren. Urlaubsbilder in sozialen Netzwerken erst bei der Rückkehr posten (bzw. gar nicht), um Einbrecher nicht darauf aufmerksam zu machen. Externe Speichermedien sind möglichst nur schreibgeschützt zu verwenden. Es sind keine fremden USB-Sticks anzuschließen. Das Hotelzimmer - einschließlich Safe - ist zur Verwahrung von IT ungeeignet, da elektronische Schließsysteme nicht sicher sind. Beim Fernseher - Smart-TV - ist der Netzstecker zu ziehen. Durch Airbnb vermittelte Zimmer sind nach verstecken Kameras zu prüfen.		
Nach der Reise Das Heimnetzwerk ist wiederherzustellen, Zugangsberechtigungen sind zu überprüfen und das Passwort zu ändern. Das WLAN ist zu aktivieren, Zugangsberechtigungen sind zu überprüfen und Passwort ggf. ändern. E-Mails von unbekannten Absendern bzw. mit ungewöhnlichem Betreff sind ungelesen zu löschen. Reisedokumente aus dem USB-Stick sind sicher zu löschen. Das IT-System ist auf den neuesten Stand zu bringen (Update). Sicherheitskopien von wichtigen Daten wie Reisefotos sind zu erstellen.		

Offline sicher verhalten

Maßnahme	Termin	Umgesetzt
Ausweise: Die Ausweise (Personalausweise, Reisepass) sind in RFID-Schutzhüllen einzuhüllen, was hierüber bezogen werden kann: https://www.pass-sicherheit.de/index.php?manu=m34_RFID-Schutzhuelle-RFID-Schutz-NFC-Schutz.html **Personalausweis:** Beim Personalausweis ist darüber hinaus die sog. Online-Ausweisfunktion zu deaktivieren.		
Arztbesuch Den Arzt explizit darauf hinweisen, dass an keiner Studie - auch nicht in anonymisierter Form - teilgenommen wird. Darüber hinaus ist vor vernetzten Praxen Vorsicht zu walten (ideal ist eine Patientenakte in Papierform, um digitale Abflüsse zu vermeiden). Eine Arztterminvereinbarung ist nicht online durchzuführen, da diese meist nicht nur unsicher sind, sondern auch tracken (bspw. Doctolib). Daher ausschließlich telefonisch Termine vereinbaren.		
Befragungen/Feedbacks Aus Prinzip ist an Befragungen/Feedbacks - sowohl online als auch offline - nicht teilzunehmen, auch wenn Anonymisierung angeboten wird.		
Bilder/Filme Nach Möglichkeit von Personen außerhalb der Familie nicht fotografieren bzw. filmen lassen, insbesondere vor allem im Gesichtsbereich sowie den Händen (Stichwort: Fingerabdrücke). Hochauflösende Fotos bzw. Filme stellen auch ein erhebliches Risiko dar. Das Risiko für (u.a. unbewussten) Missbrauch durch Dritte ist zu hoch.		
Callcenter Callcenter sind nach Möglichkeit nicht zu nutzen, da diese i.d.R. mit Spracherkennungstechnologien ausgestattet sind, womit u.a. die Stimmung erfasst wird und zu dieser Stimmung passende Antworten automatisiert generiert werden.		
Gewinnspiele mit Erhebung der Kontaktdaten Keine Teilnahme an Gewinnspielen jedweder Art.		

IoT Geräte / Smart Speaker / Smart-TV Auf jede Art von IoT-Geräten einschließlich u.a. Fitnesstracker, Smart Speaker sowie Smart-TV ist zu verzichten. Bei Nutzung nur, wenn der Zugang ins Internet gesperrt ist. Sonst sind die Datenschutz- und Sicherheitsrisiken zu hoch.		
Vertrauliche Gespräche Hier ist darauf zu achten, dass nicht nur bei Ihnen alle elektronischen Geräte ausgeschaltet sind, sondern auch beim Gesprächspartner.		

Optimales Licht

Maßnahme	**Termin**	**Umgesetzt**
Smartphone Eine sog. „Bluelightprotect“-App ist zu installieren. Hinweis: die u.g. Schutzbrille ist wirksamer, da der Blaulichtanteil nicht wirklich wesentlich reduziert wird.		
Schutzbrille bei jedweder Art von Bildschirmen Entweder beim Augenoptiker eine Brille kaufen, die den Blaulichtanteil wesentlich reduziert oder bei der Firma Innovative Eyewear bzw. bei gut geführten Läden vor Ort: https://www.innovative-eyewear.de/ Die Schutzbrillen sind zu tragen, sobald es draußen dunkel wird bzw. kann entfallen, sofern das Laptop bzw. der Rechner den Blaulichtanteil bei Dunkelheit automatisch reduzieren.		

PKW

Maßnahme	**Termin**	**Umgesetzt**
Bluetooth Jedwede Verbindungen zum Bordcomputer - u.a. über Bluetooth - sind nicht zu nutzen. Dies gilt vor allem für fremd genutzte Autos.		

Elektroauto Von der Nutzung eines Elektroautos - hier Tesla - ist vor allem aus Safety-Sicht abzuraten (Brandgefahr durch Akkus, unsicheres Schließsystem). Zudem werden sensible und umfangreiche Fahrdaten an den Hersteller gesendet, die nicht abgestellt werden kann.		
Navigationsgerät Bei Benutzung von eingebauten Navigationsgeräten ist bei fremden - auch gemieteten - Autos darauf zu achten, dass die eingegeben Ziele gelöscht werden. In diesem Fall ist bei Rückgabe das Bordsystem auf Werkseinstellung zurückzusetzen. Daher sollte ein eigenes Navigationsgerät (kein Smartphone) benutzt werden.		

Umzug

Maßnahme	**Termin**	**Umgesetzt**
Nach dem Umzug Beim Ummelden im Meldeamt den Widerspruch gegen Datenweitergabe gleich mitbringen. Musterformulare sind hier zu finden: https://selbstauskunft.net/meldebehoerde-widerspruch		

Weiterführende Informationen zur Informationssicherheit und zum Datenschutz

Maßnahme	**Termin**	**Umgesetzt**
Eine Übersicht über Bedrohungen in Echtzeit zeigt diese Karte an: https://cybermap.kaspersky.com/de Weitere gute Informationsmöglichkeiten zum Schutz der IT-Systeme sind folgende Seiten: https://appcheck.mobilsicher.de/, https://www.kuketz-blog.de/, https://secuso.aifb.kit.edu/642.php, https://www.privacy-handbuch.de/download/privacy-handbuch.pdf, https://prism-break.org/de/, https://www.eff.org/ oder https://ssd.eff.org/ (auf Englisch), https://www.privacyinternational.org/ (auf Englisch), https://tacticaltech.org/ (auf Englisch), https://spreadprivacy.com/tag/device-privacy-tips/ (auf Englisch).		
Kostenfreie Lernplattformen		

Eine digitale Lernplattform ist das Hasso-Plattner-Institut: https://open.hpi.de/. Dort werden u.a. folgende Themen vorgestellt: Linux für Alle, Embedded Smart Home, Big Data Analytics, Wie funktioniert das Internet?, Sicherheit im Internet, Sichere Email, Social Media (What No One has Told You about Privacy - auf Englisch). Informationen zur Künstlicher Intelligenz gibt es darüber: https://ki-campus.org/. Die Anwendung von Verschlüsselung kann hierüber erfolgen: http://openpgp-schulungen.de/. Wie Verschlüsselung funktioniert, kann hier erlernt werden: https://www.cryptool.org/de/.		

7. Fazit

Wie wenig Optionen beim Nutzer übrigbleiben, um nicht nur Informationssicherheit, sondern auch Datenschutz möglichst umfassend praktizieren zu können, ist als sehr kritisch zu bewerten. Hier ist eindeutig zu konstatieren, dass der eigene Handlungsspielraum bereits jetzt klein geworden ist und langfristig immer enger sein wird. Die Rahmenbedingungen zwingen Menschen dazu, mehr für ihren eigenen Schutz handeln zu müssen, wie es früher nicht der Fall war. Ein Fallbeispiel dazu: Während es noch heute einen Aufschrei gibt, wenn jede beliebige Person eine Wohnung von jemanden unerlaubt durchsucht hätte, ist es auf der digitalen Ebene bereits längst Realität geworden. Wie im Kapitel 6 aufgezeigt wurde, ist es möglich, sich vor allem im persönlichen Bereich ganzheitlich zu schützen, wobei die Schutzmöglichkeiten außerhalb des eigenen Haushaltes erheblich geringer bzw. z.T. gar nicht möglich sind. Der Umfang bzw. die Vielfalt der Schutzmaßnahmen sind dem Umstand geschuldet, dass die Digitalisierung sich in immer mehr Lebensbereiche ausbreitet, so dass der Aufwand hierfür adäquat ansteigt. Dies wäre nicht der Fall gewesen, wenn von Anfang an, die im Kapitel 4 genannten Schutzmaßnahmen - privacy by security etc. - sowie vor allem Verschlüsselung berücksichtigt worden wären, einschließlich der Anwendung von Datenminimierung. Gerade letztere hätte nicht die Entwicklung von Plattformen wie Alphabet oder Meta ermöglicht, wenn die dortigen US-Gesetze entsprechende Vorgaben gehabt hätten. In diesem Zusammenhang nützen die besten Sicherheitsempfehlungen des BSI für die meisten Soft- bzw. Hardware-Produzenten nicht, da diese sich außerhalb des EU-Rechtsrahmens befinden und damit nicht bindend sind. Anders gelagert wäre es der Fall gewesen, wenn in der EU europaweit eine verbindliche Vorgabe gegeben hätte, in der Soft- als auch Hardware-Produzenten zur Berücksichtigung der Mindeststandards der Informationssicherheit verpflichtet gewesen wären, bevor diese in der EU eingesetzt werden dürfen. In diesem Fall wäre der Aufwand für den (EU-)Nutzer erheblich geringer und zugleich überschaubarer gewesen, zudem wäre mehr Vertrauen in IT-Systeme entsprechend gerechtfertigt gewesen. Das Bewusstsein des Nutzers für Gefahren durch IT-Systeme ist einerseits - wenn auch in Teilen - vorhanden, aber andererseits werden Schutzmaßnahmen nicht umgesetzt, bspw. durch die bislang nicht vermehrte Nutzung von E-Mailverschlüsselungsprogrammen, was aufzeigt, dass hier ein erheblicher Bedarf an Sensibilisierungen besteht. Bei entsprechendem Bewusstsein wäre die Nachfrage nach Schutzmöglichkeiten wie bspw. Jondonym https://anonymous-proxy-servers.net/index.html (Stand: 25.03.2022) oder eBlocker https://eblocker.org/ (Stand: 25.03.2022), sonst wesentlich höher gewesen und die beiden Firmen hätten den Service inzwischen nicht aus wirtschaftlichen Gründen einstellen müssen. Immerhin besteht bei eBlocker die Möglichkeit, die Software weiterhin zu nutzen. Dies gilt auch für die Tatsache, dass bspw. die beiden Plattformen Alphabet und Meta überdurchschnittlich hohe Nutzer vorweisen, anstatt - aufgrund des jeweiligen Geschäftsmodells und des Gebarens ggü. Nutzern - diese zu meiden, da die Risiken sowohl für den Einzelnen als auch für die Gesellschaft insgesamt erheblich höher und umfangreicher sind als der Nutzen. Zudem kommt noch das Risiko der Zweckentfremdung der Daten hinzu.

Die effektivste Schutzmaßnahme ist vor diesem Hintergrund Datenminimierung, was letzten Endes Selbstdatenschutz ist. Hilfreich wäre an dieser Stelle eine weltweite Rankingliste der größten Datensammler zu erstellen, weil diese i.d.R. sehr intransparent dabei vorgehen, was potentielle Nutzer in falsche Sicherheit wiegen lässt. Solange Daten von Unternehmen als strategische Ressource angesehen werden, müssen alle Services unter diesem Gesichtspunkt betrachtet werden. Bspw. ist eine App dahingehend zu prüfen, ob diese so entwickelt wurde, dass bei Nutzung der App dabei ein Maximum an Datenspuren entstehen oder ist diese datensparsam entwickelt worden, wobei letztere derzeit sich in der Minderzahl befindet. Am ehesten sind diese Apps beim App Store F-Droid zu finden. Selbst eine interdisziplinäre Forschungsgruppe, die zwei Jahre zum Thema Daten geforscht hat, kommt zum Fazit: „Es ist für die durchschnittlichen NutzerIn gegenwärtig schwierig und vermutlich unmöglich, eine Internetnutzung ohne Tracing/Tracking vorzunehmen, wenn man das gesamte Spektrum von Tracking Pixel, Fingerprint, etc. Praktiken betrachtet.“ [369, p. 47]. Allein nur durch die Bewegungen am Touchscreen ist es möglich, mit einer Erfolgsrate von über 90 % die Nutzer korrekt wieder zu identifizieren, so dass hier das Risiko einer dauerhaften eindeutigen Tracking Möglichkeit besteht s. [370]. Daher bleibt die Frage zu gesetzlichen Regelungen zur Datenhoheit bzw. Datensouveränität weiterhin offen.

Öffentliche Aussagen der Regierung zu Geheimdienstangelegenheiten sind kritisch zu hinterfragen. Als Beispiel wird auf die öffentliche Zusage vom damaligen Präsidenten Barack Obama ggü. der damaligen Bundeskanzlerin Angela Merkel verwiesen, dass ihr Handy nicht mehr von der NSA abgehört wird s. [371]. Stattdessen hat die NSA u.a. über den dänischen Geheimdienst Merkels Handy weiterhin überwachen lassen und von diesem die Daten erhalten s. [372]. Die Aussage von Präsident Obama an sich war richtig gewesen, dies schließt dennoch die Option nicht aus, dass “befreundete“ Geheimdienste für die NSA zuarbeiten. Davon unabhängig gibt es weiterhin die Option, den unmittelbaren Personenkreis von der damaligen Bundeskanzlerin Merkel zu überwachen, um Einblicke in ihr Regierungshandeln zu erhalten. Seit der Veröffentlichung von Edward Snowden sind neun Jahre vergangen, in dem sich die Abhör- und Speicherkapazitätsfähigkeiten der Geheimdienste - insbesondere der Five Eyes - inzwischen deutlich verbessert haben. Zudem wurden auch mehr Überwachungsbefugnisse für deutsche Geheimdienste sowie für Strafverfolgungsbehörden eingeräumt, ohne dass dabei eine Überwachungsgesamtrechnung durchgeführt wurde. Bevor eine Aufzeichnung von Kommunikationsinhalten durch die Strafverfolgungsbehörden erfolgen darf, muss ein Richter dies erst genehmigen bzw. im Nachhinein bei Gefahr in Verzug. Hier ist allerdings zu konstatieren, dass „[i]n der Praxis … derartige Anträge … selten abgelehnt [werden] … was darauf hindeutet, dass eine eingehende Prüfung der Rechtmäßigkeit durch die … Richter nicht durchweg sichergestellt ist.“ [373, p. 236]. Zudem wurde festgestellt, dass die Parlamentarische Nachrichtenkontrolle des Bundestages bislang nicht seiner Aufgabe in dem Umfang nachgekommen ist, wie es erforderlich wäre. Selbst der UN-Menschenrechtsausschuss ist über die weitreichenden Befugnisse für die Terrorismusbekämpfung in Deutschland besorgt und hat daher Deutschland angemahnt, „dass die Be-

fugnisse, die den Strafverfolgungsbehörden durch die Gesetzgebung … in voller Übereinstimmung mit dem Pakt stehen, einschließlich der Grundsätze der Rechtmäßigkeit und Verhältnismäßigkeit.“ [374, p. 4]. Darüber hinaus muss berücksichtigt werden, dass über das Internet verschlüsselte Daten abgefangen werden, wie es z.B. durch den GHCQ praktiziert wird, um es später durch neue Entschlüsselungsmöglichkeiten wie der Quantenkryptographie entschlüsseln zu können. Selbst wenn ein Quantencomputer in 10 Jahren geben sollte, dauert es einen gewissen Zeitrahmen bis die jetzt gegenwärtigen Verschlüsselungsmethoden auf die Post-Quanten-Kryptographie umgestellt sind, sofern die vorhandenen Software-Produkte updatefähig ist. Bis dahin wären alle derzeit verschlüsselten Daten “öffentlich“ verfügbar. Darüber hinaus gibt es bereits jetzt neue Ansätze verschlüsselte Datensätze zu analysieren. Einem israelischem Forschungsteam ist es gelungen, anhand des verschlüsselten Internetverkehrs mit Hilfe vom Deep-Learning-Techniken „die Kategorie des Datenflusses (Browsen, Chat, Video usw.) und die verwendete Anwendung“ [328] mit hoher Genauigkeit zu klassifizieren s. [328]. Mit diesem Ansatz sowie zukünftig weiteren Ansätzen wäre eine Identifikation von Tor Nutzern absehbar im Bereich des Möglichen. Derzeit wird das Tor-Netzwerk durch einen bislang unbekannten - vermutlich staatlich unterstützten - Angreifer versucht - mit Hilfe von bis zu 900 bösartigen Servern im Tor-Netzwerk - Nutzer zu de-anonymisieren, um sie identifizieren zu können s. [375]. Der Angreifer ist unter dem Namen KAX17 bekannt geworden und dieser hatte somit bereits fast 10 % von derzeit über 7.000 Knoten bzw. Servern unter seiner Kontrolle gehabt s. [375]. Trotz dieses Angriffes ist die Nutzung des Tor-Netzwerkes bis dato die beste Option, um kurz- bis mittelfristig eine hohe Anonymität zu bewahren. Allein dieser Angriff zeigt auf, dass eine echte vertrauliche Nutzung durch Nutzer weltweit nicht erwünscht ist und zeigt eine zentrale Schwachstelle und Risiko zugleich an anderer Stelle auf. Wenn Tor dermaßen infiltriert sein bzw. nicht mehr geben sollte, so ist in diesem Fall eine möglichst anonyme und sichere Onlinenutzung nicht mehr möglich. Abschließend wird auf dieses Zitat aufmerksam gemacht: „Hinter jedem Algorithmus stecken Menschen mit Interessen und Absichten.“ [376, p. VIII]. Solange Menschen hinter IT-Systemen stehen, kann ein Missbrauch nicht ausgeschlossen werden, daher sind Schutzmaßnahmen unumgänglich.

8. Zusammenfassung und Ausblick

Durch die zunehmende Digitalisierung ist der ganzheitliche Informationssicherheitsschutz nicht nur unmittelbar auf den eigenen Haushaltsbereich des Bürgers beschränkt, sondern auch auf Organisationen, die der Bürger z.T. unter Zwang benutzt - hier Meldestelle, Finanzamt, Versicherungen etc. -. Der ganzheitliche Blick ermöglicht neue Einsichten, wie weit der Bürger bereits von IT-Systemen abhängig ist - die er auch nicht selbst unmittelbar beeinflussen kann -, sei es bei IT-Systemen in Banken, Behörden, Plattformen, Versicherungen etc.. Als Fallbeispiel weisen Banken sehr viele Schnittstellen zu anderen Organisationen auf, u.a. zu Scoringstellen sowie zu Amtsgerichten hinsichtlich potentieller Insolvenzbekanntmachungen. Allein die Schnittstellen ermöglichen Angreifer einen vielfältigen Einblick in die Daten unterschiedlicher Organisationen. Verschärft wird diese Entwicklung durch den zunehmenden Einsatz von Big-Data-Mechanismen, in dem tiefgreifende Erkenntnisse über den jeweiligen Bürger gezogen werden können, die u.U. zum dessen Nachteil gereichen können und mind. das Schutzziel Vertraulichkeit verletzt. Dies gilt analog auch für den vermehrten Einsatz von KI, bei dem keinerlei Schutzmaßnahmen zurzeit greifen können. Die Inanspruchnahme von Onlinediensten - vor allem außerhalb von Europa - zeigen auf, dass hier eine systematische Abhängigkeit der Nutzer gewollt ist. Diese rühren zum einen durch Netzwerk- bzw. Sogeffekte, wie sie bspw. durch die möglichst breite Nutzung von WhatsApp im Bekannten- bzw. Freundeskreis entstehen kann und zum anderen durch das Nutzungsdesign, die z.T. Dark Pattern Elemente beinhalten, um somit mehr von dem Nutzer zu erfahren und gleichzeitig zu einer langfristigen Nutzung zu bewegen, um damit dauerhafte Datenströme zu generieren. Durch die Forschung im Persönlichkeitsbereich in Kombination mit den erhobenen Onlinedaten gibt es inzwischen sehr tiefe Einblicke in die Persönlichkeitsmerkmale der Nutzer. Bereits jetzt sind in Echtzeit aufgrund der darin erhobenen Erkenntnisse Manipulationen möglich wie es bspw. bei den Wahlen in den USA durch Cambridge Analytica zur Wahl von Donald Trump im Jahr 2018 angewendet wurde s. [377]. Hinzu kommen noch geostrategische Interessen, die aufzeigen, dass das Schutzziel Verfügbarkeit auch aus anderen Gründen gefährdet sein kann wie es bspw. durch die temporäre Einstellung des US-Bezahldienstleisters Paypal aufgrund der aktuellen Geschehnisse an russische Bürger erfolgt ist. Zusätzlich gehören auch aus geheimdienstlichen Interessen bewusst eingebaute Hintertüren, die nachweislich durch die NSA in IT-Produkten von US-Firmen implementiert wurden und weltweit verkauft werden, was u.a. das Schutzziel Vertraulichkeit sowohl der Organisation, die diese IT-Produkte nutzen als auch der Nutzer, die die Dienste der Organisation in Anspruch nehmen, gefährdet. Seit der Veröffentlichung von Edward Snowden haben die Strafverfolgungsbehörden sowie Geheimdienste - nicht nur in Deutschland - mehr Befugnisse zur Überwachung erhalten, wobei bis heute in Deutschland eine Überwachungsgesamtrechnung ausblieb. Zudem wurde konstatiert, dass die Prüfung sowohl auf Seiten der Gerichte für die Strafverfolgungsbehörden als auch im Parlamentarischen Kontrollgremium des Bundestages für die Geheimdienste nicht immer mit der gebotenen Sorgfalt erfolgt.

Warum die Handy bzw. Smartphone Nutzung nicht zu empfehlen ist, zeigt dieses Fallbeispiel exemplarisch auf: Das Unternehmen Syniverse wurde bereits seit 2016 gehackt. Dieses Unternehmen „bietet Backbone-Dienste für Mobilfunkanbieter … weltweit an [und] verfügt über „direkte Verbindungen“ zu mehr als 300 Mobilfunkbetreibern“ [378]. Die Angreifer hatten Zugang zu „Metadaten wie Dauer und Kosten, Anrufer- und Empfängernummern, Standort der Gesprächspartner sowie zum Inhalt von SMS-Nachrichten“ [378]. Da dieser Angriff sechs Jahre lang unentdeckt blieb und einen Einblick in den weltweiten Mobilfunkverkehr ermöglicht hat, ist die Wahrscheinlichkeit sehr hoch, dass hier ein staatlicher Angreifer dahinterstehen könnte.

Was die zukünftige Perspektive der Informationssicherheit für Bürger angeht, so wird der Optimismus von Prof. Dr. Hannes Federrath nicht geteilt, der wie folgt Stellung genommen hat: „Ich bin überzeugt davon, dass wir auf lange Sicht zu einer Steigerung der Sicherheit kommen werden, da immer mehr Sensibilität vorhanden ist und auch die Schutztechnologien in dieser Hinsicht besser werden.“ [379]. Bereits im Jahr 2017 gab es ein Gutachten, die die Entwicklung der digitalen Souveränität für Verbraucher als „besorgniserregend“ [380, p. 59] bezeichnet hat und nach jetzigem Stand fast gar nicht zu realisieren ist. Dazu wurde unter anderem gefordert, das Recht auf Vergessenwerden zu ermöglichen und Audits beim Datenhandel zu ermöglichen s. [380, p. 58]. Beide Ansätze sollten spätestens im Jahr 2022 konkret umgesetzt sein, was bis heute nicht geschehen ist. Auch sind die notwendigen Voraussetzungen für die Grundlagenforschung geeigneter Open-Source-Software bislang nicht geschaffen sowie der Einsatz von datenschutzfreundlichen kryptographischen Methoden nicht vorgeschrieben worden s. [380, p. 59]. Erschwerend kommt hinzu, dass der Europäische Parlamentarische Forschungsdienst eine Studie zur Massenüberwachung geschrieben hat und als Schutzmöglichkeit auf viele Open Source Projekte aufmerksam gemacht, wovon einige heute nicht mehr existieren, was aufzeigt, dass ein dauerhafter Service nicht immer gewährleistet wird s. [381, pp. 45-53]. Diese Fallbeispiele zeigen exemplarisch auf, dass der Bürger sich nicht darauf verlassen kann, dass die politischen Stellen - die als einzige Stelle noch in der Lage ist - folgendes umsetzen würden: U.a. sollen die Hersteller von Hard- und Software zur Berücksichtigung von Mindeststandards der Informationssicherheit verpflichtet werden, was vor Inbetriebsetzung durch eine unabhängige Organisation zu prüfen ist. Falls diese Forderungen nicht umgesetzt werden sollten, verbleibt dem Bürger als Nutzer zugleich als einzige wirkungsvolle Option übrig, eine minimalistische Nutzung von nur erforderlichen vollverschlüsselten IT-Systemen sowie bei Onlinenutzung Tor in Anspruch zu nehmen. Damit kann dieser sich einerseits kurz- bis mittelfristig schützen und andererseits mit dieser Vorgehensweise den wirtschaftlichen Akteuren sowie der Politik Nachdruck verleihen, dass die soeben genannten bzw. in Kapitel 4 vollständig aufgeführten Anforderungen an die Politik vollumfassend durch die wirtschaftlichen Akteure und der öffentlichen Verwaltung zu realisieren sind. Ohne die politische Unterstützung ist langfristig eine Realisierung von ganzheitlicher Informationssicherheit für Bürger aufgrund der in dieser Arbeit genannten Rahmenbedingungen nicht möglich. Ob die in Kapitel 6 genannten ganzheitlichen Schutzmaßnahmen für den Bürger praktikabel sind, wäre an dieser Stelle noch zu erforschen.

Literaturverzeichnis

[1] T. WITTENHORST, „Windows 10: Microsoft gibt Übermittlung von Telemetriedaten neue Bezeichnungen," 7. März 2020. [Online]. Available: https://www.heise.de/newsticker/meldung/Windows-10-Microsoft-gibt-Uebermittlung-von-Telemetriedaten-neue-Bezeichnungen-4678330.html. [Zugriff am 23. März 2022].

[2] G. MASCOLO, „Die Bilanz der Regierung im NSA-Skandal ist beschämend," 13. Februar 2017. [Online]. Available: https://www.sueddeutsche.de/politik/geheimdienste-die-bilanz-der-regierung-im-nsa-skandal-ist-beschaemend-1.3375209. [Zugriff am 22. März 2022].

[3] G. RAAB, A. UNGER und F. UNGER, Die Theorie kognitiver Dissonanz, In: Marktpsychologie. Gabler., 2010, p. 42.

[4] M. BRANDT, „Nur eine Minderheit verschlüsselt E-Mails," Statista, März 2018. [Online]. Available: https://de.statista.com/infografik/9522/nutzung-von-ende-zu-ende-verschluesselung/. [Zugriff am 12. März 2022].

[5] STEINEBACH, BADER, RINSDORF, KRÄMER und ROßNAGEL, Desinformation aufdecken und bekämpfen, 1. Auflage Hrsg., Baden-Baden: Nomos Verlagsgesellschaft mbh & Co. KG, 2020.

[6] L. MROHS, „Facebook missbraucht Handynummern zu Werbezwecken," 6. März 2019. [Online]. Available: https://netzpolitik.org/2019/facebook-missbraucht-handynummern-zu-werbezwecken/. [Zugriff am 20. März 2022].

[7] C. ECKERT, IT-Sicherheit Konzepte - Verfahren – Protokolle, 10. Auflage Hrsg., De Gruyter Oldenbourg, 2018, p. 1.

[8] N. POHLMANN, Cyber-Sicherheit, Springer Vieweg, 2019, p. 3.

[9] R. ANDERSON, Security Engineering A Guide to Building Dependable Distributed Systems, 3. Auflage Hrsg., Wiley, 2020.

[10] BSI, „BSI-Standard 200-1," November 2017. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_1.html?nn=128578.

[11] BSI, „Register aktueller Cyber-Gefährdungen und -Angriffsformen," Juli 2018. [Online]. Available: https://www.allianz-fuer-

cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_026.pdf?__blob=publicationFile&v=1. [Zugriff am 26 März 2022].

[12] ANONLEAKS, „ProSite … alter Klabauter, das ist doch kein Hoster," November 2021. [Online]. Available: https://anonleaks.net/2021/optinfoil/prosite-alter-klabauter-das-ist-doch-kein-hoster/.

[13] K. BIERMANN, „BKA hat NSO-Spähtrojaner bereits mehrfach eingesetzt," September 2021. [Online]. Available: https://www.zeit.de/politik/deutschland/2021-09/spionagesoftware-pegasus-bka-einsatz-nso-trojaner-israel.

[14] F. FKIE, „Hardware- und Hardwarenahe Trojaner - Überblick und Bedrohungslage," Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE, August 2017. [Online]. Available: https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HWT-Bericht/HWT-Bericht_Cover.pdf.

[15] D. SCHIRRMACHER, „Sicherheitsupdates: Cisco entfernt Backdoor aus Business Switches," 8. November 2018. [Online]. Available: https://www.heise.de/security/meldung/Sicherheitsupdates-Cisco-entfernt-Backdoor-aus-Business-Switches-4216400.html. [Zugriff am 7. Dezember 2021].

[16] E&E, „Hardware-Trojaner - Die unterschätzte Gefahr," 5. September 2017. [Online]. Available: https://www.industr.com/de/hardware-trojaner-die-unterschaetzte-gefahr-2304085. [Zugriff am 20. August 2021].

[17] M. SCHWARZ, „A Practical Introduction to Transient Execution Attacks," 5. September 2017. [Online]. Available: https://esorics2021.athene-center.de/tutorial-07-28.php. [Zugriff am 20. August 2021].

[18] BSI, „Die Lage der IT-Sicherheit in Deutschland 2020," Oktober, Bonn, 2020.

[19] FRAUNHOFER FKIE, „Erhebliche Sicherheitsmängel bei Home Routern festgestellt," Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE, 26. Juni 2020. [Online]. Available: https://www.fkie.fraunhofer.de/de/Pressemeldungen/Home-Router.html. [Zugriff am 20. August 2021].

[20] FRAUNHOFER FKIE, „FACT - Firmware Analysis and Comparison Tool," Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE, 2020. [Online]. Available:

https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/FraunhoferSolutionDays2020/FKIE_Produktblatt_FACT_DE.pdf.

[21] CCC, „CCC und OpenWrt: Technische Richtlinie des BSI zu sicheren Routern unzureichend," Computer Chaos Club, 19. November 2018. [Online]. Available: https://www.ccc.de/de/updates/2018/risikorouter. [Zugriff am 12. Dezember 2021].

[22] BUNDESVERBAND IT-SICHERHEIT e.V. (TeleTrusT), „Handreichung zum „Stand der Technik"," 2021.

[23] M. GURI, Y. SOLEWICZ, A. DAIDAKULOV und Y. ELOVICI, „SPEAKE(a)R: Turn Speakers to Microphones for Fun and Profit," November 2016.

[24] N. JURRAN, „Smartphone-Spiele belauschen Nutzer," 30. Dezember 2017. [Online]. Available: https://www.heise.de/newsticker/meldung/Smartphone-Spiele-belauschen-Nutzer-3928850.html. [Zugriff am 12. Dezember 2021].

[25] MDR, „Smartphone: Was tun, wenn die App mithört?," 1. Februar 2022. [Online]. Available: https://www.mdr.de/brisant/ratgeber/app-smartphone-mithoeren-werbung-100.html. [Zugriff am 5. Februar 2022].

[26] J. MÜLLER, V. MLADENOV, J. SOMOROVSKY und J. SCHWENK, „SoK: Exploiting Network Printers," Mai 2017.

[27] BSI, „CON.5: Entwicklung und Einsatz von Individualsoftware," BSI, Bonn, 2020.

[28] C. WINDECK, „Intel-Prozessoren: undokumentierter Debugging-Zugriff erforscht," 19. Dezember 2018. [Online]. Available: https://www.heise.de/newsticker/meldung/Intel-Prozessoren-undokumentierter-Debugging-Zugriff-erforscht-4256525.html. [Zugriff am 5. Dezember 2021].

[29] M. MANTEL, „Hardware-Sicherheitslücken: Intel schloss 2021 mehr als 200 Schlupflöcher," Februar 2022. [Online]. Available: https://www.heise.de/news/Hardware-Sicherheitsluecken-Intel-schloss-2021-mehr-als-200-Schlupfloecher-6350278.html.

[30] J. RUTKOWSKA, „Intel x86considered harmful," Oktober 2015. [Online]. Available: https://blog.invisiblethings.org/papers/2015/x86_harmful.pdf. [Zugriff am 5. Februar 2022].

[31] EFF, „List of Printers Which Do or Do Not Display Tracking Dots,“ 2017. [Online]. Available: https://www.eff.org/pages/list-printers-which-do-or-do-not-display-tracking-dots. [Zugriff am 5. Januar 2022].

[32] R. GRAHAM, „How The Intercept Outed Reality Winner,“ 5. Juni 2017. [Online]. Available: https://blog.erratasec.com/2017/06/how-intercept-outed-reality-winner.html. [Zugriff am 5. Dezember 2021].

[33] M. TREMMEL, „Das Jahr der unsicheren Sicherheitssoftware,“ 18. Januar 2021. [Online]. Available: https://www.golem.de/news/antivirus-das-jahr-der-unsicheren-sicherheitssoftware-2101-153432.html. [Zugriff am 4. August 2021].

[34] RACK911 Labs, „Exploiting (Almost) Every Antivirus Software,“ 20. April 2020. [Online]. Available: https://rack911labs.ca/research/exploiting-almost-every-antivirus-software/. [Zugriff am 4. August 2021].

[35] M. HOLLAND, „Kaspersky gehackt: Israelische Agenten sollen russischen NSA-Hack entdeckt haben,“ 11. Oktober 2017. [Online]. Available: https://www.heise.de/newsticker/meldung/Kaspersky-gehackt-Israelische-Agenten-sollen-russischen-NSA-Hack-entdeckt-haben-3856403.html. [Zugriff am 5. August 2021].

[36] J. BROOME, „Harvesting Cb Response Data Leaks for fun and profit,“ 9. August 2017. [Online]. Available: https://www.directdefense.com/harvesting-cb-response-data-leaks-fun-profit/. [Zugriff am 6. Juli 2021].

[37] A. SOWA, „Austauschen statt Weglaufen,“ <*kes*>, Nr. #2, p. 6, 2015.

[38] BSI, „Mindeststandard des BSI für Schnittstellenkontrollen,“ Juli 2021. [Online]. Available: https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Schnittstellenkontrollen/Schnittstellenkontrollen_node.html. [Zugriff am 5. Januar 2022].

[39] D. CAPURRO und E. VELLOSO, „Dark Patterns, Electronic Medical Records, and the Opioid Epidemic,“ Mai 2021.

[40] BSI, „Kriterienkatalog Cloud Computing C5:2020,“ BSI, Bonn, 2020.

[41] H. A. JÄGER und R. O. RIEKEN, Manipulationssichere Cloud-Infrastrukturen, Springer Vieweg, 2020.

[42] PASSWARE, „Passware Kit Forensic,“ [Online]. Available: https://www.passware.com/kit-forensic/. [Zugriff am 5. Februar 2022].

[43] BKA, „"Cybercrime" Bundeslagebild 2020,“ BKA, 10. Mai 2021. [Online]. Available:

https://www.bka.de/SharedDocs/Kurzmeldun0gen/DE/Kurzmeldungen/210507_BLBCyber.html. [Zugriff am 5. September 2021].

[44] STATISTISCHES BUNDESAMT, „Durchschnittliche Anzahl von Tagen zur Identifizierung und Eindämmung von Datenlecks nach Branchen weltweit im Jahr 2020," August 2020. [Online]. Available: https://de.statista.com/statistik/daten/studie/1196872/umfrage/durchschnittliche-dauer-zur-identifizierung-von-datenlecks-nach-branchen/.

[45] FIREYE, „M-Trends 2021 Report," 2021.

[46] HPI, „ Wurden Ihre Identitätsdaten ausspioniert?," [Online]. Available: https://sec.hpi.de/ilc/?lang=de. [Zugriff am 16. August 2021].

[47] M. WAIDNER, M. BACKES und J. MÜLLER-QUADE, „Positionspapier Cybersicherheit in Deutschland," Fraunhofer Verlag, Stuttgart, 2017.

[48] A. WHITTEN und J. TYGAR, „Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," August 1999.

[49] M. ANDREE und T. THOMSEN, Atlas der Digitalen Welt, Frankfurt am Main: Campus Verlag GmbH, 2020.

[50] E. MÜLLING, Big Data und der digitale Ungehorsam, Wiesbaden: Springer VS, 2019.

[51] BUNDESKARTELLAMT, „Google: Feststellung der überragenden marktübergreifenden Bedeutung für den Wettbewerb," 5. Januar 2022. [Online]. Available: https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Fallberichte/Missbrauchsaufsicht/2022/B7-61-21.pdf;jsessionid=8316D512EB84EAEA83F6E05022E8BD17.2_cid390?__blob=publicationFile&v=7. [Zugriff am 17. Februar 2022].

[52] B. SCHWAN, „Google zahlt angeblich 15 Milliarden an Apple – nur für die Safari-Suche," 27. August 2021. [Online]. Available: https://www.heise.de/news/Google-zahlt-angeblich-15-Milliarden-an-Apple-nur-fuer-die-Safari-Suche-6175833.html. [Zugriff am 17. Februar 2022].

[53] BUNDESKARTELLAMT, „Hintergrundinformationen zum Facebook-Verfahren des Bundeskartellamtes," 2017.

[54] IT-MAGAZIN, „Apple speichert massenweise iCloud-Daten auf Google Cloud," 30 Juni 2021. [Online]. Available: https://www.itmagazine.ch/artikel/74958/Apple_speichert_massenweise_iCloud-Daten_auf_Google_Cloud.html. [Zugriff am 17. Februar 2022].

[55] S. HURTZ, „50 Millionen Patientendaten landen auf Googles Servern," 13. November 2019. [Online]. Available: https://www.sueddeutsche.de/digital/google-project-nightingale-gesundheitsdaten-ascension-1.4681463. [Zugriff am 2. Februar 2022].

[56] NATIONALE AKADEMIE DER WISSENSCHAFTEN LEOPOLDINA, UNION DER DEUTSCHEN AKADEMIEN DER WISSENSCHAFTEN und ACA-TECH - DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHA, „Digitalisierung und Demokratie," Nationale Akademie der Wissenschaften Leopoldina, Union der deutschen Akademien der Wissenschaften, acatech – Deutsche Akademie der Technikwissenschaften (2021): Digitalisierung und Demokratie., Halle (Saale)., 2021.

[57] S. ZUBOFF, Das Zeitalter des Überwachungskapitalismus, 1. Hrsg., Frankfurt am Main: Campus Verlag, 2018.

[58] AMNESTY INTERNATIONAL, „Surveillance giants: How the business model of Google and Facebook threatens human rights," Amnesty International Ltd, London, 2019.

[59] INTERNET SOCIETY, „The Internet is changing," 2019. [Online]. Available: https://future.internetsociety.org/2019/introduction/executive-summary/. [Zugriff am 25. März 2022].

[60] R. TANGENS, „BBA 2021 - Kategorie „Was mich wirklich wütend macht"," 11. Juni 2021. [Online]. Available: https://bigbrotherawards.de/2021/was-mich-wirklich-wuetend-macht-google#sdfootnote13sym. [Zugriff am 24. Februar 2022].

[61] N. JACOBSEN, „"Unsere Daten werden mit militärischer Effizienz gegen uns gerichtet": Apple-Chef Tim Cook erhebt erneut schwere Vorwürfe gegen Facebook und Google," 24. Oktober 2018. [Online]. Available: https://meedia.de/2018/10/24/unsere-daten-werden-mit-militaerischer-effizienz-gegen-uns-gerichtet-apple-chef-tim-cook-erhebt-erneut-schwere-vorwuerfe-gegen-facebook-und-google/. [Zugriff am 21. Februar 2022].

[62] IRISH COUNCIL FOR CIVIL LIBERTIES, „Europe's enforcement paralysis," [Online]. Available: https://www.iccl.ie/digital-data/2021-gdpr-report/. [Zugriff am 5 Dezember 2021].

[63] EDSA, „EDSA nimmt ersten Beschluss gemäß Artikel 65 an," 10. November 2020. [Online]. Available: https://edpb.europa.eu/news/news/2020/edpb-adopts-first-art-65-decision_de. [Zugriff am 21. Februar 2022].

[64] EDSA, „Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article

65(1)(a) GDPR," 28. Juli 2021. [Online]. Available: https://edpb.europa.eu/system/files/2021-09/edpb_bindingdecision_202101_ie_sa_whatsapp_redacted_en.pdf. [Zugriff am 21. Februar 2022].

[65] DERAKTIONÄR, „GAFAM Index," [Online]. Available: https://www.deraktionaer.de/aktien/kurse/gafamindex-de000sla2ua7.html. [Zugriff am 27. Februar 2022].

[66] STATISTISCHES BUNDESAMT, „Europäische Union: Bruttoinlandsprodukt (BIP) in den Mitgliedstaaten der EU im Jahr 2020," 2020. [Online]. Available: https://de.statista.com/statistik/daten/studie/188776/umfrage/bruttoinlandsprodukt-bip-in-den-eu-laendern/. [Zugriff am 23. März 2022].

[67] H. SCHMIDT, „Plattform-Ökonomie," Dezember 2021. [Online]. Available: https://www.netzoekonom.de/plattform-oekonomie/. [Zugriff am 12. Februar 2022].

[68] S. KNORRE, H. MÜLLER-PETERS und F. WAGNER, Die Big-Data-Debatte, Wiesbaden: Springer Gabler, 2020.

[69] M. JAEKEL, Die Macht der digitalen Plattformen, Wiesbaden: Springer Vieweg, 2017.

[70] R. PFISTER, „Google rät jedem, seinen Namen zu ändern," 19. August 2010. [Online]. Available: https://www.sueddeutsche.de/digital/google-chef-eric-schmidt-google-raet-jedem-seinen-namen-zu-aendern-1.990045. [Zugriff am 2. Februar 2022].

[71] C. STÖCKER, „Google will die Weltherrschaft," 8. Dezember 2009. [Online]. Available: https://www.spiegel.de/netzwelt/netzpolitik/netz-strategie-google-will-die-weltherrschaft-a-665813.html. [Zugriff am 8. Februar 2022].

[72] U. STADELMANN, „Google Vaterfigur Eric Schmidt verlässt Alphabet," 22. Dezember 2017. [Online]. Available: https://www.nzz.ch/wirtschaft/googles-vaterfigur-eric-schmidt-verlaesst-alphabet-ld.1342502. [Zugriff am 8. Februar 2022].

[73] R. L. RUTLEDGE, A. MASSEY und . A. I. ANTON, „Privacy Impacts of IoT Devices: A SmartTV Case Study," September 2016.

[74] FACHFORUM AUTONOME SYSTEME IM HIGHTECH-FORUM, „Autonome Systeme - Chancen und Risiken für Wirtschaft, Wissenschaft und Gesellschaft," Fachforum Autonome Systeme im Hightech-Forum, Berlin, 2017.

[75] J. E. A. (. MÜLLER-QUADE, „Künstliche Intelligenz und IT-Sicherheit - Bestandsaufnahme und Lösungsansätze Whitepaper," Plattform Lernende Systeme, München, 2019.

[76] J. SCHMIDT, „Ripple20 erschüttert das Internet der Dinge," 17. Juni 2020. [Online]. Available: https://www.heise.de/security/meldung/Ripple20-erschuettert-das-Internet-der-Dinge-4786249.html. [Zugriff am 2. Februar 2022].

[77] E. RODRIGUES, R. ASSUNCAO, G. L. PAPPA, R. MIRANDA und W. MEIRA JR, „Uncovering the location of Twitter users," Oktober 2013.

[78] G. XU, L. LI, Y. ZHANG, X. YI und M. KITSUREGAWA, „Modeling user hidden navigational behavior for Web recommendation," Januar 2011.

[79] A. BARCZOK, „Versteckspiel Ortung auf dem Smartphone verhindern," *C'T* , Nr. Heft 16/2013, 2013.

[80] M. REUTER, „Wie Bluetooth-Kopfhörer unseren Standort verraten," 2. September 2021. [Online]. Available: https://netzpolitik.org/2021/tracking-wie-bluetooth-kopfhoerer-unseren-standort-verraten/. [Zugriff am 20. Februar 2022].

[81] W. CHRISTL, „Corporate Surveillance in Everyday Life," Juni 2017. [Online]. Available: https://crackedlabs.org/en/corporate-surveillance. [Zugriff am 1. Februar 2022].

[82] M. SCHREMS, „Übersicht über Datenkategorien von Facebook," 3. April 2012. [Online]. Available: http://europe-v-facebook.org/fb_cat1.pdf. [Zugriff am 27. Februar 2022].

[83] M. TURCK, J. WU und FIRSTMARK, „Machine Learning, Artificial Intelligence, and Data (MAD) Landscape," November 2021. [Online]. Available: https://46eybw2v1nh52oe80d3bi91u-wpengine.netdna-ssl.com/wp-content/uploads/2021/12/Data-and-AI-Landscape-2021-v3-small.jpg. [Zugriff am 1. Februar 2022].

[84] M. TURCK, „Red Hot: The 2021 Machine Learning, AI and Data (MAD) Landscape," November 2021. [Online]. Available: https://mattturck.com/data2021/. [Zugriff am 1. Februar 2022].

[85] R. SHMELKIN, T. FRIEDLANDER und L. WOLF, „Generating Master Faces for Dictionary Attacks with a Network-Assisted Latent Space Evolution," August 2021.

[86] M. ANDERSON, „‘Master Faces’ That Can Bypass Over 40% Of Facial ID Authentication Systems,“ 4. August 2021. [Online]. Available: https://www.unite.ai/master-faces-that-can-bypass-over-40-of-facial-id-authentication-systems/. [Zugriff am 12. Januar 2022].

[87] CLEARVIEW, „Company Overview,“ [Online]. Available: https://www.clearview.ai/overview. [Zugriff am 24. März 2022].

[88] T. RUDL, „Clearview AI zieht gegen kanadische Datenschutzbehörde vor Gericht,“ 25. Januar 2022. [Online]. Available: https://netzpolitik.org/2022/biometrie-clearview-ai-zieht-gegen-kanadische-datenschutzbehoerde-vor-gericht/. [Zugriff am 12. Februar 2022].

[89] CNBC, „Ukraine has started using Clearview AI’s facial recognition during war,“ 13. März 2022. [Online]. Available: https://www.cnbc.com/2022/03/13/ukraine-has-started-using-clearview-ais-facial-recognition-during-war.html. [Zugriff am 14. März 2022].

[90] SPIEGEL, „Künstliche Intelligenz soll Menschen am Gang erkennen,“ 7. November 2018. [Online]. Available: https://www.spiegel.de/netzwelt/netzpolitik/china-kuenstliche-intelligenz-erkennt-menschen-an-ihrem-gang-a-1237157.html. [Zugriff am 20. Februar 2022].

[91] A. LOBE, „Was der Gang über die Person verrät,“ 16. Februar 2022. [Online]. Available: https://www.spektrum.de/kolumne/lobes-digitalfabrik-was-der-gang-ueber-die-person-verraet/1987888. [Zugriff am 20. Februar 2022].

[92] S. L. H. NANDYALA, „Privacy Impact Assessment: Instagram,“ Januar 2018.

[93] B. PEREZ, M. MUSOLESI und G. STRINGHINI, „You Are Your Metadata: Identification and Obfuscation of Social Media Users using Metadata Information,“ März 2018.

[94] D. SELLA-VILLA, „Drones and Data: A Limited Impact on Privacy,“ März 2020.

[95] RHEINPFALZ Redaktion, „Sauna-Überflug bleibt ein Rätsel,“ 1. Juli 2017. [Online]. Available: https://www.rheinpfalz.de/startseite_artikel,-sauna-%C3%BCberflug-bleibt-ein-r%C3%A4tsel-_arid,922611.html. [Zugriff am 12. Februar 2022].

[96] R. ZHANG, N. ZHANG, C. DU, W. LOU, Y. T. HOU und Y. KAWAMOTO, „From Electromyogram to Password: Exploring the Privacy Impact of Wearables in Augmented Reality,“ September 2017.

[97] J. TORRES-SOSPEDRA und A. OMETOV, „Data from Smartphones and Wearables,“ April 2021.

[98] Z. ALRABABAH, „Privacy and Security of Wearable Devices,“ Dezember 2020.

[99] A. ROSSI, E. D. POZZO, D. MENICAGLI, C. TREMOLANTI, C. PRIAMI, A. SIRBU, D. A. CLIFTON, C. MARTINI und D. MORELLI, „A Public Dataset of 24-h Multi-Levels Psycho-Physiological Responses in Young Healthy Adults,“ September 2020.

[100] G. JHANSI, G. S. RAMA, K. RANGANATH, T. K. JULURI, C. VINAY, K. REDDY und V. R. CHALAMALLA, „Face detection authentication analysis on smartphones Face detection authentication analysis on smartphones,“ Dezember 2020.

[101] J. L. KRÖGER und P. RASCHKE, „Is My Phone Listening in? On the Feasibility and Detectability of Mobile Eavesdropping,“ Juni 2019.

[102] S. A. ANAND, C. WANG, J. LIU, N. SAXENA und Y. CHEN, „Spearphone: A Speech Privacy Exploit via Accelerometer-Sensed Reverberations from Smartphone Loudspeakers,“ Juli 2019.

[103] G. BAL, „Revealing Privacy-Impacting Behavior Patterns of Smartphone Applications,“ Januar 2012.

[104] V. BRIEGLEB, „Carrier IQ: Der Spion, der mit dem Smartphone kam?,“ 1. Dezember 2011. [Online]. Available: https://www.heise.de/newsticker/meldung/Carrier-IQ-Der-Spion-der-mit-dem-Smartphone-kam-1388109.html. [Zugriff am 22. Februar 2022].

[105] M. HATAMIAN, N. MOMEN, L. FRITSCH und K. RANNENBERG, „A Multilateral Privacy Impact Analysis Method for Android Apps,“ Juni 2019.

[106] A. KLINGEL, „GESUND DANK ALGORITHMEN? Chancen und Herausforderungen von Gesundheits-Apps für Patient:innen,“ Stiftung Neue Verantwortung, Berlin, 2019.

[107] B. FUEST, „Der neue Überwachungswahn im Kinderzimmer,“ 9. Januar 2015. [Online]. Available: https://www.welt.de/wirtschaft/webwelt/article136216319/Der-neue-Ueberwachungswahn-im-Kinderzimmer.html. [Zugriff am 1. Februar 2022].

[108] M-SPY, „Die beste Mobilftelefonversorgung für die Kindersicherung,“ [Online]. Available: https://www.mspy.com.de/. [Zugriff am 17. März 2022].

[109] GREENBONE, „Sicherheitsbericht Ungeschützte Patientendaten im Internet,“ 16. September 2019. [Online]. Available: http://web.archive.org/web/20190917074148/https://www.greenbone.net/wp-content/uploads/CyberResilienceReport_DE.pdf. [Zugriff am 6. Dezember 2021].

[110] Y. MIRSKY, T. MAHLER, I. SHELEF und Y. ELOVICI, „CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning,“ Januar 2019.

[111] C. BERNDT, K. KAMPLING und J. KLOFTA, „Patientendaten sind meist schlecht geschützt,“ 12. November 2019. [Online]. Available: https://www.sueddeutsche.de/politik/patientendaten-hacker-sicherheit-1.4678689. [Zugriff am 5. Januar 2022].

[112] P. WELCHERING, „Der Handel mit Corona-Daten boomt,“ 10. Januar 2021. [Online]. Available: https://www.zdf.de/nachrichten/panorama/corona-darknet-patienten-daten-100.html. [Zugriff am 2. Februar 2022].

[113] M. MUTH, „"Diese Menschen haben keinerlei Mitgefühl",“ 29. Oktober 2020. [Online]. Available: https://www.sueddeutsche.de/digital/vastaamo-erpresser-cyberkriminalitaet-1.5097181. [Zugriff am 2. Februar 2022].

[114] S. DAS, „Mental health helpline funded by royals shared users' conversations,“ 19. Februar 2022. [Online]. Available: https://www.theguardian.com/society/2022/feb/19/mental-health-helpline-funded-by-royals-shared-users-conversations. [Zugriff am 21. Februar 2022].

[115] R. EICKENBERG, H. GIESELMANN und S. TREMMEL, „Massive Datenschutzmängel in der Gesundheits-App Ada,“ https://www.heise.de/ct/artikel/Massive-Datenschutzmaengel-in-der-Gesundheits-App-Ada-4549354.html, 11. Oktober 2019. [Online]. [Zugriff am 2. Februar 2022].

[116] W. RUDSCHIES und T. KROHER, „Autonomes Fahren: So fahren wir in Zukunft,“ 8. September 2021. [Online]. Available: https://www.adac.de/rund-ums-fahrzeug/ausstattung-technik-zubehoer/autonomes-fahren/technik-vernetzung/aktuelle-technik/. [Zugriff am 1. März 2022].

[117] N. GATZERT, S. KNORRE, H. MÜLLER-PETERS und F. WAGNER, „Big Data in der Mobilität - Grünbuch -,“ 2022.

[118] GOSLAR INSTITUT, „Goslar Diskurs 2022: Big Data in der Mobilität,“ Januar 2022. [Online]. Available: https://www.goslar-

institut.de/veranstaltung/goslar-diskurs-2022-big-data-in-der-mobilitaet/. [Zugriff am 15. Januar 2022].

[119] T. KROHER, „Neues EU-Gesetz überwacht Kraftstoff- und Stromverbrauch," 13. Januar 2022. [Online]. Available: https://www.adac.de/rund-ums-fahrzeug/ausstattung-technik-zubehoer/assistenzsysteme/obfcm/. [Zugriff am 2. Februar 2022].

[120] EU, „Verordnung (EU) 2019/631 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Festsetzung von CO2-Emissionsnormen für neue Personenkraftwagen und für neue leichte Nutzfahrzeuge und zur Aufhebung der Verordnungen (EG) Nr. 443/2009 und (EU) Nr.," 17. April 2019. [Online]. Available: https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A32019R0631. [Zugriff am 1. Februar 2022].

[121] F. ROSENGART, „Der BigBrotherAward 2021 in der Kategorie Verkehr geht an die Europäische Kommission für die Einführung des „On-Board Fuel Consumption Meter" (OBFCM)," 11. Juni 2021. [Online]. Available: https://bigbrotherawards.de/2021/verkehr-europaeische-kommission. [Zugriff am 1. Februar 2022].

[122] R. EICKENBERG, J. HEIDRICH, H. GIESELMANN und C. WÖLBERT, „Daten-Leak bei Autovermietung Buchbinder: 3 Millionen Kundendaten offen im Netz," 22. Januar 2020. [Online]. Available: https://www.heise.de/ct/artikel/Daten-Leak-bei-Autovermietung-Buchbinder-3-Millionen-Kundendaten-offen-im-Netz-4643015.html. [Zugriff am 5. Dezember 2021].

[123] T. BOLTON, T. DARGAHI, S. BELGUITH, M. AL-RAKHAMI und A. H. SODHRO, „On the Security and Privacy Challenges of Virtual Assistants," März 2021.

[124] Z. HUANG, J. EPPS und D. JOACHIM, „Investigation of Speech Landmark Patterns for Depression Detection," Oktober 2019.

[125] E. MAOR, J. D. SARA, D. M. ORBELO, L. O. LERMAN, Y. LEVANON und A. LERMAN, „Voice Signal Characteristics Are Independently Associated With Coronary Artery Disease," Juli 2018.

[126] K. CRAWFORD und V. JOLER, „Anatomy of an AI System," 7. September 2018. [Online]. Available: https://anatomyof.ai/. [Zugriff am 29. Januar 2022].

[127] L. KAISER, „Amazon Echo: Alexa sendet Privatgespräch heimlich an Arbeitskollegen," 25. Mai 2018. [Online]. Available:

https://netzpolitik.org/2018/amazon-echo-alexa-sendet-privatgespraech-heimlich-an-arbeitskollegen/. [Zugriff am 1. März 2022].

[128] G. CHALHOUB und I. FLECHAIS, „“Alexa, are you spying on me?”: Exploring the Effect of User Experience on the Security and Privacy of Smart Speaker Users,“ Juli 2020.

[129] DR. DATENSCHUTZ, „Datenerhebung in Hotels und ihre rechtlichen Grenzen,“ 15. November 2017. [Online]. Available: https://www.dr-datenschutz.de/datenerhebung-in-hotels-und-ihre-rechtlichen-grenzen/. [Zugriff am 4. August 2021].

[130] M. HOLLAND, „Marriott: Daten von 500 Millionen Hotelgästen abgegriffen,“ 30. November 2018. [Online]. Available: https://www.heise.de/security/meldung/Marriott-Daten-von-500-Millionen-Hotelgaesten-abgegriffen-4236576.html. [Zugriff am 8. Februar 2022].

[131] S. R. PEPPET, „Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future,“ 2011.

[132] G. GOLDACKER, „Internettracking,“ Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS - Kompetenzzentrum Öffentliche Informationstechnologie, Berlin, 2018.

[133] K.-P. ECKERT, L. HENCKEL und P. HOEPNER, „Big Data - Ungehobene Schätze oder digitaler Albtraum,“ Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS, Berlin, 2014.

[134] T. WEICHERT, „Prism, Big Data und der Datenschutz - bei uns und in den USA,“ 9. Juli 2013. [Online]. Available: https://www.datenschutzzentrum.de/artikel/98-Prism,-Big-Data-und-der-Datenschutz-bei-uns-und-in-den-USA.html. [Zugriff am 22. Februar 2022].

[135] BSI, „Künstliche Intelligenz,“ [Online]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/kuenstliche-intelligenz_node.html. [Zugriff am 24. März 2022].

[136] DATENETHIKKOMMISSION DER BUNDESREGIERUNG, „Gutachten der Datenethikkommission,“ Datenethikkommission der Bundesregierung Bundesministerium des Innern, für Bau und Heimat, Berlin, 2019.

[137] DIN/DKE, „Whitepaper Ethik und Künstliche Intelligenz: Was können technische Normen und Standards leisten?,“ DIN e.V. DKE Deutsche Kommission Elektrotechnik , Berlin / Frankfurt, 2020.

[138] BSI, „Sicherer, robuster und nachvollziehbarer Einsatz von KI," BSI, Bonn, 2021.

[139] AW ALGORITHM WATCH gGmbH, „Atlas der Automatisierung / Automatisierte Entscheidungen und Teilhabe in Deutschland," AW ALGORITHM WATCH gGmbH, Berlin, 2019.

[140] CCC, „Biometrische Videoüberwachung: Der Südkreuz-Versuch war kein Erfolg," 13. Oktober 2018. [Online]. Available: https://www.ccc.de/de/updates/2018/debakel-am-suedkreuz. [Zugriff am 1. Januar 2022].

[141] C. HUSTEDT, „„Es muss nicht immer KI sein": Carla Hustedt warnt Behörden vor Software, die sie nicht verstehen," 17. März 2021. [Online]. Available: https://algorithmenethik.de/2021/03/17/es-muss-nicht-immer-ki-sein/. [Zugriff am 22. Februar 2022].

[142] S. BECK et al, „Künstliche Intelligenz und Diskriminierung Herausforderungen und Lösungsansätze," Lernenende Systeme - Die Plattform für Künstliche Intelligenz, München, 2019.

[143] BSI, „Deepfakes - Gefahren und Gegenmaßnahmen," [Online]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html. [Zugriff am 22. März 2022].

[144] ENISA, „Artificial Intelligence Cybersecurity Challenges," ENISA, Attiki, 2020.

[145] J. HEESEN, J. MÜLLER-QUADE und S. WROBEL et al, „Kritikalität von KI-Systemen in ihren jeweiligen Anwendungskontexten," Lernende Systeme - Die Plattform für Künstliche Intelligenz, München, 2021.

[146] J. KIPPER, Künstliche Intelligenz - Fluch oder Segen?, 1. Auflage Hrsg., Stuttgart: J.B. Metzler, 2020.

[147] PLATTFORM LERNENDE SYSTEME, „Von Daten zu Wertschöpfung," Lernende Systeme - Die Plattform für Künstliche Intelligenz, München, 2020.

[148] DEUTSCHE AKADEMIE DER WISSENSCHAFTEN acatech, „KI-Regulierung: Wie sich vertrauenswürdige Systeme gestalten lassen," 23. November 2021. [Online]. Available: https://www.acatech.de/allgemein/ki-regulierung-wie-sich-vertrauenswuerdige-systeme-gestalten-lassen/. [Zugriff am 28. Januar 2022].

[149] CENTER FOR HUMANE TECHNOLOGY, „Ledger of Harms,“ Juni 2021. [Online]. Available: https://ledger.humanetech.com/. [Zugriff am 12. Dezember 2021].

[150] S. VOSOUGHI, D. ROY und R. S. ARAL, „The spread of true and false news online,“ März 2018.

[151] O. BENDEL, „Social Bots,“ Juli 2021. [Online]. Available: https://wirtschaftslexikon.gabler.de/definition/social-bots-54247/version-384530. [Zugriff am 14. Dezember 2021].

[152] M. DEL VICARIO, A. BESSI, F. ZOLLO, F. PETRONI, A. SCALA, G. CALDARELLI, H. E. STANLEY und W. QUATTROCIOCCHI, „The spreading of misinformation online,“ 2016.

[153] M. R. UNCAPHER und A. D. WAGNER, „Minds and brains of media multitaskers: Current findings and future directions,“ Oktober 2018.

[154] HAUFE ONLINE REDAKTION, „Arbeitsunterbrechungen und Multitasking: Ungestört arbeitet es sich besser,“ 22. März 2019. [Online]. Available: https://www.haufe.de/arbeitsschutz/gesundheit-umwelt/multitasking-kleine-unterbrechungen-mit-grossen-folgen_94_404590.html. [Zugriff am 12. Oktober 2021].

[155] L. CHEN, R. NATH und Z. TANG, „Understanding the Determinants of Digital Distraction: An Automatic Thinking Behavior Perspective,“ November 2019.

[156] M. BOER, G. STEVENS, C. FINKENAUER und R. v. d. EIJNDEN, „Attention Deficit Hyper-activity Disorder-Symptoms, Social Media Use Intensity, and Social Media Use Problems in Adolescents,“ Oktober 2019.

[157] Q. HE, O. TUREL und A. BECHARA, „Brain anatomy alterations associated with Social Networ-king Site (SNS) addiction,“ März 2017.

[158] M. TIGGEMANN, . S. HAYDEN, Z. BROWN und J. VELDHUIS, „The effect of Instagram “likes” on women’s social comparison and body dissatisfaction,“ September 2018.

[159] P. G. TURNER und C. E. LEFEVRE, „Instagram use is linked to increased symptoms of orthorexia nervosa,“ März 2017.

[160] N. P. ANDREWS, K. YOGEESWARAN, M.-J. WANG, K. NASH, D. R. HAWI und C. G. SIBLEY, „Is Social Media Use Changing Who We Are? Examining the Bidirectional Relationship Between Personality and Social Media Use,“ November 2020.

[161] S. LEMOLA, N. PERKINSON-GLOOR, S. BRAND, J. DEWALD-KAUFMANN und A. GROB, „Adolescents' Electronic Media Use at Night, Sleep Disturbance, and Depressive Symptoms in the Smartphone Age," Februar 2014.

[162] M. H. RIBEIRO, R. OTTONI, R. WEST, V. A. F. ALMEIDA und W. MEIRA, „Auditing Radicalization Pathways on YouTube," Oktober 2021.

[163] R. EPSTEIN und R. E. ROBERTSON, „The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections," August 2015.

[164] M. KAY, C. MATUSZEK und S. A. MUNSON, „Unequal Representation and Gender Stereotypes in Image Search Results for Occupations," April 2015.

[165] S. NOBLE, „Algorithms of oppression: How search engines reinforce racism," New York University Press, 2018. [Online]. Available: https://nyupress.org/9781479837243/algorithms-of-oppression/. [Zugriff am 5. Oktober 2021].

[166] J. SULER, „The Online Disinhibition Effect," Juli 2004.

[167] N. SADIDA und R. CANINSTI, „Considering Innovativeness and Engagement to Overcome Online Disinhibition Effect on Facebook," November 2017.

[168] A. X. WU, H. TANEJA und J. G. WEBSTER, „Going with the flow: Nudging attention online," Juli 2020.

[169] J. D.-S. GUTIÉRREZ, F. R. d. FONSECA und G. RUBIO, „Cell-Phone Addiction: A Review," Oktober 2016.

[170] S. VASANTHAKUMARI und B. WAKUMA, „Nomophobia - Smartphone Addiction," September 2019.

[171] J. LUGURI und L. J. STRAHILEVITZ, „Shining a Light on Dark Patterns," März 2021.

[172] C. M. GRAY, Y. KOU, B. BATTLES, J. HOGATT und A. L. TOOMBS, „The Dark (Patterns) Side of UX Design," April 2018.

[173] A. ROSSE und K. BONGARD-BLANCHY, „All in one stroke? Intervention Spaces for Dark Patterns," März 2021.

[174] C. CARA, „Dark Patterns In The Media: A Systematic Review," Januar 2020.

[175] H. GRASSEGGER und M. KROGERUS, „Ich habe nur gezeigt, dass es die Bombe gibt,“ 3. Dezember 2016. [Online]. Available: https://web.archive.org/web/20170127181034/https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/. [Zugriff am 5. Oktober 2021].

[176] L. L. SALA, J. SKUES und S. GRANT, „Personality Traits and Facebook Use: The Combined/Interactive Effect of Extraversion, Neuroticism and Conscientiousness,“ Oktober 2014.

[177] G. SEIDMAN, „The Big 5 and relationship maintenance on Facebook,“ April 2018.

[178] Y. BACHRACH, M. KOSINSKI, T. GRAEPEL, P. KOHLI und D. STILLWELL, „Personality and Patterns of Facebook Usage,“ Juni 2012.

[179] C.-L. YANG, „The relationships between personality and Facebook photographs: A study in Taiwan,“ Februar 2019.

[180] G. NAVE, J. MINXHA, D. M. GREENBERG, M. KOSINSKI, D. STILLWELL und J. RENTFROW, „Musical Preferences Predict Personality: Evidence from Active Listening and Facebook Likes,“ Juli 2018.

[181] Y. WANG und M. KOSINSKI, „Deep neural networks are more accurate than humans at detecting sexual orientation from facial images,“ 2018.

[182] M. KOSINSKI, „Facial recognition technology can expose political orientation from naturalistic facial images,“ Januar 2021.

[183] S. MATZ und M. KOSINSKI, „Using Consumers’ Digital Footprints for More Persuasive Mass Communication,“ Mai 2019.

[184] W. BENDA, „Wie wirkt sich Rauchen auf die Versicherungen aus?,“ 22. November 2020. [Online]. Available: https://die-finanzpruefer.de/versicherungen/wie-ist-rauchen-in-zusammenhang-mit-versicherungen-zu-bewerten/. [Zugriff am 5. Novemer 2021].

[185] L. CHEN, T. GONG, M. KOSINSKI, D. STILLWELL und R. L. DAVIDSON, „Building a profile of subjective well-being for social media users,“ November 2017.

[186] S. MATZ, M. KOSINSKI, G. NAVE und D. J. STILLWELL, „Psychological targeting as an effective approach to digital mass persuasion,“ November 2017.

[187] W. LAWANONT, P. MONGKOLNAM und C. NUKOOLKIT, „Smartphone posture monitoring system to prevent unhealthy neck postures,“ Juli 2015.

[188] T. R. NASH, E. S. CHOW, A. D. LAW, S. D. FU, E. FUSZAZA, A. BILSKA, P. BEBAS, D. KRETZSCHMAR und J. M. GIEBULTOWICZ, „Daily blue-light exposure shortens lifespan and causes brain neurodegeneration in Drosophila,“ Oktober 2019.

[189] . D. I. TAMIR und J. P. MITCHELL, „Disclosing information about the self is intrinsically rewarding,“ Mai 2012.

[190] M. MORGENROTH, Sie kennen dich! Sie haben dich! Sie steuern dich!, München: Droemer Verlag, 2014.

[191] J. LANIER, „„And so I can’t call these things social networks anymore. I call them behavior modification empires.“,“ TED2018, 07:24 Min, Online, 2018.

[192] C. LAUER, „Überwachungskapitalisten unter sich,“ 14. Oktober 2014. [Online]. Available: https://www.faz.net/aktuell/feuilleton/debatten/ueberwachung/datenschutz-wenn-ueberwachungskapitalisten-unter-sich-sind-13208092.html. [Zugriff am 9. Februar 2022].

[193] A. BENDIEK, „Sorgfaltsverantwortung im Cyberraum,“ Stiftung Wissenschaft und Politik, Berlin, 2016.

[194] M. ANDREAS, „Die Virtualisierung der Kriegsführung,“ *In: Kasprowicz D., Rieger S. (eds) Handbuch Virtualität,* 2019.

[195] A. BENDIEK und M. SCHALLBRUCH, „Europas dritter Weg im Cyberraum,“ Stiftung Wissenschaft und Politik, Berlin, 2019.

[196] H. FARELL und A. L. NEWMAN, „Weaponized Interdependence: How Global Economic Networks Shape State Coercion,“ *International Security ,* pp. 42-79, Juli 2019.

[197] EUROPÄISCHE KOMMISSION, „Gemeinsame Mitteilung an das Europäische Parlament, den Europäischen Rat und den Rat: EU-China - Strategische Perspektiven,“ 2. März 2019. [Online]. Available: https://ec.europa.eu/info/sites/default/files/communication-eu-china-a-strategic-outlook_de.pdf. [Zugriff am 5. Dezember 2021].

[198] CONGRESSIONAL RESEARCH SERVICE, „Renewed Great Power Competition: Implications for Defense - Issues for Congress,“ 1. März 2022. [Online]. Available: https://sgp.fas.org/crs/natsec/R43838.pdf. [Zugriff am 10. März 2022].

[199] TSMC, „About TSMC,“ [Online]. Available: https://www.tsmc.com/english/aboutTSMC. [Zugriff am 22. März 2022].

[200] WIKIPEDIA, „Taiwan Semiconductor Manufacturing Company, Limited (TSMC),“ https://de.wikipedia.org/wiki/TSMC, Januar 2022. [Online]. [Zugriff am 22. März 2022].

[201] J. LEE und J.-P. KLEINHANS, „Taiwan, Chips, and Geopolitics: Part 1,“ 10. Dezember 2020. [Online]. Available: https://thediplomat.com/2020/12/taiwan-chips-and-geopolitics-part-1/. [Zugriff am 5. Dezember 2021].

[202] J. LEE und J.-P. KLEINHANS, „Would China Invade Taiwan for TSMC?,“ 15. Dezember 2020. [Online]. Available: https://thediplomat.com/2020/12/would-china-invade-taiwan-for-tsmc/. [Zugriff am 5. Dezember 2021].

[203] J. LEE, „Chinas Halbleiterindustrie: Strategische Dimensionen und Schlussfolgerungen,“ 30. Juni 2021. [Online]. Available: https://merics.org/de/studie/chinas-halbleiterindustrie-strategische-dimensionen-und-schlussfolgerungen. [Zugriff am 2. Februar 2022].

[204] M. HENNING, „Digitalwirtschaften ärmerer Länder sollen weiter schutzlos bleiben,“ 9. März 2021. [Online]. Available: https://netzpolitik.org/2021/verhandlungen-bei-der-wto-digitalwirtschaften-aermerer-laender-sollen-weiter-schutzlos-bleiben/. [Zugriff am 5. Dezember 2021].

[205] J. KELSEY, „How a TPP-Style E-commerce Outcome in the WTO would Endanger the Development Dimension of the GATS Acquis (and Potentially the WTO),“ *Journal of International Economic Law,* pp. 273-295, Mai 2018.

[206] J. STEILING, „„Free Basics“ von Facebook: Zero Rating, Zero Netzneutralität, Zero Datenschutz,“ 26. August 2017. [Online]. Available: https://netzpolitik.org/2017/free-basics-von-facebook-zero-rating-zero-netzneutralitaet-zero-datenschutz/. [Zugriff am 22. Februar 2022].

[207] G. GREENWALD, Die globale Überwachung. Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen, München: Droemer Verlag, 2014.

[208] A. LOBE, „Google will beim Sturz von Assad mithelfen,“ 24. März 2016. [Online]. Available: https://www.luzernerzeitung.ch/international/google-will-beim-sturz-von-assad-mithelfen-ld.1544782. [Zugriff am 8. Februar 2022].

[209] S. KREMPL, „Maschinenlernen: Google unterstützt das Pentagon mit KI-Technik für Drohnen," 7. März 2018. [Online]. Available: https://www.heise.de/newsticker/meldung/Maschinenlernen-Google-unterstuetzt-das-Pentagon-mit-KI-Technik-fuer-Drohnen-3988378.html. [Zugriff am 8. Februar 2022].

[210] D. SCHIRRMACHER, „Cisco schließt Super-Admin-Lücke," 4. August 2017. [Online]. Available: https://www.heise.de/security/meldung/Cisco-schliesst-Super-Admin-Luecke-3793025.html. [Zugriff am 8. Dezember 2021].

[211] S. CHECKOWAY, J. MASKIEWICZ, C. GARMAN, J. FRIED, S. COHNEY, M. GREEN, N. HENINGER und R.-P. WEINMANN, „RESCORLA, Eric; SHACHAM, Hovav: A Systematic Analysis of the Juniper Dual EC Incident," April 2016.

[212] FAZ, „„Das Internet spaltet sich in zwei Teile auf"," 21. September 2018. [Online]. Available: https://www.faz.net/aktuell/wirtschaft/digitec/ex-google-chef-eric-schmidt-ueber-die-spaltung-des-internets-15799311.html. [Zugriff am 21. Februar 2022].

[213] J. CHUMTONG und C. STOLTE, „Digitale Technologie als neue Machtressource," in *Auslandsinformationen Globale Machtverschiebung*, Berlin, Konrad-Adenauer-Stiftung, 2021, pp. 103-104.

[214] TAGESSCHAU, „Diese Firmen stoppen Russland-Geschäfte," 7. März 2022. [Online]. Available: https://www.tagesschau.de/wirtschaft/unternehmen/russland-rueckzug-unternehmen-101.html. [Zugriff am 11. März 2022].

[215] G. GOLDACKER, „DIGITALE SOUVERÄNITÄT," Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS, Berlin, 2017.

[216] T. KLEINZ, „31C3: Warnung vor Secure Boot und Trusted Computing," 29. Dezember 2014. [Online]. Available: https://www.heise.de/newsticker/meldung/31C3-Warnung-vor-Secure-Boot-und-Trusted-Computing-2507013.html. [Zugriff am 21. Februar 2022].

[217] M. WAIDNER, M. BACKES und J. MÜLLER-QUADE, „Positionspapier Sicherheitstechnik im IT-Bereich," European Center for Security and Privacy by Design Technische Universität Darmstadt, Darmstadt, 2013.

[218] A. WEBER, S. REITH, M. KASPER, D. KUHLMANN, J.-P. SEIFERT und C. KRAUß, „Souveränität und die IT-Wertschöpfungskette," pp. 291-293, April 2018.

[219] A. GREENBERG, „Hackers Remotely Kill a Jeep on the Highway - With Me in It,“ 21. Juli 2015. [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. [Zugriff am 5. Dezember 2021].

[220] H. Dr. GENZKEN, Interviewee, [Interview]. 17. September 2020.

[221] INTEL, „Intel® Transparent Supply Chain,“ [Online]. Available: https://servermarketinglibrary.intel.com/intel-transparent-supply-chain/. [Zugriff am 25. März 2022].

[222] H. DR. GENZKEN, „E-MAIL Befragung,“ ONLINE, 2021.

[223] GRAZ UNIVERSITY OF TECHNOLOGY, „Meltdown and Spectre,“ 2017. [Online]. Available: https://meltdownattack.com/. [Zugriff am 5. Dezember 2021].

[224] C. Wöbert, „Wolkenschloss,“ *c't 2020, Heft 22,* pp. 12-13, Oktober 2020.

[225] E. STEINER, „Putin baut Russlands mächtigste Bank zum Tech-Giganten um,“ 29. März 2021. [Online]. Available: https://www.welt.de/wirtschaft/plus229306501/Wladimir-Putin-baut-Sberbank-zu-russischem-Tech-Giganten-um.html. [Zugriff am 6. Dezember 2021].

[226] BUNDESREGIERUNG, „Dritter Nationaler Aktionsplan verabschiedet,“ 30. Juni 2021. [Online]. Available: https://www.open-government-deutschland.de/opengov-de/dritter-nationaler-aktionsplan-verabschiedet-1936776. [Zugriff am 12. August 2021].

[227] BUNDESKANZLERAMT, „Dritter Nationaler Aktionsplan 2021–2023,“ Berlin, 2021.

[228] H. SCHUMANN und E. SIMANTKE, „Europas fatale Abhängigkeit von Microsoft,“ 13. Mai 2017. [Online]. Available: https://www.tagesspiegel.de/gesellschaft/cyber-attacken-auf-staatliche-it-europas-fatale-abhaengigkeit-von-microsoft/19628246.html. [Zugriff am 22. Februar 2022].

[229] SPIEGEL, „Bundesregierung zahlte mehr als eine Milliarde für Berater,“ 23. September 2021. [Online]. Available: https://www.spiegel.de/politik/deutschland/bundesregierung-zahlte-seit-2017-mehr-als-eine-milliarde-fuer-externe-berater-a-ca9fa226-774f-430f-aa88-d2117d20cdf2. [Zugriff am 10. Oktober 2021].

[230] A. WEBER, G. HEISER, D. KUHLMANN, M. SCHALLBRUCH, A. CHATTOPADHYAY, S. GUILLEY, M. KASPER, C. KRAUß, P. S. KRÜGER, S. REITH und J.-P. SEIFERT, „Sichere IT ohne Schwachstellen und Hintertüren," April 2020.

[231] G. BECKER, F. REGAZZONI, C. PAAR und W. BURLESON, „Stealthy Dopant-Level Hardware Trojans," *In: Bertoni G., Coron JS. (eds) Cryptographic Hardware and Embedded Systems - CHES 2013,* 2013.

[232] MITRE, „2021 CWE Top 25 Most Dangerous Software Weaknesses," 2021. [Online]. Available: https://cwe.mitre.org/top25/archive/2021/2021_cwe_top25.html. [Zugriff am 25. März 2022].

[233] MITRE, „Gesamtanzahl der Schwachstellen," [Online]. Available: https://cwe.mitre.org/cve/. [Zugriff am 21. Januar 2022].

[234] I. SKIERKA, „Fragenkatalog Anhörung des Ausschusses Digitale Agenda zum Thema IT-Sicherheit von Hard- und Software als Voraussetzung für Digitale Souveränität," Berlin, 2019.

[235] S. BÖTTNER, „Sicherstellung und Beschlagnahme von E-Mails auf dem Mailserver des Providers nicht verfassungswidrig," [Online]. Available: https://www.strafrecht-bundesweit.de/strafrecht-blog/sicherstellung-und-beschlagnahme-von-emails-auf-dem-mailserver-des-providers-nicht-verfassungswidrig/. [Zugriff am 20. Januar 2022].

[236] BUNDESRECHTSANWALTSKAMMER, „Stellungnahme Nr. 21. Zu der im Regierungsentwurf eines Gesetzes zur Fortentwicklung der Strafprozessordnung (BR-Drs. 57/21) als § 95a StPO-E vorgesehenen Möglichkeit, im Falle von Durchsuchungen und Beschlagnahmen bei Dritten die bislang gebotene Benachr," Februar 2021. [Online]. Available: https://www.brak.de/fileadmin/05_zur_rechtspolitik/stellungnahmen-pdf/stellungnahmen-deutschland/2021/februar/stellungnahme-der-brak-2021-21.pdf. [Zugriff am 12. Dezember 2021].

[237] M. HIÉRAMENTE, „In aller Heimlichkeit," 5. März 2021. [Online]. Available: https://netzpolitik.org/2021/beschlagnahme-von-e-mails-in-aller-heimlichkeit/. [Zugriff am 9. Oktober 2021].

[238] A. MEISTER, „Große Koalition einigt sich auf Staatstrojaner-Einsatz schon vor Straftaten," 8. Juni 2021. [Online]. Available: https://netzpolitik.org/2021/bundespolizeigesetz-grosse-koalition-einigt-sich-auf-staatstrojaner-einsatz-schon-vor-straftaten/. [Zugriff am 10. Oktober 2021].

[239] V. TRIPP, „"Die Vorratsdatenspeicherung ist und bleibt grundrechtswidrig",“ 22. April 2015. [Online]. Available: https://www.bpb.de/themen/medien-journalismus/netzdebatte/205437/die-vorratsdatenspeicherung-ist-und-bleibt-grundrechtswidrig/. [Zugriff am 5. Oktober 2021].

[240] DER BUNDESBEAUFTRAGE FÜR DEN DATENSCHUTZ UND DIE INFORMATIONSFREIHEIT, „Leitfaden zur Speicherung von Verkehrsdaten,“ November 2021. [Online]. Available: https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Telefon-Internet/Datenschutzpraxis/LeitfadenVerkehrsdaten.html. [Zugriff am 5. Januar 2022].

[241] BUNDESVERFASSUNGSGERICHT, „Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -. Rn. 1-345,“ 2. März 2010. [Online]. Available: http://www.bverfg.de/e/rs20100302_1bvr025608.html. [Zugriff am 10. Oktober 2021].

[242] BUNDESNETZAGENTUR (BNetzA), „Hinweis zur TR TKÜV Ausgabe 7.2,“ 16. Juni 2021. [Online]. Available: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/TechnUmsetzung110/Downloads/TR-TKUEV-Ver-7-2-DE.pdf?__blob=publicationFile&v=6. [Zugriff am 10. Oktober 2021].

[243] M. REUTER, „Die individuelle Personenkennzahl kommt,“ 5. März 2021. [Online]. Available: https://netzpolitik.org/2021/bundesrat-die-individuelle-personenkennzahl-kommt/. [Zugriff am 24. Oktober 2021].

[244] „Gesetz zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz - TerrorBekämpfG,“ 2002. [Online]. Available: https://www.buzer.de/gesetz/4197/index.htm.

[245] AUSSCHUSS FÜR INNERES UND HEIMAT (Bundestag), „Bedenken gegen Entfristung von Vorschriften zur Terrorismusbekämpfung,“ 2. November 2020. [Online]. Available: https://www.bundestag.de/dokumente/textarchiv/2020/kw45-pa-innen-antiterrorgesetze-799842. [Zugriff am 5. Dezember 2021].

[246] T. MULDER und M. TUDORICA, „Privacy policies, cross-border health data and the GDPR,“ Juli 2019.

[247] T. SIGMUND, „Attention Paid to Privacy Policy Statements,“ März 2021.

[248] N. JENTZSCH, „Dateneigentum - Eine gute Idee für die Datenökonomie?,“ Stiftung Neue Verantwortung, Berlin, 2018.

[249] A. M. MCDONALD und L. F. CRANOR, „The Cost of Reading Privacy Policies,“ 2008.

[250] EUROPÄISCHE KOMMISSION, „Vorschlag für eine RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren,“ 17. April 2018. [Online]. Available: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52018PC0226. [Zugriff am 6. Dezember 2021].

[251] BUNDESRECHTSANWALTSKAMMER, „Stellungnahme Nr. 28/2018. Zum Vorschlag der Kommission für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (COM[2018] 225 final vom 1,“ September 2018. [Online]. Available: https://www.brak.de/fileadmin/05_zur_rechtspolitik/stellungnahmen-pdf/stellungnahmen-deutschland/2018/september/stellungnahme-der-brak-2018-28.pdf. [Zugriff am 15. Dezember 2021].

[252] M. SCHALLBRUCH, „e-Evidence: Outsourcing von Grundrechtsschutz (Teil 3),“ 10. Mai 2018. [Online]. Available: https://www.cr-online.de/blog/2018/05/10/e-evidence-outsourcing-von-grundrechtsschutz-teil-3/. [Zugriff am 21. November 2021].

[253] KONFERENZ DER UNABHÄNGIGEN DATENSCHAUFSICHTSBEHÖRDEN DES BUNDES UND DER LÄNDER, „Entschließung: Der Vorschlag der EU-Kommission für eine E-Evidence-Verordnung führt zum Verlust von Betroffenenrechten und verschärft die Problematik der sog. Vorratsdatenspeicherung,“ November 2018. [Online]. Available: https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Entschliessungen_Datenschutzkonferenz/Inhalt/96_-Konferenz/E-Evidence-Verordnung/Entschliessung-E-Evidence.pdf. [Zugriff am 25 März 2022].

[254] M. BORGERS, „Unterlassungsklage von Erdogan / Warten auf die „Böhmermann-Entscheidung“,“ 1. November 2016. [Online]. Available: https://www.deutschlandfunk.de/unterlassungsklage-von-erdogan-warten-auf-die-boehmermann-100.html. [Zugriff am 19. November 2021].

[255] DISCOVER U.S. GOVERNMENT INFORMATION, „PUBLIC LAW 110-261,“ Juli 2008. [Online]. Available:

https://www.govinfo.gov/content/pkg/STATUTE-122/pdf/STATUTE-122-Pg2436.pdf. [Zugriff am 13. Februar 2021].

[256] J. BALLWEBER, „Wie US-Geheimdienste Daten aus der EU abgreifen könnten," 26. Januar 2022. [Online]. Available: https://netzpolitik.org/2022/gutachten-veroeffentlicht-wie-us-geheimdienste-daten-aus-der-eu-abgreifen-koennten/. [Zugriff am 25. Februar 2022].

[257] DEPARTMENT OF JUSTICE, „DIVISION V - CLOUD ACT," März 2018. [Online]. Available: https://www.justice.gov/dag/page/file/1152896/download. [Zugriff am 13. Februar 2022].

[258] AUSSCHUSS FÜR INNERES UND HEIMAT (Bundestag), „Experten reserviert mit Blick auf eine „Überwachungsgesamtrechnung"," 22. Februar 2021. [Online]. Available: https://www.bundestag.de/dokumente/textarchiv/2021/kw08-pa-innen-ueberwachungsgesamtrechnung-820524. [Zugriff am 14. Februar 2022].

[259] A. (. ADENSAMER, „Handbuch Überwachung," epicenter.works - Plattform Grundrechtspolitik, Mai 2020. [Online]. Available: https://handbuch-ueberwachung.at/lesen/. [Zugriff am 14. Februar 2022].

[260] FAZ, „Nachrichtendienst darf weiter Daten von Internet-Knoten abzapfen," 31. Mai 2018. [Online]. Available: https://www.faz.net/aktuell/wirtschaft/digitec/de-cix-verliert-klage-gegen-bnd-15616005.html. [Zugriff am 15. Februar 2022].

[261] SZ, „Betreiber des Frankfurter Internet-Knotens verliert Klage gegen den BND," 31. Mai 2018. [Online]. Available: https://www.sueddeutsche.de/digital/ueberwachung-am-de-cix-betreiber-des-frankfurter-internet-knoten-verliert-klage-gegen-den-bnd-1.3996859. [Zugriff am 22. Februar 2022].

[262] BUNDESVERWALTUNGSGERICHT (BVerwG), „Urteil vom 30.05.2018 - BVerwG 6 A 3.16," 30. Mai 2018. [Online]. Available: https://www.bverwg.de/de/300518U6A3.16.0. [Zugriff am 25. März 2022].

[263] BUNDESVERWALTUNGSGERICHT (BVerwG), „Urteil vom 28.05.2014 - BVerwG 6 A 1.13," 28. Mai 2014. [Online]. Available: https://www.bverwg.de/280514U6A1.13.0. [Zugriff am 15. Februar 2022].

[264] S. KREMPL, „EU-Parlament erlaubt flächendeckende Scans nach Kinderpornografie," 7. Juli 2021. [Online]. Available:

https://www.heise.de/news/EU-Parlament-erlaubt-flaechendeckende-Scans-nach-Kinderpornografie-6130267.html. [Zugriff am 1. März 2022].

[265] „LI (lawful interception),“ Januar 2015. [Online]. Available: https://www.itwissen.info/LI-lawful-interception.html. [Zugriff am 17. Februar 2022].

[266] BAYERISCHES STAATSMINISTERIUM DER JUSTIZ, „Kostenverteilung zwischen Polizei und Staatsanwaltschaften im Strafverfahren,“ https://wiki.piratenpartei.de/wiki/images/5/54/Bayern-skype-tkue.pdf, 19. September 2008. [Online]. Available: https://wiki.piratenpartei.de/wiki/images/5/54/Bayern-skype-tkue.pdf. [Zugriff am 25. März 2022].

[267] D. BORCHERT, „Überwachungssoftware: Aus Hacking Team wurde Hacked Team,“ 6. Juli 2015. [Online]. Available: https://www.heise.de/security/meldung/Ueberwachungssoftware-Aus-Hacking-Team-wurde-Hacked-Team-2736160.html. [Zugriff am 1. März 2022].

[268] LEAKTHEANALYST, „LeakTheAnalyst group Leak critical data from Verint security company,“ 24. Februar 2022. [Online]. Available: https://www.reddit.com/r/InfoSecNews/comments/sxxzju/leaktheanalyst_group_leak_critical_data_from/. [Zugriff am 2. März 2022].

[269] M. B. SEYYAR und Z. GERADTS, „Privacy impact assessment in large-scale digital forensic investigations,“ *Forensic Science International: Digital Investigation,* Nr. Volume 3, Juni 2020.

[270] EU, „Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolg,“ 27. April 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32016L0680. [Zugriff am 5. Oktober 2021].

[271] SANS, „The Most Relevant Evidence per Gigabyte,“ März 2021. [Online]. Available: https://sansorg.egnyte.com/dl/70HVz2FsAd/. [Zugriff am 20. Januar 2022].

[272] BSI, „Leitfaden IT-Forensik,“ BSI, Bonn, 2011.

[273] T. KAHLER, Massenzugriff der Staatsanwaltschaft auf Kundendaten von Banken zur Ermittlung von Internetstraftaten, 1. Auflage Hrsg., Baden-Baden: Nomos Verlag, 2017.

[274] INNENMINISTERIUM NORDRHEIN-WESTFALEN, „Illegalen Geldern auf der Spur - Polizei investiert halbe Million Euro in Finanzanalyse-Software," 30. Dezember 2020. [Online]. Available: https://www.land.nrw/pressemitteilung/illegalen-geldern-auf-der-spur-polizei-investiert-halbe-million-euro-finanzanalyse. [Zugriff am 2. März 2022].

[275] V. DIAZ, „Kaspersky Security Bulletin: Threat Predictions for 2019," November 2018. [Online]. Available: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/11/27082929/KSB_Predictions-2019_General-APT.pdf. [Zugriff am 2. Februar 2022].

[276] BUNDESAMT FÜR VERFASSUNGSSCHUTZ, „Verfassungsschutzbericht 2020," 15. Juni 2021. [Online]. Available: https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/verfassungsschutzberichte/2021-06-verfassungsschutzbericht-2020-fakten-und-tendenzen-kurzzusammenfassung.html. [Zugriff am 15. Oktober 2021].

[277] PARLAMENTARISCHES KONTROLLGREMIUM (Bundestag), „Parlamentarisches Kontrollgremium (PKGr)," [Online]. Available: https://www.bundestag.de/ausschuesse/weitere_gremien/parlamentarisches_kontrollgremium. [Zugriff am 19. Februar 2022].

[278] G10-KOMMISSION (Bundestag), „G10-Kommission," [Online]. Available: https://www.bundestag.de/webarchiv/Ausschuesse/ausschuesse19/weitere_gremien/g10_kommission/mitglieder-538794. [Zugriff am 19. Februar 2022].

[279] VERTRAUENSGREMIUM (Bundestag), „Vetrauensgremium," [Online]. Available: https://www.bundestag.de/webarchiv/Ausschuesse/ausschuesse19/weitere_gremien/vertrauensgremium#. [Zugriff am 19. Februar 2022].

[280] T. WETZLING, „Aufklärung ohne Aufsicht? Über die Leistungsfähigkeit der Nachrichtendienstkontrolle in Deutschland," Heinrich-Böll-Stiftung, Berlin, 2016.

[281] BUNDESVERFASSUNGSGERICHT (VerfG), „Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17 -. Rn. 1-332," 19. Mai 2020. [Online]. Available: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2020/bvg20-037.html. [Zugriff am 24. Februar 2022].

[282] J. SINGER, Praxiskommentar zum Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes, Berlin, Heidelberg: Springer Verlag, 2016.

[283] S. BIDDLE, „The U.S. Treasury is buying private app data to target and investigate people," 4. November 2021. [Online]. Available: https://theintercept.com/2021/11/04/treasury-surveillance-location-data-babel-street/. [Zugriff am 20. Februar 2022].

[284] K. LYONS, „Congress investigating how data broker sells smartphone tracking info to law enforcement," 25. Juni 2020. [Online]. Available: https://www.theverge.com/2020/6/25/21303190/congress-data-smartphone-tracking-fbi-security-privacy. [Zugriff am 20. Februar 2022].

[285] J. THOMA, „NSA bezahlte RSA Security, um Krypto-Backdoor einzusetzen," 21. Dezember 2013. [Online]. Available: https://www.golem.de/news/bsafe-nsa-zahlte-rsa-security-um-krypto-backdoor-einzusetzen-1312-103540.html. [Zugriff am 18. Februar 2022].

[286] T. PERRIN, „[Cfrg] Requesting removal of CFRG co-chair," 20. Dezember 2013. [Online]. Available: https://mailarchive.ietf.org/arch/msg/cfrg/scLoq7DvtXzo9Jl9AG9fQOcSGsM/. [Zugriff am 18. Februar 2022].

[287] C. COHN und T. TIMM, „The NSA is Making Us All Less Safe," 2. Oktober 2013. [Online]. Available: https://www.eff.org/de/deeplinks/2013/10/nsa-making-us-less-safe. [Zugriff am 18. Februar 2022].

[288] THE NEW YORK TIMES, „Secret Documents Reveal N.S.A. Campaign Against Encryption," 6. September 2013. [Online]. Available: https://archive.nytimes.com/www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?ref=us. [Zugriff am 18. Februar 2022].

[289] J. BUCHMANN, „Sustainable Cybersecurity & Privacy," 17. Juni 2021. [Online]. Available: https://cybersec.kcist.kit.edu/91.php. [Zugriff am 18. Dezember 2021].

[290] J. SCHMIDT, „NSA und GCHQ: Großangriff auf Verschlüsselung im Internet," 6. September 2013. [Online]. Available: https://www.heise.de/security/meldung/NSA-und-GCHQ-Grossangriff-auf-Verschluesselung-im-Internet-1950935.html. [Zugriff am 23. Februar 2022].

[291] A. v. GERNLER und S.-L. GAZDAG, „Post-Quanten-Kryptographie," Firma Genua, 11. Juli 2018. [Online]. Available: https://www.unibw.de/code/events/jt-2018-

innovationstagung/10_gernler_post-quanten-kryptographie.pdf. [Zugriff am 15. Februar 2022].

[292] COMMONCRITERIA (CC) PORTAL, „Certfication Report BSI-DSZ-CC-0782-V2-2015 for Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware) from Infineon Technol," November 2015. [Online]. Available: https://www.commoncriteriaportal.org/files/epfiles/0782V2a_pdf.pdf.

[293] M. NEMEC, M. SYS, P. SVENDA, D. KLINEC und V. MATYAS, „The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli," Oktober 2017. [Online]. Available: https://crocs.fi.muni.cz/public/papers/rsa_ccs17. [Zugriff am 18. Februar 2022].

[294] H. BÖCK, „Infineon erzeugt Millionen unsicherer Krypto-Schlüssel," 18. Oktober 2017. [Online]. Available: https://www.golem.de/news/rsa-sicherheitsluecke-infineon-erzeugt-millionen-unsicherer-krypto-schluessel-1710-130691.html. [Zugriff am 20. Februar 2022].

[295] H. BÖCK, „Unsichere Verschlüsselung - trotz Zertifikat vom Bundesamt," 19. Oktober 2017. [Online]. Available: https://www.zeit.de/digital/datenschutz/2017-10/infineon-verschluesslung-personalausweis-tpm-bsi-zertifiziert/komplettansicht. [Zugriff am 15. Februar 2022].

[296] M. ATMANI, A. FICHTER, S. GRUHNWALD und G. GILBERT-LODGE, „Die mysteriöse Schwesterfirma," 11. November 2020. [Online]. Available: https://www.republik.ch/2020/11/11/die-mysterioese-schwesterfirma. [Zugriff am 10. Februar 2022].

[297] G. GREENWALD, „How covert agents infiltrate the internet to manipulate, deceive, and destroy reputations," 25. Februar 2014. [Online]. Available: https://theintercept.com/2014/02/24/jtrig-manipulation/. [Zugriff am 20. Februar 2022].

[298] U. SCHMIDT, „Das NSA-Handbuch der Verleumdung und Lügen," 25. Februar 2014. [Online]. Available: https://www.welt.de/politik/ausland/article125188439/Das-NSA-Handbuch-der-Verleumdung-und-Luegen.html. [Zugriff am 20. Februar 2022].

[299] SPIEGEL, „Britischer Geheimdienst speichert weltweiten Internet-Verkehr," 21. Juni 2013. [Online]. Available: https://www.spiegel.de/netzwelt/netzpolitik/spionageskandal-britischer-

geheimdienst-sammelt-gewaltige-datenmengen-a-907260.html. [Zugriff am 20. Februar 2022].

[300] J. GOETZ, H. LEYENDECKER und F. OBERMAIER, „Britischer Geheimdienst zapft Daten aus Deutschland ab," 28. August 2013. [Online]. Available: https://www.sueddeutsche.de/politik/internet-ueberwachung-britischer-geheimdienst-zapft-daten-aus-deutschland-ab-1.1757068. [Zugriff am 20. Februar 2022].

[301] UNTERSUCHUNGSAUSSCHUSS (Bundestag), „Untersuchungsausschuss zur NSA-Affäre eingesetzt," 20. März 2014. [Online]. Available: https://www.bundestag.de/webarchiv/textarchiv/2014/50038460_kw12_de_untersuchungsausschuss_nsa-216546. [Zugriff am 20. Februar 2022].

[302] DEUTSCHER BUNDESTAG, „Stenografisches Protokoll der 104. Sitzung. 1. Untersuchungsausschuss Berlin, den 23. Juni 2016, 11.30 Uhr," 23. Juni 2016. [Online]. Available: https://dserver.bundestag.de/btd/18/CD12850/D_I_Stenografische_Protokolle/Protokoll%20104%20I.pdf. [Zugriff am 10. Januar 2022].

[303] F. OELMAIER und F. WIMMER, „NSA Report," Corporate Trust, Januar 2017. [Online]. Available: https://www.corporate-trust.de/wp-content/uploads/2017/02/170123-NSA_ReportfinalDE.pdf. [Zugriff am 10. Februar 2022].

[304] T. SHORROCK, „5 Corporations Now Dominate Our Privatized Intelligence Industry," 8. September 2016. [Online]. Available: https://www.thenation.com/article/archive/five-corporations-now-dominate-our-privatized-intelligence-industry/. [Zugriff am 11. März 2022].

[305] OPENDATACITY, „Stasi versus NSA," [Online]. Available: https://opendatacity.github.io/stasi-vs-nsa/. [Zugriff am 20. Februar 2022].

[306] MAPPR, „European Continent/Map of Europe," [Online]. Available: https://www.mappr.co/thematic-maps/european-continent-map-of-europe/. [Zugriff am 20. Februar 2022].

[307] H. EICHLER, „Innenministerin geht nach Datenleck auf Distanz zur Uniklinik Magdeburg," 5. November 2021. [Online]. Available: https://www.mz.de/mitteldeutschland/sachsen-anhalt/innenministerin-geht-nach-datenleck-auf-distanz-zur-uniklinik-magdeburg-3271879. [Zugriff am 10. Februar 2022].

[308] A. FRÖHLICH, „Datenschutzbeauftragte kritisiert Berliner Polizei," 28. März 2019. [Online]. Available: https://www.tagesspiegel.de/berlin/pannen-

missbrauch-und-lecks-datenschutzbeauftragte-kritisiert-berliner-polizei/24157448.html. [Zugriff am 12. Februar 2022].

[309] M. REUTER, „Mehr als 130 Datenbanken und fast 100.000 personengebundene Hinweise gespeichert," 18. Juli 2020. [Online]. Available: https://netzpolitik.org/2020/berliner-polizei-mehr-als-130-datenbanken-und-fast-100-000-personengebundene-hinweise-gespeichert/. [Zugriff am 19. Februar 2022].

[310] J. WEBER, „Innentäter in Unternehmen," BKA, Wiesbaden, 2017.

[311] M. LAAF, „Wie eine Cyberattacke einen ganzen Landkreis lahmlegt," 12. Juli 2021. [Online]. Available: https://www.zeit.de/digital/datenschutz/2021-07/hackerangriff-anhalt-bitterfeld-cyber-katastrophenfall-kommunen-internetkriminalitaet. [Zugriff am 19. Februar 2022].

[312] L. WURSCHER und H. TANRIVERDI, „Datenleck: Ungelöschte Festplatten auf ebay Kleinanzeigen," 30. Juni 2021. [Online]. Available: https://www.daserste.de/information/wirtschaft-boerse/plusminus/sendung/daten-festplatten-ebay-kleinanzeigen-100.html. [Zugriff am 19. Februar 2022].

[313] M. LORENZ, „Datenschutzskandal bei der Bremer Polizei," 30. Juli 2021. [Online]. Available: https://www.behoerden-spiegel.de/2021/07/30/datenschutzskandal-bei-der-bremer-polizei/. [Zugriff am 17. Februar 2022].

[314] POLIZEI BREMEN, „Datenschutzbeauftragte der Polizei Bremen," [Online]. Available: https://www.polizei.bremen.de/oeffentlichkeitsarbeit/wir-ueber-uns/datenschutzbeauftragter-der-polizei-bremen-7125. [Zugriff am 17. Februar 2022].

[315] M. REUTER, „Schon wieder desaströse Sicherheitslücke in Luca App," 26. Mai 2021. [Online]. Available: https://netzpolitik.org/2021/it-sicherheit-schon-wieder-desastroese-sicherheitsluecke-in-luca-app/. [Zugriff am 25. März 2022].

[316] J. RAAB, „Corona-Chaos bei Ikea: App-Zwang im Möbelhaus - Kunden sauer: „Dann sitz' ich lieber auf Bananenkisten"," 24. September 2021. [Online]. Available: https://www.merkur.de/wirtschaft/ikea-corona-luca-app-pflicht-nachverfolgung-datenschutz-berlin-sicherheit-90461341.html. [Zugriff am 17. März 2022].

[317] H.-J. WOLTER, „„Schon 2023 kann es für die Versorgungssicherheit kritisch werden"," 23. November 2020. [Online]. Available: https://www.aktiv-

online.de/news/schon-2023-kann-es-fuer-die-versorgungssicherheit-kritisch-werden-4541. [Zugriff am 24. Februar 2022].

[318] A. v. (. MASSENBACH, „Konzernmacht beschränken," INKOTA-Netzwerk, Dezember 2018. [Online]. Available: https://www.oxfam.de/system/files/konzernmacht_digitale_welt_final.pdf. [Zugriff am 19. Februar 2022].

[319] M. ROSENBACH, L. POITRAS und H. STARK, „How the NSA Accesses Smartphone Data," 9. September 2013. [Online]. Available: https://www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html. [Zugriff am 22. Februar 2022].

[320] SPIEGEL, „GHCQ: Mobile apps doubleheader: BADASS Angry Birds," [Online]. Available: https://www.spiegel.de/media/716e3462-0001-0014-0000-000000035670/media-35670.pdf. [Zugriff am 18. Februar 2022].

[321] DATAFLURRY, [Online]. Available: https://www.dataflurry.com/. [Zugriff am 2. März 2022].

[322] C. HAN, I. REYES, Á. FEAL, J. REARDON, P. WIJESEKERA, N. VALLINA-RODRIGUEZ, A. ELAZARI, K. A. BAMBERGER und S. EGELMA, „The Price is (Not) Right: Comparing Privacy in Free and Paid Apps," März 2020.

[323] M. EBERL, „Facebook trackt Nutzer auf drei Viertel aller deutschen Nachrichtenseiten," 3. Juni 2019. [Online]. Available: https://rufposten.de/blog/2019/06/03/facebook-tracker-auf-deutschen-medienseiten/. [Zugriff am 24. Februar 2022].

[324] WEBKOLL, [Online]. Available: https://webbkoll.dataskydd.net/de/results?url=http%3A%2F%2Fwww.sueddeutsche.de%2F. [Zugriff am 24. Februar 2022].

[325] R. GUTJAHR, „Wir pfeifen auf Ihre Privatsphäre," 11. Dezember 2020. [Online]. Available: https://www.gutjahr.biz/2020/12/wir-pfeifen-auf-ihre-privatsphaere/. [Zugriff am 22. März 2022].

[326] Gesellschaft für Informatik (GI), „NSA: Back-Doors in 80.000 strategischen Servern weltweit," 23. September 2013. [Online]. Available: https://gi.de/meldung/nsa-back-doors-in-80000-strategischen-servern-weltweit. [Zugriff am 23. Februar 2022].

[327] K. v. HEUVEL und S. F. COHEN, „Edward Snowden: A 'Nation' Interview," 28. Oktober 2014. [Online]. Available:

https://www.thenation.com/article/archive/snowden-exile-exclusive-interview/. [Zugriff am 22. Februar 2022].

[328] T. SHAPIRA und Y. SHAVITT, „FlowPic: Encrypted Internet Traffic Classification is as Easy as Image Recognition," Nr. IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 680-687, 2019.

[329] E. GUO und H. NOORI, „Wie die afghanische Biometrie-Datenbank in die Hände der Taliban gelangte," 8. September 2021. [Online]. Available: https://www.heise.de/hintergrund/Wie-die-afghanische-Biometrie-Datenbank-in-die-Haende-der-Taliban-gelangte-6184168.html. [Zugriff am 15. März 2022].

[330] BSI, „Basistipps zur IT-Sicherheit," [Online]. Available: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/cyber-sicherheitsempfehlungen_node.html. [Zugriff am 5. März 2022].

[331] FACEBOOK, „Keeping Passwords Secure," 21. März 2019. [Online]. Available: https://about.fb.com/news/2019/03/keeping-passwords-secure/. [Zugriff am 22. März 2022].

[332] M. SCHALLBRUCH, Schwacher Staat im Netz, Wiesbaden: Springer, 2018.

[333] L. POITRAS, J. APPELBAUM, M. ERMERT, C. GROTHOFF, J. KIRSCH und H. MOLTKE, „NSA/GCHQ: Das HACIENDA-Programm zur Kolonisierung des Internet," 15. August 2014. [Online]. Available: https://www.heise.de/ct/artikel/NSA-GCHQ-Das-HACIENDA-Programm-zur-Kolonisierung-des-Internet-2292574.html?hg=1&hgi=0&hgf=false. [Zugriff am 11. März 2022].

[334] SZ, „NSA soll deutsche Tor-Nutzer ausspioniert haben," 3. Juli 2014. [Online]. Available: https://www.sueddeutsche.de/digital/internet-ueberwachung-nsa-soll-deutschen-tor-nutzer-ausspioniert-haben-1.2029100?. [Zugriff am 11. März 2022].

[335] J. APPELBAUM, A. GIBSON, C. GUARNIERI, A. MÜLLER-MAGUHN, L. POITRAS, M. ROSENBACH, L. RYGE, H. SCHMUNDT und M. SONTHEIMER, „Die NSA rüstet zum Cyber-Feldzug," 18. Januar 2015. [Online]. Available: https://www.spiegel.de/netzwelt/netzpolitik/snowden-dokumente-wie-die-nsa-digitale-kriege-vorbereitet-a-1013521.html. [Zugriff am 5. März 2022].

[336] H. G. v. MOLTKE, „Zur Sicherheit softwarebasierter Produkte," Bitkom, Berlin, 2020.

[337] N. WEAVER, „Extra Unofficial XKEYSCORE Guide: Jihobbiests, Mojahaden Secrets, and PGP," 5. Juli 2015. [Online]. Available: https://medium.com/@nweaver/extra-unofficial-xkeyscore-guide-b8513600ad24#.q43xlla2m. [Zugriff am 24. Februar 2022].

[338] K. YAMAMOTO, „Pgpdump," Februar 2022. [Online]. Available: http://www.mew.org/~kazu/proj/pgpdump/en/. [Zugriff am 25. März 2022].

[339] FRAUNHOFER SIT, „Forensische Textanalyse mit NLP und Machine Learning," [Online]. Available: https://www.cybersicherheit.fraunhofer.de/content/dam/zv/cybersicherheit-zv/documents/brosch%C3%BCren/einzelbrosch%C3%BCren/it-forensik/Forensische%20Textanalyse%20mit%20NLP%20und%20machine%20Learning_V1.pdf. [Zugriff am 24. Februar 2022].

[340] C. WINTER, V. BATTIS und O. HALVANI, „Herausforderungen für die Anonymisierung von Daten," November 2019.

[341] H. JÄGER und R. RIEKEN, „Die Sealed-Cloud-Versiegelung - Verschlüsselung allein genügt für sicheres Cloud Computing nicht," 14. Februar 2014. [Online]. Available: https://www.idgard.de/pdf/Die-Sealed-Cloud-Versiegelung.pdf. [Zugriff am 24. Februar 2022].

[342] A. WEIGEND, Data for the people, Hamburg: Murmann Publishers GmbH, 2017.

[343] BSI, „IT-Sicherheit auf dem digitalen Verbrauchermarkt: Fokus Gesundheits-Apps," BSI, 17. Mai 2021. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/gesundheitsapps.pdf;jsessionid=F5193CCD996945663FB4817469FF2D8C.internet462?__blob=publicationFile&v=2#download=1. [Zugriff am 12. Februar 2022].

[344] PRIVACY INTERNATIONAL (PI), „No Body's Business But Mine: How Menstruation Apps Are Sharing Your Data," 7. Oktober 2020. [Online]. Available: https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data. [Zugriff am 13. Februar 2022].

[345] A. ACQUISTI, L. BRANDIMARTE und G. LOEWENSTEIN, „Privacy and human behavior in the age of information," Januar 2015.

[346] A. G. REECE und C. M. DANFORTH, „Instagram photos reveal predictive markers of depression," August 2016.

[347] W. CHRISTL, „Digitale Überwachung und Kontrolle am Arbeitsplatz," Cracked Labs, Wien, 2021.

[348] M. SPITZER, Cyberkrank! - Wie das digitalisierte Leben unsere Gesundheit ruiniert, Droemer Verlag, 2015.

[349] M. SCHNEIDER, M. ENZMANN und M. STOPCZYNSKI, „Web-Tracking-Report 2014," Fraunhofer-Institut fur Sichere Informationstechnologie SIT, Darmstadt, 2014.

[350] S. HEUER, „Immer im Visier," 16. Juli 2009. [Online]. Available: https://www.heise.de/hintergrund/Immer-im-Visier-276659.html. [Zugriff am 24. Februar 2022].

[351] K. NEß, „Smartphones," [Online]. Available: https://www.privacy-handbuch.de/handbuch_70.htm. [Zugriff am 24. Februar 2022].

[352] SPIEGEL, „Uber analysiert One-Night-Stands seiner Nutzer," 8. Januar 2015. [Online]. Available: https://www.spiegel.de/netzwelt/apps/uber-trackt-offenbar-one-night-stands-seiner-nutzer-a-1011770.html. [Zugriff am 13. Februar 2022].

[353] D. SÜRIG, „"Mark Zuckerberg könnte einiges von Europa lernen"," 12. April 2018. [Online]. Available: https://www.sueddeutsche.de/digital/physiker-andreas-weigend-mark-zuckerberg-koennte-einiges-von-europa-lernen-1.3940967. [Zugriff am 13. Februar 2022].

[354] EXODUS, „Exodus Test App N26," [Online]. Available: https://reports.exodus-privacy.eu.org/de/reports/de.number26.android/latest/. [Zugriff am 24. Februar 2022].

[355] J. KRIEGER-LAMINA, „Privatsphäre in Online-Spielen," Österreichische Akademie der Wissenschaften, Wien, 2017.

[356] S. BIDDLE, „Feds Seized Chicago Man's Computers in Celeb Nude Leak Investigation," 6. September 2015. [Online]. Available: https://www.gawker.com/feds-seized-chicago-mans-computers-in-celeb-nude-leak-i-1709153721. [Zugriff am 24. Februar 2022].

[357] M. BERGEN und J. SURANE, „Google and Mastercard Cut a Secret Ad Deal to Track Retail Sales," 30. August 2018. [Online]. Available: https://www.bloomberg.com/news/articles/2018-08-30/google-and-

mastercard-cut-a-secret-ad-deal-to-track-retail-sales. [Zugriff am 24. Februar 2022].

[358] S. MARE, F. ROESNER und T. KOHNO, „Smart Devices in Airbnbs: Considering Privacy and Security for both Guests and Hosts," August 2019.

[359] M. CELKO, „Hyperlocality: Die Neuschöpfung der Wirklichkeit," GDI Impuls.2008.

[360] M. (. d. S. A. BRNOVICH, „The Superior Court of the State of Arizona in and for the County of Maricopa - Plaintiff State of Arizona ex rel. Mark Brnovich, Attorney General, for its Complaint against Defendant Google LLC ("Google")," 27. Mai 2020. [Online]. Available: https://www.azag.gov/sites/default/files/2021-05/Complaint%20%28redacted%29.pdf. [Zugriff am 17. Februar 2022].

[361] B. SCHNEIER, „NSA Surveillance: a Guide to Staying Secure," 6. September 2013. [Online]. Available: https://www.schneier.com/essays/archives/2013/09/nsa_surveillance_a_g.html. [Zugriff am 22. Februar 2022].

[362] I. FOUAD, N. BIELOVA, A. LEGOUT und N. SARAFIJANO-DJUKIC, „Missed by Filter Lists: Detecting Unknown Third-Party Trackers with Invisible Pixels," Februar 2020.

[363] WIKIPEDIA, „TR-069," Dezember 2021. [Online]. Available: https://de.wikipedia.org/wiki/TR-069. [Zugriff am 25. März 2022].

[364] K. SOLOMOS, J. KRISTOFF, C. KANICH und J. POLAKIS, „Tales of Favicons and Caches: Persistent Tracking in Modern Browsers," Februar 2021.

[365] B. SCHNEIER, „NSA surveillance: A guide to staying secure," 6. September 2013. [Online]. Available: https://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance. [Zugriff am 23. Februar 2022].

[366] S. KREMPL, „Massive Online-Überwachung: Google ist "am besten", Apple "phänomenal"," 27. Februar 2022. [Online]. Available: https://www.heise.de/news/Massive-Online-Ueberwachung-Google-ist-am-besten-Apple-phaenomenal-6527237.html. [Zugriff am 16. März 2022].

[367] B. SCHWAN, „Apple plant iPhone-Scanning auf Kinderpornos - Sicherheitsforscher alarmiert," 6. August 2021. [Online]. Available: https://www.heise.de/news/Apple-plant-iPhone-Scanning-auf-Kinderpornos-Sicherheitsforscher-alarmiert-6156542.html. [Zugriff am 2. Februar 2022].

[368] BSI, „Sichere Technik, auch auf Reisen,“ [Online]. Available: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/IT-Sicherheit-auf-Reisen/it-sicherheit-auf-reisen_node.html. [Zugriff am 25 März 2022].

[369] B. N. R. (. SCHOLZ, DiDat Weißbuch Verantwortungsvoller Umgang mit digitalen Daten - Orientierungen eines transdisziplinären Prozesses, Baden-Baden: Nomos Verlagsgesellschaft mbh & Co. KG, 2021.

[370] R. MASOOD, B. Z. H. ZHAO, H. J. ASGHAR und M. A. KAAFAR, „Touch and You’re Trapp(ck)ed: Quantifying the Uniqueness of Touch Gestures for Tracking,“ Dezember 2017.

[371] S. FISCHER, „Obama und das Handy der Kanzlerin,“ 24. Oktober 2013. [Online]. Available: https://www.spiegel.de/politik/deutschland/obama-und-das-handy-der-kanzlerin-usa-unter-spaeh-verdacht-a-929656.html. [Zugriff am 17. Februar 2022].

[372] SPIEGEL, „Dänemark half offenbar der NSA beim Bespitzeln von EU-Politikern,“ 30. Mai 2021. [Online]. Available: https://www.spiegel.de/ausland/daenemark-half-offenbar-der-nsa-beim-bespitzeln-von-eu-politikern-a-8d77d428-cb7b-4414-b9f4-952e56706e88. [Zugriff am 17. Februar 2022].

[373] A. ROßNAGEL, M. FRIEDEWALD und M. (. HANSEN, Die Fortentwicklung des Datenschutzes, Wiesbaden: Springer Vieweg, 2018.

[374] HUMAN RIGHTS COMMITTEE (UN), „Concluding observations on the seventh periodic report of Germany,“ 11. November 2021. [Online]. Available: https://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/DEU/CCPR_C_DEU_CO_7_47161_E.pdf. [Zugriff am 6. Februar 2022].

[375] C. CIMPANU, „A mysterious threat actor is running hundreds of malicious Tor relays,“ 3. Dezember 2021. [Online]. Available: https://therecord.media/a-mysterious-threat-actor-is-running-hundreds-of-malicious-tor-relays/. [Zugriff am 13. Februar 2022].

[376] S. STIRNIMANN, Der Mensch als Risikofaktor bei Wirtschaftskriminalität, Wiesbaden: Springer Fachmedien, 2021.

[377] I. DACHWITZ, T. RUDL und S. REBIGER, „Was wir über den Skandal um Facebook und Cambridge Analytica wissen [UPDATE],“ 21. März 2018. [Online]. Available: https://netzpolitik.org/2018/cambridge-analytica-was-

wir-ueber-das-groesste-datenleck-in-der-geschichte-von-facebook-wissen/. [Zugriff am 19. März 2022].

[378] L. FRANCESCHI-BICCIERAI, „Company That Routes Billions of Text Messages Quietly Says It Was Hacked," 4. Oktober 2021. [Online]. Available: https://www.vice.com/en/article/z3xpm8/company-that-routes-billions-of-text-messages-quietly-says-it-was-hacked. [Zugriff am 26. Februar 2022].

[379] Prof. H. Federrath, Interview, *Befragung per E-Mail.* [Interview]. 6. Februar 2022.

[380] R. WEIS, S. LUCKS und V. GRASSMUCK, „Technologien für und wider Digitale Souveränität," Sachverständigenrat für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz , Berlin, 2017.

[381] EUROPEAN PARLIAMENTARY RESEARCH SERVICE, SCIENCE AND TECHNOLOGY OPTIONS ASSESSMENT, „Mass Surveillance - Part 1 - Risks and opportunities raised by the current generation of network services and applications," Directorate-General for Parliamentary Research Services, European Parliament, Brüssel, 2014.

[382] P. BERLINQUETTE, „How Google Tracks Your Personal Information," 4 Dezember 2018. [Online]. Available: https://medium.com/s/story/the-complete-unauthorized-checklist-of-how-google-tracks-you-3c3abc10781d. [Zugriff am 2 März 2022].

[383] BUNDESVERBAND IT-SICHERHEIT e.V. (TeleTrusT), „TeleTrusT unterstützt Initiative gegen Mitwirkungspflicht für Kommunikationsdienste bei staatlicher Überwachung und Schwächung von Verschlüsselung," 14 Mai 2021. [Online]. Available: https://www.teletrust.de/uploads/media/210514-Gemeinsamer_Brief_BVerfSchG_-_Artikel_10-G.pdf. [Zugriff am 29 September 2021].

[384] S. KREMPL, „Bundestag: Auch Zollfahnder dürfen künftig den Bundestrojaner einsetzen," 20 Dezember 2019. [Online]. Available: https://www.heise.de/newsticker/meldung/Bundestag-Auch-Zollfahnder-duerfen-kuenftig-den-Bundestrojaner-einsetzen-4620790.html. [Zugriff am 25 September 2021].

[385] BUNDESVERFASSUNGSGERICHT (VerfG), „Erweiterte Datennutzung („Data-mining") nach dem Antiterrordateigesetz teilweise verfassungswidrig," 11 Dezember 2020. [Online]. Available: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2020/bvg20-104.html. [Zugriff am 8 Oktober 2021].

[386] BUNDESREGIERUNG, „Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. - Drucksache 19/26018 -," 2 Februar 2021. [Online]. Available: https://dserver.bundestag.de/btd/19/263/1926367.pdf.

[387] ECO – VERBAND DER INTERWIRTSCHAFT e.V., „Stellungnahme zum Referentenentwurf eines Gesetzes zur Bekämpfung des Rechtextremismus und der Hasskriminalität," 17 Januar 2020. [Online]. Available: https://bmjv.de/SharedDocs/Gesetzgebungsverfahren/Stellungnahmen/2020/Downloads/011720_Stellungnahme_eco_RefE__Belaempfung-Rechtsextremismus-Hasskriminalitaet.pdf. [Zugriff am 25 September 2021].

[388] o.V., „Heartbleed," [Online]. Available: https://heartbleed.com/. [Zugriff am 17. Dezember 2021].

[389] ISO, „Extranet," [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27033:-1:ed-2:v1:en:term:3.10. [Zugriff am 22. März 2022].

[390] D. BERNHARD, R. SYMANZIK und M. WASSEREK, „Internetökonomie als Ökonomie der Aufmerksamkeit," Weimar, 2010.

[391] A. MOSER-KNIERIEM, Vorratsdatenspeicherung Zwischen Überwachungsstaat und Terrorabwehr, Wiesbaden: Springer Vieweg, 2014, p. S. 268.

Bilderverzeichnis

Tabellenverzeichnis

Anhang

A Folgende Daten besitzt Google, nach denen getrackt wird: (Zu Kapitel 3.3.3)

„Ihr Alter

Ihr Einkommen

Ihr Geschlecht

Ihr elterlicher Status

Ihr Beziehungsstatus

Ihr Surfverhalten (langfristig und kurzfristig)

Ihr Gerät (Telefon, Tablet, Desktop, TV)

Ihr physischer Standort

Das Alter Ihres Kindes (Kleinkind, Säugling, etc.)

Wie gut Sie in der High School waren

Welchen Abschluss Sie haben

Die (Tages-)Zeit Ihrer Google-Nutzung

Die Sprache, die Sie sprechen

Ob Sie gerade ein wichtiges Lebensereignis hinter sich haben

Ihr Status als Hausbesitzer

Ihr Mobilfunkanbieter

Die genauen Wörter, die Sie in die Google-Suche eingeben

Den Kontext und die Themen der Websites, die Sie besuchen

Die Produkte, die Sie kaufen

Die Produkte, die Sie fast gekauft haben

Ihre Wi-Fi-Geräteart

Ihre Nähe zu einem Mobilfunkmast

Ihre App-Installationshistorie

Die Zeit, die Sie mit bestimmten Apps verbringen

Ihr Betriebssystem

Der Inhalt Ihrer E-Mails

Die Zeit, die Sie auf bestimmten Websites verbringen

Ob Sie umziehen (z. B. in eine neue Wohnung)

Ob Sie sich bewegen (z. B. zu Fuß oder im Zug)“ [382]

B Bild: Übersicht über Machine Learning (ML), KI und Daten Landschaft 2021

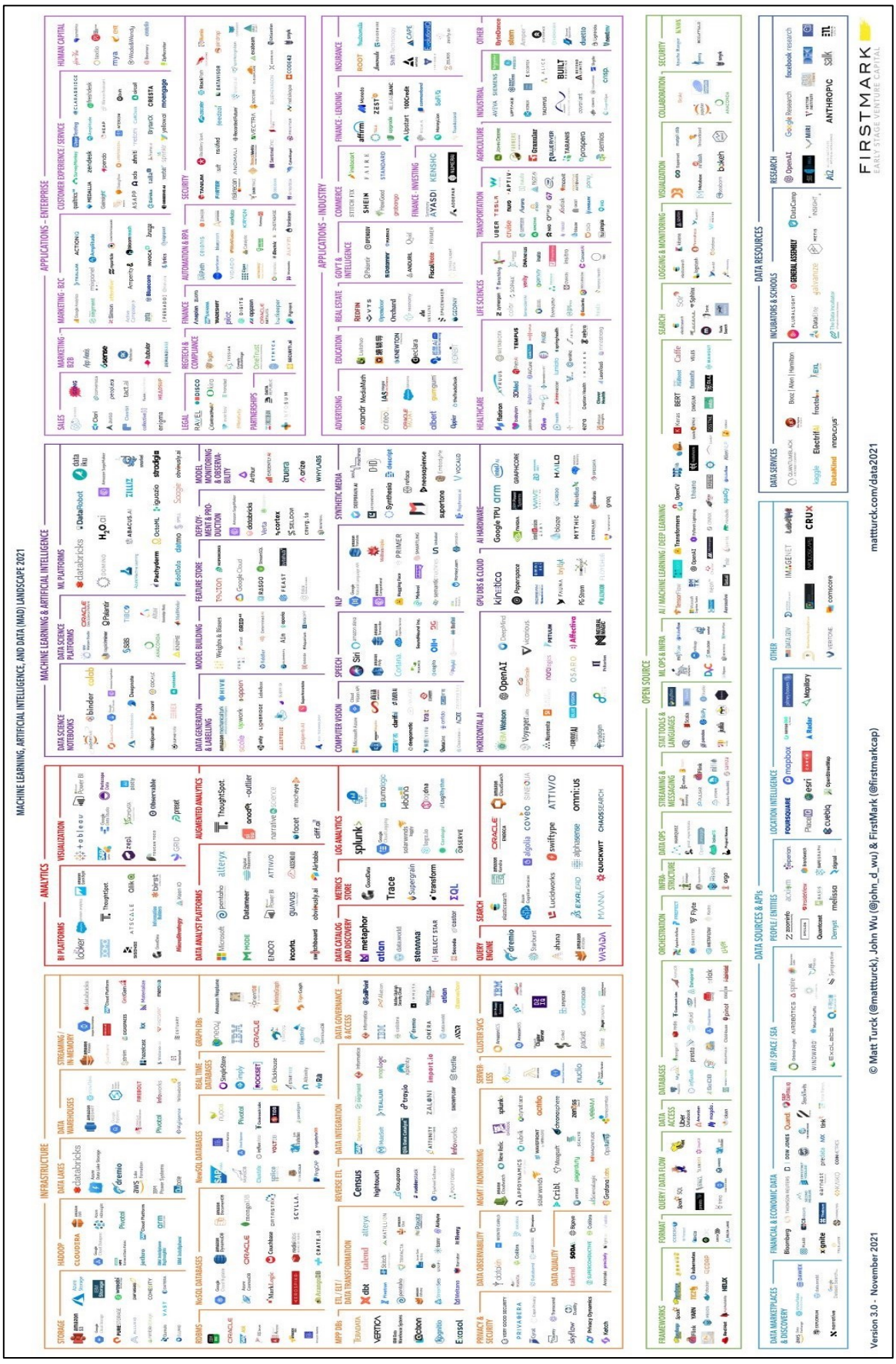


Bild 12: Übersicht über Machine Learning (ML), KI und Daten Landschaft 2021 [83]

C Bild: Übersicht über alle Mobilitätsdaten

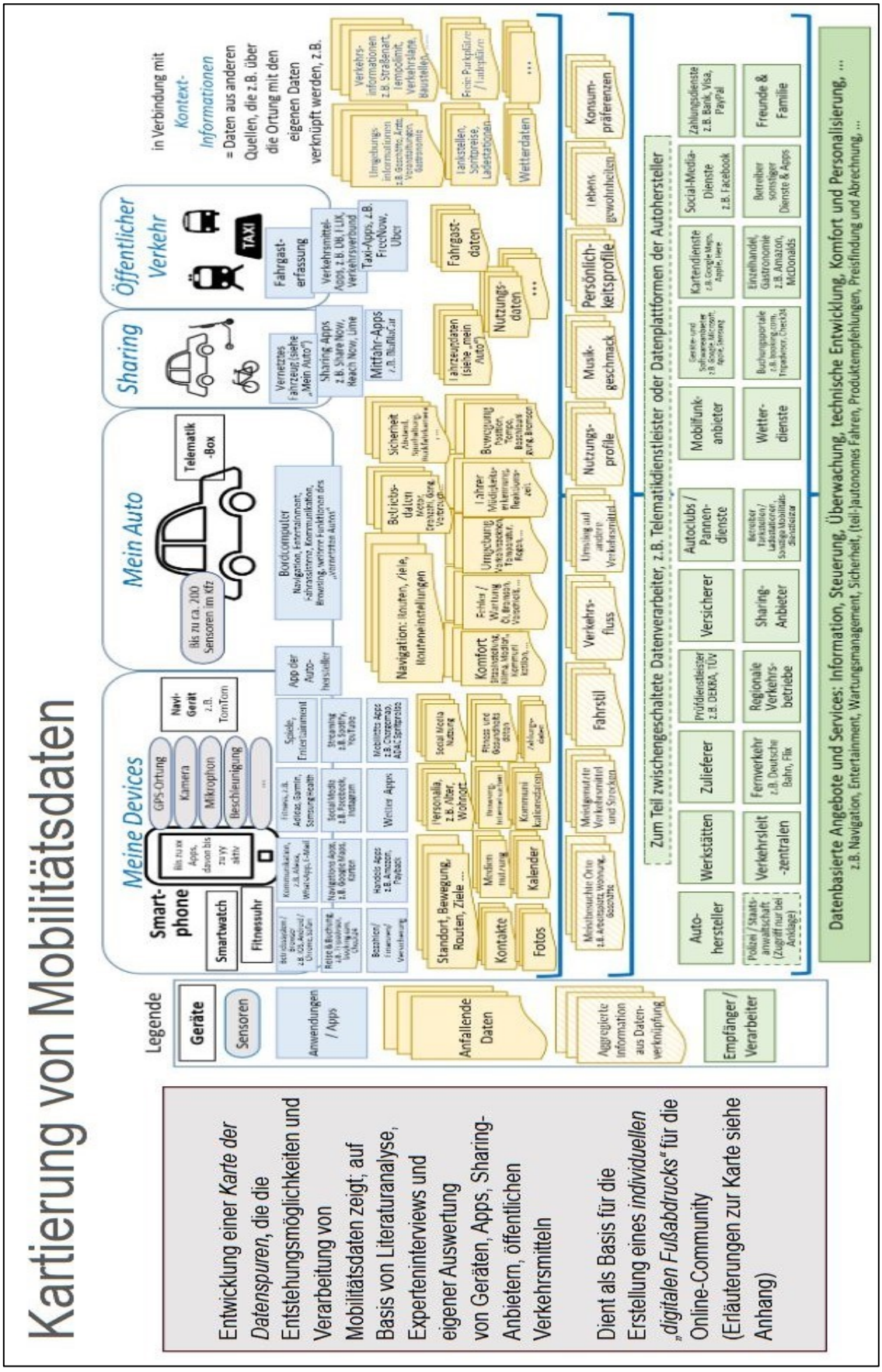


Bild 13: Übersicht aller Mobilitätsdaten [117, p. Folie 24]

D Gesetze

Gesetz über den Bundesnachrichtendienst (BND-Gesetz - BNDG)

Folgende Gesetze des BND-Gesetz BNDG schränken ein:

§§ 6, 7, 8, 9, 12, 13, 14 BNDG.

Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz - G 10)

Folgende Gesetze des Artikels 10- Gesetz G 10 schränken ein:

§§ 2, 3a, 3b, 4, 5, 5a, 6, 7, 7a, 9, 10, 11, 12, 13, 15, 15a, 16 Gesetz G 10.

Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz - BVerfSchG)

Folgende Gesetze des BVerfSchG schränken ein:

§§ 1, 2, 3, 4, 5, 6, 7, 8, 8a, 8b, 8d, 9, 9a , 9b, 10 – 19, 21-27 BVerfSchG.

Eine übergreifende Allianz aus zivilgesellschaftlichen Organisationen und Unternehmen hat sich gegen „eine unbegrenzte Ausweitung von Überwachung und für den Schutz von Verschlüsselung“ [383] bei der „Anpassung des Verfassungsschutzrechts“ ausgesprochen s. [383]. Denn die „geplante Ausweitung der Quellen-Telekommunikationsüberwachung und die damit verbundene Verpflichtung für Anbieter von Kommunikationsdiensten, bei der Überwachung mitzuwirken und im schlimmsten Fall die eigenen Nutzer zu hacken, gefährdet die Cybersicherheit aller Bürger, Unternehmen und der Zivilgesellschaft.“ [383, p. 1]. Verstärkt wird diese Aussage damit, „Wenn gerade Deutschland eines der schärfsten und invasivsten Überwachungsgesetze … verabschiedet, würde dies auch ein fatales Signal an autoritäre Regime weltweit senden.“ [383, p. 1]. Daher wird die Forderung aufgestellt, keine weiteren Maßnahmen dahingehend zu treffen, „die eine Schwächung oder das Brechen von Verschlüsselung zur Folge hätten.“ [383, p. 2], sondern im Gegenteil die Verschlüsselung „mittel- und langfristig zu stärken“ [383, p. 2], da „[d]as Vertrauen in die Integrität von digitaler Kommunikation […] der Grundpfeiler der erfolgreichen Digitalisierung unserer Gesellschaft“ [383, p. 2] ist.

Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (Kontrollgremiumgesetz - PKGrG)

Folgende Gesetze des PKGrG schränken ein:

§§ 1 – 14 PKGrG.

Bundeskriminalamtgesetz (BKAG)

Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz - BKAG)

Folgende Gesetze des BKAG schränken ein:

§§ 1 – 5, 9 – 33, 36 – 53, 55 – 66a, 69, 74 – 85 BKAG.

Gesetz über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681* (Fluggastdatengesetz - FlugDaG)

Folgende Gesetze des FlugDaG schränken ein:

§§ 1 – 10 FlugDaG.

Gesetz über das Zollkriminalamt und die Zollfahndungsämter (Zollfahndungsdienstgesetz - ZFdG)

Folgende Gesetze des ZFdG schränken ein:

§§ 1, 3, 8 - 12, 15, 18, 21, 26, 29, 30-32, 36, 41, 43, 45 47, 49, 53, 59 – 60, 62, 65, 72-73, 75, 77, 79, 90, 92-93, 98-99, 104 ZFdG.

Die Zollfahndungsämter können bereits bei Verdachtsfällen mit Hilfe von § 72 ZFdG „heimlich „dem Brief- oder Postgeheimnis unterliegenden Sendungen öffnen und einsehen sowie die dem Fernmeldegeheimnis unterliegende Telekommunikation überwachen und aufzeichnen." [384], was bedeutet, dass hier der Staatstrojaner eingesetzt werden kann. Der Bundesdatenschutzbeauftragte Prof. Dr. Ulrich Kelber hat „erhebliche verfassungsrechtliche Bedenken gegen die Bestandsdatenauskunft vorgebracht." [384], da „[d]as Zollkriminalamt … künftig auch ohne Wissen der Betroffenen Bestands-, Verbindungs-, Standort- und Nutzungsdaten bei Telekommunikationsanbietern abfragen" [384], einschließlich „auch auf PINS und vergleichbare Kennungen" [384].

Gesetz über die Bundespolizei (Bundespolizeigesetz - BPolG)

Folgende Gesetze des BPolG schränken ein:

§§ 21, 22a, 28, 28a, 29, 31a, 32, 36 BPolG.

Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz - ATDG)

Folgende Gesetze der ATDG schränken ein:

§§ 1 - 13 ATDG.

Das Bundesverfassungsgericht hat am 10.11.2021 den „§ 6a Abs. 2 Satz 1 des Gesetzes zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz - ATDG) für mit Art.

2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG unvereinbar und damit nichtig erklärt.“ [385].

Das Bundesverfassungsgericht beanstandete vor allem die „erweiterte[n] Nutzung („Data-mining“) von in der Antiterrordatei gespeicherten Datenarten, und zwar - über die Informationsanbahnung hinaus - auch zur operativen Aufgabenwahrnehmung. § 6a ATDG gestattet damit die unmittelbare Nutzung der Antiterrordatei auch zur Generierung neuer Erkenntnisse aus den Querverbindungen der gespeicherten Datensätze.“ [385].

In der Antiterrordatei sind mit Stand vom Juni insgesamt 9.523 Personen gespeichert, wovon mehrheitlich die Daten vom Bund stammen (hier: 6.197 Personen) s. [386, p. 3]. Darüber hinaus hat die Bundesregierung mit Blick auf das o.g. Verfassungsurteil erklärt, dass „[d]ie in § 6a ATDG beschriebenen Auswerte- und Analysemöglichkeiten konnten bislang technisch aufgrund des veralteten Softwarekerns der ATD, fehlender Auswertetools sowie ihrer aktuellen Datenstruktur nicht umgesetzt werden.“ [386, p. 4]. Hier ist an dieser Stelle zu fragen, warum dann ein Bedarf bestand, wenn es bislang nicht genutzt wurde.

Abgabenordnung (AO)

Folgende Gesetze der AO schränken ein:

§§ 29b, 29c, 30, 31b, 32a, 72a, 80a, 87a-d, 88a-c, 89-90, 92-93d, 117a, 122a, 138b, 139a-b, 146a, 149-150, 154, 200, 208, 211, 397, 413 AO.

Kreditwesengesetz (KWG)

§ 24c KWG.

Bundesmeldegesetz (BMG)

Folgende Gesetze des BMG schränken ein:

§§ 17, 34 BMG.

Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz - PAuswG)

Folgende Gesetze des PAuswG schränken ein:

§§ 1, 5, 12, 18, 23, 25-36 PAuswG.

Die oben genannten Gesetze gelten auch 1:1 für das **Paßgesetz (PaßG)**.

Straßenverkehrsgesetz (StVG)

Folgende Gesetze der StVG schränken ein:

§§ 1g, 35-36, 36b, 48 StVG.

Netzwerkdurchsetzungsgesetz (NetzDG)

§§ 1-6 NetzDG.

Der Eco - Verband der Internetwirtschaft e.V. ist der Ansicht, dass das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität „zum Teil mit tiefen Einschnitten in das informationelle Selbstbestimmungsrecht gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz (GG), in das Recht auf Gewährleistung der Vertraulichkeit und Integrität von Kommunikationssystemen nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG sowie in das Fernmeldegeheimnis gem. Art. 10 GG für die Bürgerinnen und Bürger einher[geht]“ [387, p. 1]. Begründet wird dies neben einer Meldepflicht für die Betreiber sozialer Netzwerke damit, dass „rechtliche Grundlagen für die Datenerhebung sowie Weitergabe im Telemediengesetz und Herausgabepflichten, u.a. zu Nutzerpasswörtern, für die Betreiber von Telemediendiensten geschaffen werden“ [387, p. 1] sollen s. [387, p. 1]. Als Fazit werden „erhebliche datenschutzrechtliche, verfassungsrechtliche und europarechtliche Fragen“ [387, p. 1] aufgeworfen. Bei der Herausgabe von Passwörtern wird eingewendet, dass in der Mehrzahl die „Passwörter serverseitig verschlüsselt gespeichert werden und damit in der praktischen Verwendung ohne Ermittlungswert sind, ist ein derartiger Eingriff in die digitale Privatsphäre der Nutzerinnen und Nutzer unter Berücksichtigung von Verhältnismäßigkeit und technischer Umsetzbarkeit in höchstem Maß bedenklich“ [387, p. 2].

Landesrecht, hier das Allgemeines Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung in Berlin (Allgemeines Sicherheits- und Ordnungsgesetz - ASOG Bln)

Allgemeines Sicherheits- und Ordnungsgesetz - ASOG Berlin in der Fassung vom 11. Oktober 2006

Folgende Gesetze der ASOG Bln schränken ein:

§ 25a-b, 42-43,46-49 ASOG Bln.

Verzeichnis der Abkürzungen

2FA	Zwei-Faktor-Authentisierung
3GPP	Third Generation Partnership Project
ADM	Automated Decision Making
AES	Advanced Encryption Standard
AGB	Allgemeinen Geschäftsbedingungen
ANT	Advanced Network Technology
API	Programmierschnittstelle
APT	Advanced Persistent Threats
AR	Augmented-Reality
AWS	Amazon Web Services
beA	Besonderes elektronisches Anwaltspostfach
BfDI	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BfV	Bundesamt für Verfassungsschutz
BIOS	Basic Input Output System
BKA	Bundeskriminalamt
BMI	Bundesministerium des Innern
BND	Bundesnachrichtendienst
BSI	Bundesamt für Sicherheit in der Informationstechnik
BNetzA	Bundesnetzagentur
BVerfG	Bundesverfassungsgericht
BVerwG	Bundesverwaltungsgericht
Can-Bus	Controller Area Network
CC	Common Criteria
CCC	Computer Chaos Club
CDR	Call Data Records
CIA	Central Intelligence Agency
CNIL	Commission Nationale de l'Informatique et des Libertés

CSRF	Cross-Site-Request-Forgery
CPU	Central Processing Unit
C’T	Magazin für Computer Technik
CWE	Common Weakness Enumeration
DDR	Deutsche Demokratische Republik
DECT	Digital Enhanced Cordless Telecommunications
DMA	Direct Memory Access
DoS	Denial of Service
DDoS	Distributed Denial of Service
DMZ	Demilitarisierte Zone
DNS	Domain Name Service
DSGVO	Datenschutz-Grundverordnung der Europäischen Union
DUD	Datenschutz und Datensicherheit
EDR	Endpoint Detection Respond
EDSA	Europäische Datenschutzausschuss
EFF	Electronic Frontier Foundation
EKG	Elektrokardiogramm
ENISA	Agentur der Europäischen Union für Cybersicherheit
ETSI	European Telecommunications Standards Institute
EU	Europäische Union
EXE	Executable
FAZ	Frankfurter Allgemeine Zeitung
FIPS	Federal Information Processing Standard
FISA	Foreign Intelligence Surveillance Act
FKIE	Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie
FOMO	Fear Of Missing Out
SIT	Fraunhofer-Institut für Sichere Informationstechnologie
GHCQ	Government Communications Headquarters

GG	Grundgesetz
GI	Gesellschaft für Informatik
GPS	Globales Positionsbestimmungssystem
HID	Human Interface Devices
HPI	Hasso-Plattner-Institut
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IKT	Informations- und Kommunikationstechnik
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IT	Informationstechnik
ISO	Internationale Organisation für Normung
LAN	Local Area Network
LED	Leuchtdiode
KI	Künstliche Intelligenz
LI	Lawful Interception
LTE	Long Term Evolution
M2M	Machine-to-Machine
MA	Mitarbeiter
ME	Management Engine (Intel)
MI5	Military Intelligence, Section 5
MAD	Militärischer Abschirmdienst
MIC	Machine Identification Code
NAS	Network Attached Storage
NFC	Near Field Communication
NGO	Nichtregierungsorganisation
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OBFCM	On-Board Fuel Consumption Meter

OEM	Originalgerätehersteller
OSS	Open Source Software
PACS	Picture Archiving and Communication Systems
PDF	Portable Document Format
PI	Privacy International
PIN	Persönliche Identifikationsnummer
PKGr	Parlamentarische Kontrollgremium
PKI	Public-Key-Infrastruktur
PGP	Pretty Good Privacy
RDP	Remote Desktop Protocol
RegMoG	Registermodernisierungsgesetz
RNG	Zufallszahlengenerator
ROC	Remote Operation Center
RSA	Rivest-Shamir-Adleman
TLS	Transport Layer Security
SANS	SysAdmin, Audit, Networking and Security
SMU	System Management Unit (AMD)
SQL	Structured Query Language
SSL	Secure Sockets Layer
StPO	Strafprozessordnung
SWIFT	Society for Worldwide Interbank Financial Telecommunication
SWP	Stiftung Wissenschaft und Politik
SZ	Süddeutschen Zeitung
TAO	Tailored Access Operations
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung
TMG	Telemediengesetz
TPM	Trusted Platform Module
TR	Technische Richtlinie

TSMC	Taiwan Semiconductor Manufacturing Company Limited
TÜV	Technischer Überwachungsverein
UEFI	Unified Extensible Firmware Interface
UN	United Nations
V.i.S.d.P.	Verantwortlich im Sinne des Presserechts
VoIP	Voice over IP
VP	Vizepräsident
VPN	Virtual Private Network
WLAN	Wireless Local Network Area
WTO	World Trade Organization
XSS	Cross-Site-Scripting

Thesen

Thema: „Ist ganzheitliche Informationssicherheit für Bürger in Deutschland möglich?“

- Der Begriff „ganzheitliche Informationssicherheit“ wurde um die Anforderungen des privacy by design sowie privacy by default aus dem Datenschutzbereich erweitert und vergrößert somit die bisherige Methodik um weitere Aspekte.
- Durch die zunehmende Digitalisierung in immer mehr Lebensbereichen wird zugleich die Abhängigkeit und damit die Vulnerabilität für die Gesellschaft insgesamt erhöht.
- Eine gesellschaftliche Teilhabe ohne Einsatz von IT-Systemen ist daher aufwändiger geworden, so dass sich der Handlungsspielraum des Bürgers zunehmend verkleinert.
- Die gegenwärtigen IT-Systeme beinhalten i.d.R. Schwachstellen in Hard- und Software einschließlich der Betriebssysteme, woraus zukünftig die Anforderung vor Inbetriebnahme erfüllt sein muss, von Anfang an die ganzheitlichen Informationssicherheitsanforderungen wie security by design, privacy by design sowie privacy by default umzusetzen, was anschließend von einer unabhängigen Stelle geprüft wird.
- Eine erhebliche Gefährdung geht durch den zunehmenden Einsatz von Big-Data-Mechanismen aus, in der es u.a. durch die Forschung im Persönlichkeitsbereich möglich ist, tiefgreifende Erkenntnisse bei den Persönlichkeitsmerkmalen der Bürger zu gelangen, was negative Konsequenzen nach sich ziehen kann und zukünftig zusätzlich sich durch den Einsatz von KI verschärfen wird.
- Eine ganzheitliche Informationssicherheit für Bürger ist kurz- bis mittelfristig mit einem hohen Aufwand möglich, sofern die IT-Systeme in dessen ausschließlicher Verfügungsgewalt stehen.
- Die gegenwärtigen Rahmenbedingungen erschweren die Möglichkeit, dauerhaft eine ganzheitliche Informationssicherheit durch den Bürger zu praktizieren, da u.a. auf der einen Seite mit der zunehmenden Anzahl von IT-Systemen die Aufwände für die Schutzmaßnahmen sich erhöhen und auf der anderen Seite durch die Internetnutzung zusätzliche nicht kontrollierbare Risiken entstehen.
- Ohne die politische Unterstützung ist langfristig keine ganzheitliche Informationssicherheit für Bürger möglich, da nur diese in der Lage sind, bspw. folgende Beschlüsse zu erlassen: Tracking in jedweder Form zu verbieten bzw. das Mindeststandards der Informationssicherheit für Hersteller von Hard- und Software von Anfang an zu berücksichtigen sind, da sonst keine Inbetriebnahme in Deutschland bzw. der EU erfolgen kann.