STELLUNGNAHME ZUR ANHÖRUNG DES NSA-UNTERSUCHUNGSAUSSCHUSSES AM 26. JUNI 2014*

MICHAEL WAIDNER || Diese Stellungnahme beantwortet die technischen Leitfragen des Untersuchungsausschusses. Sie gliedert sich in zwei Teile, die unabhängig voneinander gelesen werden können. Der erste Teil umfasst die Abschnitte 2 bis 4 und stellt wichtige technische Fakten zusammen. Abschnitt 2 erklärt die Funktionsweise des Internets und die umfangreichen Möglichkeiten, dort abzuhören. Abschnitt 3 erläutert, wie abgehörte bzw. gespeicherte Daten mittels „Big Data" analysiert werden können. Abschnitt 4 beschreibt Möglichkeiten und Grenzen der IT-Sicherheit durch Technik. Der zweite Teil dieser Stellungnahme umfasst Abschnitt 5 und gibt zehn Empfehlungen für Gesetzgeber und Regierung, die insgesamt zu einer deutlichen Verbesserung des Sicherheitsniveaus führen können.

1. ZUSAMMENFASSUNG

Die Grundlage der IT-Sicherheit ist die *Kryptographie* (Abschnitt 4.1). Sie kann auch gegenüber der NSA Sicherheit bieten, und gerade gegenüber der Massenüberwachung ist sie die entscheidende Technologie. Herausforderungen bestehen in der Umsetzung durch Standards und Hard- bzw. Software, die sicher und ohne Hintertüren sein müssen, und in der Bereitstellung der für den Einsatz von Kryptographie notwendigen Infrastrukturen (z. B. vertrauenswürdige Dritte, PKIs) zum Schlüsselaustausch.

Um neben den Inhalts- auch die Metadaten (Verbindungsdaten) zu schützen, müssen *Anonymisierungsdienste* wie „Tor" oder das in Deutschland entwickelte „JonDo" eingesetzt werden (Abschnitt 4.2). Prinzipiell können solche Dienste einen guten Beitrag zum Schutz gegen Massen- und Einzelüberwachung leisten. Für ein flächendeckendendes, allgemein nutzbares Angebot ist allerdings noch erhebliche F&E-Arbeit zu leisten.

Sichere Dienste, insbesondere *sicheres Cloud-Computing* (Abschnitt 4.3), erfordern ebenfalls noch einige F&E-Arbeit. Sichere Cloud-Speicher lassen sich durch Verschlüsselung unter Kundenkontrolle technisch leicht realisieren, setzen sich im Markt aber nur sehr langsam durch. Die marktgetriebenen Innovationszyklen in der IT-Sicherheit sind generell deutlich länger als im Rest der Informationstechnologie, d. h. der Markt alleine reagiert im IT-Sicherheitsbereich sehr langsam. Komplexere Cloud-Dienste erfordern heute noch volles Vertrauen in den Cloud-Anbieter und bieten damit keinerlei technischen Schutz gegen einen direkten Zugriff auf die Daten beim Anbieter.

Das zentrale Thema der *System- und Softwaresicherheit* wird in Abschnitt 4.4 diskutiert. Angesichts der zahlreichen Sicherheitsprobleme heutiger IT und der scheinbar unbegrenzten Fähigkeiten der NSA und anderer Organisationen, in IT-Systeme einzudringen, ist man versucht, den „Kampf" als aussichtslos aufzugeben. Möchte die NSA oder ein vergleichbarer Dienst eine einzelne Person um jeden Preis überwachen, so

kann man dies informationstechnisch tatsächlich nicht verhindern. In der IT-Sicherheit geht es aber überhaupt nicht darum, jeden denkbaren und beliebig aufwändigen Angriff zu verhindern. Das Ziel der IT-Sicherheit ist vielmehr, mit möglichst geringen eigenen Kosten die Kosten des Angreifers nach oben zu treiben. Es geht nicht darum, Angriffe und Werkzeuge wie im Katalog der „Tailored Access Operations" (TAO) der NSA beschrieben[1] komplett zu verhindern, sondern nur darum, deren Entwicklung und Anwendung so teuer zu machen, dass sie nur sehr selektiv eingesetzt werden können. Auch inkrementelle Fortschritte in der IT-Sicherheit können sich also lohnen. Wichtig hierfür ist, auch in der Industrie den Übergang von einer primär reaktiven zu einer primär proaktiven Sicherheit zu vollziehen und das Prinzip von „Security and Privacy by Design" anzuwenden. Zugleich muss intensiv in die Forschung, Entwicklung und Anwendung alternativer, sicherheitsfreundlicher IT-Architekturen investiert werden (nicht nur, aber auch in sogenannte „clean slate" Ansätze).

Auf eine umfassende Darstellung der in den Snowden-Dokumenten beschriebenen Programme wurde verzichtet; eine gute Beschreibung findet man bei Glenn Greenwald.[2] Aus technischer Sicht erscheinen die von Greenwald basierend auf den Snowden-Dokumenten beschriebenen Programme realistisch.

Der zweite Teil dieser Stellungnahme umfasst Abschnitt 5 und gibt zehn Empfehlungen für Gesetzgeber und Regierung, die insgesamt zu einer deutlichen Verbesserung des Sicherheitsniveaus führen können:

1. Vertrauliche Ende-zu-Ende-Kommunikation: Gesetzgeber und Regierung sollten den Aufbau und den Betrieb Ende-zu-Ende-gesicherter Kommunikationsdienste aktiv fördern. Betreiber von Kommunikationsdiensten sollten dazu verpflichtet werden, entsprechende Angebote zu schaffen. Die dafür erforderlichen Infrastrukturen sollten wie z. B. das Straßennetz als öffentliche Infrastrukturen betrachtet und gefördert werden.

Dies ist die wichtigste Empfehlung, soweit es um das Problem der Massenüberwachung durch Abhören geht. In der Fachwelt herrscht Einigkeit, dass Ende-zu-Ende-Verschlüsselung das angemessenste Instrument gegen Massenüberwachung darstellt. Entsprechende Technologien sind bekannt. Die größten Herausforderungen sind die für den durchschnittlichen Nutzer verständliche und benutzbare Integration von Verschlüsselung in Anwendungen und die Schaffung geeigneter „Public Key Infrastrukturen" (PKIs). Letzteres hat sich in der Praxis oft als großes Problem erwiesen, für die Verhinderung von Massenüberwachung genügen jedoch auch vergleichsweise einfache Formen von PKIs.

2. Sichere Nutzung von Diensten: Der Gesetzgeber und die Regierung sollten die Voraussetzungen dafür schaffen, dass sichere Dienste zur Verfügung stehen. Betreiber sollten verpflichtet werden, zu jedem Dienst stets auch die nach Stand der Technik sicherste Dienstnutzungsvariante anzubieten.

Neben der weiteren Förderung von F&E für sicheres Cloud Computing geht es primär darum, die flächendeckende Bereitstellung entsprechend sicherer Cloud-Angebote zu beschleunigen. Wie erwähnt sind die marktgetriebenen Innovationszyklen in der IT-Sicherheit deutlich länger als im Rest der Informationstechnologie, d. h. der Markt alleine reagiert im IT-Sicherheitsbereich zu langsam.

3. Verbesserung des Datenschutzes durch Technik: Um Massenüberwachung durch Unternehmen verhindern zu können, müssen Lösungen entwickelt werden, mittels derer der Fluss von Daten zu unberechtigten Dritten aktiv unterbunden werden kann. Der Gesetzgeber und die Regierung sollten die Entwicklung solcher Lösungen unterstützen und einen Rahmen schaffen, innerhalb dessen diese Lösungen angeboten bzw. als Infrastruktur aufgebaut und betrieben werden.

Die Massenüberwachung durch Nachrichtendienste und die massenhafte Profilbildung und Analyse von Nutzerverhalten durch kommerzielle Anbieter sollte man gemeinsam betrachten. Abgesehen davon, dass für die Menschen beide gleichermaßen bedeutsam sind, greifen Nachrichtendienste direkt oder indirekt auch auf die Daten der kommerziellen Organisationen zu. Hier ist intensive F&E notwendig.

4. „Security and Privacy by Design": Der Gesetzgeber und die Regierung sollten die Weiterentwicklung und Umsetzung des Paradigmas „Security and Privacy by Design" in der IT-Industrie fördern. Dies sollte zunächst die Forschung zur Entwicklung entsprechender Werkzeuge und Prozesse umfassen. Forschungs- und Innovationsprojekte, in denen Informationstechnologie entwickelt oder angewendet wird, sollten verpflichtet werden, die Fragen der IT-Sicherheit in angemessenem Maße zu berücksichtigen.

Dies ist die wichtigste Empfehlung zur Verbesserung der IT-Sicherheit: Wirtschaft, Staat und Forschung müssen den Fokus von reaktiver zu proaktiver Sicherheit verschieben.

5. Prüfung von IT-Sicherheit: Der Gesetzgeber und die Regierung sollten die Voraussetzungen dafür schaffen, dass IT-Produkte hinsichtlich ihrer Sicherheitseigenschaften überprüft werden können. Die Ergebnisse der Überprüfung sollten Anwendern vollständig zugänglich sein. Für Produkte, die in sicherheitskritischen Umgebungen eingesetzt werden, sollten solche Überprüfungen verpflichtend sein, d. h. Produkte sollten nicht eingesetzt werden dürfen, wenn kein der Produktklasse entsprechendes positives Prüfergebnis vorliegt.

Gute IT-Sicherheit kann sich im Markt nur dann behaupten, wenn sie von Käufern und Anbietern als Wettbewerbsvorteil wahrgenommen wird. Dazu müssen Unterschiede in der Sicherheit sichtbar gemacht werden, durch Siegel, Zertifikate usw., und basierend auf objektiven und ohne unnötig hohen Aufwand überprüfbaren Kriterien. Durch eine gezielte Entwicklung solcher Kriterien und darauf basierende Beschaffungsrichtlinien der öffentlichen Hand kann Deutschland bzw. Europa auch entscheidend Einfluss auf die Technologie- und Marktentwicklung nehmen. Die Überprüfbarkeit von IT-Sicherheit erfordert ein hohes Maß an F&E und Investitionen in Infrastrukturen und Labore.

6. Unterstützung von Verbrauchern: Um die Cybersicherheit von Verbrauchern zu verbessern, sollten Gesetzgeber und Regierung eine Organisation zum Verbraucherschutz im Zusammenhang mit Cybersicherheit schaffen, die Verbraucher aktiv darin unterstützt, ihre eigene Sicherheit zu verbessern. Die Arbeit dieser Organisation sollte durch die anwendungsorientierte Forschung begleitet werden.

Verbraucher benötigen für ihre eigene Cybersicherheit eine aktive Interessensvertretung gegenüber Wirtschaft und Staat. Diese Rolle kann auch als Erweiterung des Auftrags an eine bestehende Organisation realisiert werden.

7. Standardisierungssouveränität: Auf Europäischer Ebene sollte eine Organisation identifiziert oder aufgebaut werden, die für eine eigenständig Europäische, mittelfristig internationale Standardisierung im Bereich der Cybersicherheit verantwortlich ist.

Die wichtigsten Cybersicherheitsstandards werden heute vom US-amerikanischen „National Institute of Standards and Technology" (NIST) entwickelt und dann von internationalen Organisationen und anderen Staaten übernommen. Dieser Prozess birgt stets die Gefahr einer einseitigen Bevorzugung US-amerikanischer politischer oder wirtschaftlicher Interessen. Eklatantestes Beispiel ist die von der NSA eingebrachte geheime Hintertür in einem kryptographischen Standard des NIST.[3] Eine intensive, aber vollständig transparente und über jeden Verdacht erhabene Standardisierung unter Europäischer Kontrolle wäre wünschenswert. Die entsprechenden technischen Kompetenzen sind in Europa und Deutschland vorhanden.

8. Technologische Souveränität: Auf Europäischer Ebene sollten die Voraussetzungen dafür geschaffen werden, dass in Europa marktführende Hersteller von Informationstechnologie und IT-Sicherheitstechnologie entstehen.

Deutschland und Europa sind nahezu vollständig von IT-Produkten aus anderen Regionen, insbesondere aus den USA und Asien, insbesondere China, abhängig. Die Überprüfbarkeit von IT-Sicherheit (Empfehlung 5) kann helfen, Vertrauen wiederherzustellen. Darüber hinaus ist es aber auch erforderlich, die Europäische IT- und insbesondere IT-Sicherheitsindustrie zu fördern. Innovationen in der IT

entstehen gemeinhin im Zusammenspiel von exzellenter Forschung und starker, forschungsnaher Industrie.

9. Cybersicherheitsforschung in Deutschland: Der Gesetzgeber und die Regierung sollten einen strategischen und finanziellen Rahmen zur Förderung der Cybersicherheitsforschung in Deutschland schaffen. Der Umfang der nationalen Forschungsförderung sollte deutlich erhöht werden. Deutschland sollte sich intensiv für ein gezieltes Forschungsprogramm zur Cybersicherheit auf Europäischer Ebene einsetzen. Die Politik der Bildung nationaler, auf Dauer angelegter und an Exzellenz auf internationalem Niveau ausgelegter Kompetenzzentren für Cybersicherheitsforschung sollte fortgesetzt und ausgebaut werden. Cybersicherheit ist ein Querschnittsthema und sollte als solches bei allen öffentlich geförderten Innovationsprojekten zwingend Berücksichtigung finden.

Anwendungs- und Grundlagenforschung sind essenziell für die Cybersicherheit. Hier geht es primär darum, die in Deutschland vorhandenen Forschungskapazitäten zur Cybersicherheit weiter zu bündeln, zu fördern und auszubauen. Aus meiner Sicht als Leiter eines der drei vom BMBF finanzierten Kompetenzzentren zur Cybersicherheitsforschung hat sich das Konzept der Bildung von Zentren sehr bewährt und sollte fortgesetzt und ausgebaut werden. Inhaltlich wurden bereits strategische Schwerpunkte gesetzt, z. B. auf „Security and Privacy by Design“, und eine kritische Masse exzellenter Forscherinnen und Forscher erreicht, die auch international als Schwergewicht wahrgenommen wird. Eine entsprechende Fokussierung auf Cybersicherheit fehlt leider im Programm „Horizon 2020“ der EU.

10. Verzahnung von Rechts- und Technikgestaltung: Um die Rechts- und Technikgestaltung besser miteinander verzahnen zu können, sollten die Verträglichkeit des Rechts- und Technikrahmens kontinuierlich überwacht werden, die Techniktrends hinsichtlich ihrer Relevanz für den Rechtsrahmen möglichst früh analysiert werden, Betroffene möglichst früh über die relevanten Implikationen neuer gültiger Rechtsgestaltung empfängeradäquat informiert und Vorschläge für juristische Diskussionen und neue Rechtsrahmen ggf. vor ihrer Verabschiedung im Rahmen von Simulationsstudien geprüft werden.

Recht und Technik sind in den Bereichen Cybersicherheit und Privatsphärenschutz sehr eng verwoben und müssen sich dementsprechend synchron weiterentwickeln.

Zuordnung zu den Leitfragen

Die Leitfragen des Untersuchungsausschusses werden in den folgenden Abschnitten dieser Stellungnahme beantwortet:

- Frage 1 (Grundlegendes zur Informationstechnik) wird in den Abschnitten 2 (Internet), 4.2 (Anonyme Kommunikation) und 3 („Big Data“) beantwortet.
- Frage 2 (Grundlegendes zu den Zugriffstechniken) wird in den Abschnitten 2 (Zugriff auf Internetkommunikation) und 4 (Umgehung von Schutzmaßnahmen) beantwortet.
- Frage 3 (Auswertung von Inhalts- und Metadaten) wird in Abschnitt 3 („Big Data“) beantwortet.
- Frage 4 (Abwehrmöglichkeiten) wird in Abschnitt 4 (Sicherheit) beantwortet, sowie im Sinne von Empfehlungen in Abschnitt 5.
- Fragen 5 und 6 (Notwendige Änderungen) werden in Abschnitt 5 (Empfehlungen) beantwortet.

Dank

Diese Stellungnahme entstand in Zusammenarbeit mit Dr. Markus Schneider und Dr. Michael Kreutzer. Für ihre großzügige Unterstützung möchte ich mich sehr herzlich bedanken. Ebenfalls herzlich bedanken möchte ich mich bei Dr. Birgit Baum-Waidner, Dr. Mathias Fischer, Dr. Haya Shulman und Hervais Simo für ihre Hilfe bei der Recherche einzelner Fragen.

2. FUNKTIONSWEISE UND ABHÖRRISIKEN DES INTERNETS

Kapitel 2 fasst grundlegende technische Sachverhalte zusammen, die für ein Verständnis der bekannt gewordenen Massenüberwachungsmaßnahmen hilfreich sind.

2.1 Grundlegendes zur Kommunikation im Internet

Das Internet hat sich mit dem Durchbruch des World Wide Web in den vergangenen 20 Jahren zur universell genutzten Kommunikationsinfrastruktur entwickelt. Im Folgenden werden die für das weitere Verständnis wichtigen technischen Aspekte des Internets dargestellt.

Autonome Systeme

Das Internet ist kein einheitliches Netz mit einer zentralen Steuerung, sondern tatsächlich ein „Inter-netz", ein Netz von Netzen. Derzeit besteht das Internet aus ca. 11.000 Teilnetzen, genannt „Autonomous Systems" (AS), die meist von spezialisierten „Internet Service Providern" (ISP) betrieben werden.[4]

Durch die Digitalisierung kann das Internet heute für nahezu jede elektronische Kommunikation genutzt werden. Kommunikationsdienste, die früher über eigene Kommunikationsnetze angeboten wurden (z. B. Telefonie, Radio und Fernsehen), nutzen heute ebenfalls die Infrastruktur des Internets, insbesondere im Weitverkehrsbereich zur Überwindung großer räumlicher Distanzen mit den leistungsfähigen Backbone-Netzen der großen AS.

Die Firma Cisco prognostiziert, dass sich das Datenvolumen im Internet innerhalb der nächsten vier Jahre mehr als verdoppeln wird, von ca. 1.700 Petabytes / Tag in 2013 auf ca. 4.300 Petabytes / Tag in 2018.[5] Die NSA schätzt, dass sie ca. 1,6 % dieses Volumens „berührt".[6]

Internet Protokoll

Die Übertragung von Nachrichten (z. B. E-Mails, Web-Seiten, Video-Streams, VoIP-Telefongesprächen) innerhalb und zwischen den AS erfolgt nach einem einheitlichen Standard, dem „Internet Protocol" (IP) in den beiden Versionen IPv4 und IPv6. Da IP nur sehr kurze Nachrichten, sogenannte IP-Pakete, übertragen kann, müssen die meisten Nachrichten beim Sender auf mehrere IP-Pakete verteilt („fragmentiert") und beim Empfänger entsprechend zusammengesetzt werden. IP-Pakete enthalten neben den eigentlichen Inhaltsdatenfragmenten auch Metadaten, z. B. die Sender- und Empfängeradressen.

Status Verschlüsselung

Inhaltsdaten und Metadaten werden durch IP im Klartext, also ungeschützt, übertragen. Sollen die Inhaltsdaten vor Manipulation und unerlaubtem Mitlesen geschützt werden, so geschieht das im Netz höchstens auf ausgewählten Strecken zwischen bestimmten Netzknoten (Rechnern). Die Ver- und Entschlüsselung wird dann von den jeweiligen Netzknoten vorgenommen. Das bedeutet, dass Daten in den Netzknoten ungeschützt vorliegen. Um eine durchgängige Sicherung zu erhalten, muss die Anwendung, die die Daten beim Sender produziert oder beim Empfänger entgegennimmt (also z. B. E-Mail-Programme, Web-Server und Browser, VoIP-Endgeräte), selbst für die geeignete Ende-zu-Ende-Verschlüsselung sorgen. In Europa werden derzeit ca. 6 % des Internet-Verkehrs verschlüsselt (SSL/TLS Anteil am TCP-Verkehr), was zwar nicht viel ist, aber eine Vervierfachung gegenüber dem Vorjahr, also der Zeit „vor Snowden", darstellt.[7]

Metadaten werden für die Funktionsweise von IP benötigt und können von der Anwendung deshalb nicht direkt geschützt werden. Anonymisierungsdienste dienen der Vermeidung bzw. Verbergung von Metadaten (Abschnitt 4.2).

Routing und BGP

Die entscheidende Fähigkeit des Internets ist es, IP-Pakete von jedem beliebigen Sender zu jedem beliebigen Empfänger transportieren zu können. Der Sender muss hierfür lediglich die IP-Adresse des Empfängers kennen (z. B. „141.12.72.204" für den Web-Server des Fraunhofer SIT). Im Allgemeinen muss ein IP-Paket dazu über mehrere Vermittlungsrechner und mehrere Autonome Systeme hinweg weitergereicht werden. Das hierzu notwendige „Routing", also die Bestimmung des Weges, den ein IP-Paket vom Sender zum Empfänger nimmt, erfolgt dezentral. Jeder AS-Betreiber kann autonom festlegen, nach welchen Regeln innerhalb seines Netzes das Routing stattfinden soll. Das Routing zwischen den AS ist über das sogenannte „Border Gateway Protocol" (BGP) standardisiert und basiert auf Routingtabellen, die jedes AS selbst verwaltet. Diese Tabellen werden ständig aktualisiert, basierend auf Informationen, die die AS untereinander austauschen.

Sofern sich die AS korrekt verhalten und keine falschen Informationen verbreiten, geben die Routingtabellen an, welches die aktuell günstigsten Wege zu allen anderen AS sind.

Das Internet-Routing ist sehr robust gegen zufällige Ausfälle einzelner AS, aber nicht besonders sicher gegen Angriffe. Durch Modifikationen in Routingtabellen können die Wege, entlang derer Datenpakete übertragen werden, geändert werden, so dass Daten auf ihrem Weg andere Netzknoten passieren.

Nachrichten gehen Umwege

Zum einen ist der günstigste Weg zwischen zwei AS meist nicht der kürzeste. Die bestimmenden Faktoren sind eher Verträge, Kosten und Durchleitungskapazitäten. Häufig führt der günstigste Weg zwischen zwei geographisch nahe gelegenen AS daher über größere, global agierende „Tier 1“ AS. Der damit verbundene Umweg kann zu zusätzlichen Abhörmöglichkeiten führen, insbesondere zur Massenüberwachung. Die meisten der global agierenden „Tier 1“ AS haben ihren Firmensitz in den USA. Die Deutsche Telekom betreibt allerdings ebenfalls ein „Tier 1“ AS.

Zum anderen wird die Information, die zum Aufbau der Routingtabellen und damit zur Festlegung der günstigsten Wege führt, von den AS kaum überprüft. Ein AS kann deshalb relativ einfach dafür sorgen, dass der Internetverkehr zwischen zwei anderen AS vollständig über dieses eine AS geroutet wird. Damit kann dieses AS diesen Verkehr vollständig mitlesen. Seit 2013 wurde dieses Verhalten vermehrt beobachtet; beispielsweise wurde der Verkehr innerhalb (!) der US-amerikanischen Stadt Denver zeitweilig über ein AS in Island umgeleitet.[8] Diese Angriffstechnik ist für eine längerfristige Massenüberwachung allerdings weniger geeignet.

DNS und DNSSEC

Eine weitere, für Angriffe leicht ausnutzbare Schwachstelle des Internets verbirgt sich im „Domain Name System“ (DNS) bzw. der Infrastruktur, die DNS-Namen wie „www.sit.fraunhofer.de“ auf IP-Adressen wie „141.12.72.204“ abbildet. Anwendungen nutzen erstere, das Routing im Internet letztere. Wer die Übersetzung zwischen beiden kontrolliert, kann sehr leicht Verbindungen über eigene Systeme umleiten und so den Verkehr mitlesen. Entsprechende Angriffstechniken sind seit langem bekannt und werden aktiv verwendet. Besonders einfach auszuführen sind solche Angriffe im öffentlichen WLAN oder, wie in den Snowden-Dokumenten,[2, 9] unter „QUANTUM“ und „FOXACID“ beschrieben, in Kooperation mit großen AS. Diese Angriffe eignen sich für die Einzelüberwachung.

Ende der 1990er-Jahre wurde mit den „Domain Name System Security Extensions“ (DNSSEC) und 2011 mit dem darauf aufbauenden „DNS-based Authentication of Named Entities“ (DANE) eine Erweiterung von DNS entwickelt, die diese und viele andere Probleme der Internet-Sicherheit im Prinzip stark reduzieren könnten. DNSSEC wird international stark gefördert, allerdings mit mäßigem Erfolg: Anfang 2014 waren weltweit mehr als 50 % aller „Top Level Domains“ (TLD) mit DNSSEC abgesichert, aber weniger als 1 % aller „Second Level Domains“. Weltweit konnten weniger als 5 % der „Resolver“, also DNS Clients, mit DNSSEC umgehen.[10]

2.2 Angriffspunkte für die Massenüberwachung

Für die Massenüberwachung sind all die Stellen von besonderem Interesse, an denen der Internetverkehr gebündelt wird und folglich mit vergleichsweise geringem Aufwand und ohne ein größeres Entdeckungsrisiko ein großes Volumen abgegriffen werden kann. Mit dieser Strategie kann mit vergleichsweise wenigen Zugriffspunkten auf sehr viele Verbindungen zugegriffen werden. Darüber hinaus können Datenpakete so gelenkt werden, dass sie die Stellen passieren, an denen Zugriffsmöglichkeiten bestehen, z. B. indem Daten wie in Abbildung 1 gezeigt durch bestimmte Länder gelenkt werden. Von den Zugriffspunkten können die Daten in Kopie über Kommunikationsnetze zu weiteren Speicher-, Untersuchungs- und Verarbeitungseinrichtungen geleitet werden.

Die globalen „Tier 1“ AS wurden bereits als Angriffspunkte erwähnt.

Abbildung 1: Einordnung von PRISM, von E. Snowden veröffentlicht

Ein ähnlicher Zugriff kann an den sogenannten „Internet Exchange Points“ (IXP) erfolgen, die die eigentliche Verbindung zwischen AS herstellen. Ein IXP besteht im Prinzip aus sehr leistungsstarken „Switches“, die eingehenden Datenverkehr möglichst verzögerungsfrei in die richtige Richtung weiterleiten. Geschätzt existieren derzeit ca. 350 globale IXP, an die jeweils zwischen 150 bis 500 AS angeschlossen sind.[4]

Der IXP mit dem weltweit größten Datendurchsatz ist das DE-CIX in Frankfurt am Main. Im Jahr 2012 verband DE-CIX über 480 AS aus 50 Ländern und erreichte einen Datendurchsatz von 12 Petabyte pro Tag (das entspricht 2,7 Millionen DVDs pro Tag). Erstmals überstieg der Spitzendatendurchsatz 2 Tbit/s (Terabit pro Sekunde).[11] Einen ähnlichen Spitzendatendurchsatz erreichen auch andere IXP, z. B. der IXP linx in London. Über einen direkten Zugriff ausländischer Nachrichtendienste auf DE-CIX ist mir nichts bekannt.

Weitere lohnende Angriffspunkte ergeben sich auf allen Übertragungswegen, über die ein großes Datenvolumen übertragen wird. Insbesondere zählen hierzu die Tiefseekabel, über die der Großteil des interkontinentalen Internetverkehrs läuft, sowie Satellitenverbindungen, Überlandkabel und Richtfunkstrecken. Die Snowden-Dokumente erwähnen hierzu diverse Programme, z. B. GCHQ's TEMPORA.[12]

Wie Vodafone kürzlich eingeräumt hat, existieren in einigen europäischen Staaten Stellen, an denen Behörden direkt auf Kommunikationsdaten zugreifen können.[13] Diese Zugangsmöglichkeiten ergeben sich unmittelbar aus gesetzlichen Verpflichtungen der Netzbetreiber in den betroffenen Ländern. Wenn direkte Zugriffsmöglichkeiten eingeräumt werden, dann gelten diese immer nur für die Behörden des Landes, in dem der Zugriff liegt. Nach Aussage von Vodafone gibt es in Deutschland keinen direkten Zugang für Behörden.

Anmerkung zum „Schengen-Routing“

Angesichts der eben dargestellten Angriffspunkte wurde vorgeschlagen, durch Eingriffe in das Routing zu verhindern, dass Nachrichten zwischen zwei Endpunkten im Schengen-Raum über AS und Leitungen außerhalb des Schengen-Raums geleitet werden.[14] Eine Massenüberwachung dieses Verkehrs könnte dann nur im Schengen-Raum erfolgen, was als unwahrscheinlich betrachtet wird.

Dieser Ansatz reduziert tatsächlich die Angriffsfläche, ist in seiner Wirkung aber sehr begrenzt. Insbesondere bleibt die Kommunikation zwischen Europa und z. B. den USA völlig ungeschützt. Umgekehrt sind die Kosten für diesen Ansatz kaum abzuschätzen. Sehr wahrscheinlich müssten die innereuropäischen IXP (z. B. DE-CIX) und Tier 1-AS (z. B. Deutsche Telekom) ihre Durchleitungskapazitäten deutlich ausbauen. Darüber hinaus kann dieser Ansatz nicht vermeiden, dass Inhalte kopiert werden und die Kopien über europäische Grenzen hinweg übertragen werden.

Das „Schengen-Routing“ kann die konsequente Ende-zu-Ende-Verschlüsselung nicht ersetzen. Letztere sollte dagegen vorrangig angestrebt werden.

3. „BIG DATA“ UND DER WERT VON METADATEN

Bei Massenüberwachung besteht der erste Schritt darin, an Daten zu gelangen. Der ganz entscheidende zweite Schritt jedoch ist, diese Daten zu analysieren und auszuwerten. Hier spielt „Big Data“ eine große Rolle. „Big Data“ ist keine Massenüberwachungstechnologie an sich, kann aber dazu genutzt werden.

Im Folgenden werden die Aspekte von „Big Data“ dargestellt, die für die Massenüberwachung von Relevanz sind bzw. sein können. Darüber hinaus soll ein Eindruck vermittelt werden, was heute bereits mit „Big Data“ möglich ist.

3.1 Grundlagen von „Big Data“

Inhalts- und Metadaten

Wenn man Daten betrachtet, dann ist eine Unterscheidung in „Inhaltsdaten“ und „Metadaten“ sinnvoll:

Unter „Inhaltsdaten“ verstehen wir die Daten, die von Personen oder von Maschinen als Kommunikationsteilnehmern generiert und ausgetauscht werden, wobei die Daten den eigentlichen Nachrichteninhalt darstellen. Beispiele für Inhaltsdaten sind die in einem Telefonat ausgetauschten Sprachdaten, der Inhalt einer E-Mail, eine abgerufene Webseite oder der Inhalt eines hochgeladenen Webformulars, ein digitalisiertes Bild oder ein Video.

Bei Inhaltsdaten kann man unterscheiden, ob es sich um strukturierte oder unstrukturierte Daten handelt. Strukturierte Daten zeichnen sich dadurch aus, dass sie einen festen Aufbau haben, so dass die Bedeutung des Inhalts aus der Struktur folgt wie z. B. bei einem mit Kontaktdaten ausgefüllten Web-Formular. Die meisten Daten sind jedoch unstrukturiert wie z. B. Volltexte, in denen die Bedeutung von einzelnen Textfragmenten für eine Maschine nicht ohne weiteres zu erschließen ist.

Für den Begriff „Metadaten“ gibt es unterschiedliche Bedeutungen. Hier verstehen wir darunter solche Daten, die Informationen zu verschiedenen Aspekten anderer Daten, z. B. Inhaltsdaten, enthalten. Im Zusammenhang mit einer Kommunikationsbeziehung wie Telefonie oder E-Mail können Metadaten Informationen beschreiben wie Sender- und Empfängeradresse, Beginn und Ende der Kommunikationsbeziehung, Dauer der Verbindung und Umfang des Inhalts. Im Zusammenhang mit Webseitenaufrufen können Metadaten Informationen beschreiben wie abgerufene URL, Referer-URL, IP-Adresse des Nutzers, Zeitpunkt des Abrufs, Aufenthaltsort, Betriebssystem oder verwendeter Browser. Bei Metadaten handelt es sich um strukturierte Daten, weshalb diese relativ einfach von Maschinen verarbeitet werden können.

Algorithmen

Algorithmen sind Verfahren zur Verarbeitung von Daten. Im Zusammenhang mit der Sammlung von Massendaten verstehen wir darunter Methoden, mit denen aus gesammelten Daten neue Informationen produziert werden. Hierbei geht es darum, dass Daten aus verschiedenen Quellen miteinander kombiniert werden, zueinander in Beziehung gesetzt werden,

um eventuell darin enthaltene Muster aufzuspüren und daraus Schlüsse zu ziehen.

Was man aus Metadaten ableiten kann

Allein aus Metadaten lassen sich heute sehr viele Informationen ableiten, die sich für unterschiedliche Zwecke verwerten lassen, z. B.:

- Aus Facebook ergeben sich Freundeskreis, Beziehungen und Interessen.
- Aus Skype ergeben sich Adressbuch, Beziehungen und Kommunikationsverhalten.
- Aus LinkedIn und XING ergeben sich Kompetenzen.
- Aus aufgerufenen URLs ergeben sich Einblicke in Interessen, politische Einstellungen, Lebenssituationen.

Können beispielsweise Metadaten zu sozialen Beziehungen, z. B. aus Facebook oder Skype, mit Daten zu Interessen oder Konsumverhalten aus den URLs aufgerufener Webseiten kombiniert werden, so können Interessen und Konsumverhalten einer Person auf eine andere Person übertragen werden, die zur ersten Person in einer sozialen Beziehung steht, z. B. „Freundschaft", was aus häufigen Kommunikationsbeziehungen zwischen den beiden Personen geschlossen wird. Solche Schlüsse aus der Kombination von Metadaten aus verschiedenen Quellen werden heute beispielsweise für die zielgerichtete Werbung verwendet.

Auch zur staatlichen Massenüberwachung lassen sich gesammelte Metadaten auswerten. Das entstehende Gefühl der Kontrolle führt zu einer Beeinträchtigung der informationellen Selbstbestimmung und Freiheit, z. B. zur Meidung von Personen, die möglicherweise von den Analysealgorithmen als verdächtig eingestuft werden könnten, oder zur Annahme einer bestimmten, für unverdächtig gehaltenen Wortwahl in E-Mails. Auch direktere Diskriminierungen sind denkbar, z. B. bei der Einreise oder durch die Nichtgewährung von Überflugrechten.[15, 16]

3.2 Der Schritt zu „Big Data"

Das Schlagwort „Big Data" bezeichnet eines der derzeit wichtigsten IT-Themen. Es geht dabei stets um große, schnell anwachsende Datenmengen unterschiedlichster Herkunft und die Frage, mit welchen Algorithmen man dort interessante Informationen „schürfen" könnte. Häufig wird Big Data über die „Drei V" definiert:[17]

„Volume", Datenumfang

Bei Big Data geht es darum, dass große Datenmengen verarbeitet werden können. Innerhalb von nur einer Minute werden gemäß Angaben von Intel weltweit durchschnittlich ca. 204 Millionen E-Mails versendet, mehr als 320 neue Twitter-Accounts angelegt und ca. 100.000 Tweets abgesetzt, 6 Millionen Seiten bei Facebook aufgerufen, mehr als 2 Millionen Suchfragen bei Google abgesetzt und ca. 640.000 GB Daten über das Internet übertragen.[18] Allein Google sammelt jeden Tag 24 PB (1 Petabyte entspricht 10^3 Terabyte) neue Daten. Dieses Volumen entspricht ausgedruckt ungefähr dem Tausendfachen aller gedruckten Werke der Library of Congress in den USA.[19]

Gerade mit Blick auf die Massenüberwachung im Internet geht es um Datenmengen im Bereich von Petabytes (PB) und Exabytes (EB).[20] Eine Speicherkapazität von 1 EB genügt, um ca. 49 Tage lang alle Daten am DE-CIX bei konstantem Spitzendurchsatz oder ca. 14 Stunden lang alle Daten des heutigen globalen Internetverkehrs zu speichern.

Für Facebook und CERN sind Datenzentren mit einer Speicherkapazität von je 1 EB geplant.[21, 22] Für die NSA ist in Utah ein Datenzentrum in Planung, das eine Kapazität von mehreren EB bis YB (1 Yottabyte ≈ 10^{24} Bytes) erreichen soll.[23]

„Variety", Datenvielfalt

Big Data umfasst die Behandlung von vielen verschiedenen Datenquellen. Hierzu gehören sowohl Metadaten als auch Inhaltsdaten, und zwar strukturiert sowie auch unstrukturiert.

Die Daten können von verschiedenen Personen und Organisationen (z. B. Behörden mit Meldedaten, Forschungszentren mit Krebsregister) wie auch unterschiedlichen Geräten generiert werden wie PC, Smartphones, Überwachungskameras, Sensoren wie Fitness Tracker, Automobile, Verkehrsleitsysteme oder Geräte für das Smart Home zur Steuerung von Haustechnik. Sie können im Zusammenhang klassi-

scher IT-Anwendungen (z. B. Textdokumente, Tabellenkalkulationen) wie auch bei verschiedenen Kommunikationsanwendungen entstehen (z. B. Telefonie, E-Mail, Web-Browsen, Suchanfragen). Die Vielfalt der Daten umfasst auch die Vielfalt verschiedener Medientypen wie Text, Audio und Video und Dokumente, die aus Kombinationen dieser Medientypen bestehen wie z. B. Webseiten oder Profile in sozialen Netzen. Darüber hinaus generieren viele Softwareanwendungen viele Metadaten, die sie an viele verschiedene Stellen versenden wie z. B. bestimmte Smartphone Apps kontinuierlich die Geoposition des aktuellen Aufenthaltsorts an Server versenden oder Browser aufgrund von Web-Tracking die Adressen der aufgerufenen Webseiten nicht selten im Hintergrund an mehr als 50 verschiedene Organisationen im Hintergrund versenden.[24]

Um diese umfangreichen Datenbestände gut nutzen zu können, müssen die Einträge aus den verschiedenen Datenquellen, die zur gleichen Person gehören, dieser Person zugeordnet werden können. Hierzu helfen oftmals Metadaten wie z. B. Identitäten, Adressen, Merkmale der technischen Ausrüstung wie Konfigurationen oder Betriebssystemversion, technische Erweiterungen, Nutzungsmuster.

„Velocity", Analysegeschwindigkeit

Die Daten werden mit speziellen Algorithmen analysiert. Hierbei werden die Daten aus verschiedenen Datenquellen kombiniert und in Beziehung gesetzt, um Informationen zu neuen Erkenntnissen aus den Daten zu extrahieren. Hierzu wird ausgehend von geeigneten Modellen (z. B. Vorhersagemodelle, Datenmodelle) nach Mustern und Korrelationen in den vorliegenden Daten gesucht, um Zusammenhänge sichtbar zu machen, die bisher nicht bekannt waren. Entscheidungen werden dann nicht mehr scharf, sondern aufgrund von Wahrscheinlichkeiten getroffen. Auf Basis der vorliegenden Daten und Wahrscheinlichkeiten wird auch versucht, Schritte in der Zukunft vorherzusagen und diese Vorhersagen für die Zukunft schon bei den Entscheidungen der Gegenwart zu berücksichtigen.

Für Analysen großer Datenbestände sind große IT-Ressourcen notwendig. Eine wichtige Unterscheidung bei der Analysegeschwindigkeit ist, wie schnell nach der Entstehung Daten analysiert werden sollen.

Bei „Big Data in Motion" werden die Daten per „Realtime Analytics" oder „Stream Processing" genauso schnell analysiert, wie sie entstehen. Häufig werden diese Daten nicht oder nur zu einem sehr geringen Umfang gespeichert. In dieser Kategorie gibt es Systeme zur Fehler-, Betrugs- und Angriffserkennung, Sprachübersetzung, Annotation von Ton- und Bildaufnahmen, Klassifikation von Nachrichten, aber auch autonome Systeme z. B. im Börsenhandel.

Bei „Big Data at Rest" werden die Daten zunächst gespeichert und zu einem beliebigen Zeitpunkt aufbereitet und per „Data Mining" analysiert. Hier geht es primär darum, nach Mustern und statistischen Korrelationen, nach den „Stecknadeln im Heuhaufen" zu suchen. Häufig geht es tatsächlich um die Suche nach Information und Wissen (z. B. bei Microsoft Bing, Google Search, IBM Watson) oder die Bewertung von Risiken, das Vorhersagen von Ereignissen, Trends und Verhalten sowie die Optimierung von Prozessen.

Big Data Analysen arbeiten oft auf vielen unterschiedlichen Datenquellen ggf. mit verschiedenen Datenformaten, da sich wertvolle Hinweise oft gerade aus Querbezügen zwischen scheinbar unabhängigen Quellen ergeben. Ein sehr einfaches Beispiel ist die „Rasterfahndung" der 1970er-Jahre, komplexere Beispiele sind die Erstellung von Meinungsbildern, basierend auf einer Analyse aller öffentlichen Nachrichtenquellen, oder das „Cognitive Computing" hinter einem System wie IBM Watson.

Für eine Analyse von Daten, die verschiedene Medientypen beinhalten, und eine Herstellung von Querbezügen über solche heterogenen Datenbestände müssen diese ggf. vorverarbeitet, transformiert oder annotiert werden, z. B. mittels Spracherkennung,[25] Textanalyse, Übersetzung, Stilometrie[26] und Autorenerkennung, Gesichtserkennung und Stimmerkennung, Szenenerkennung.

X-KEYSCORE

Das in den Snowden-Dokumenten beschriebene Programm X-KEYSCORE umfasst den kompletten Vorgang der Massenüberwachung auf Basis der Analyse von Metadaten.

Abbildung 2 fasst den Vorgang zusammen: X-KEYSCORE überwacht „Sessions“, also alle IP-Pakete, die einen zusammengehörenden Kommunikationsvorgang bilden. Algorithmen extrahieren hieraus Metadaten, die dann in einer Datenbank abgelegt werden.

Abbildung 3 benennt einige sehr einfache Beispiele von Metadaten; denkbar sind hier auch deutlich komplexere, aus den Inhaltsdaten abgeleitete Metadaten. Analysten können auf diese Datenbank zugreifen und über vordefinierte Big-Data-Algorithmen nach Mustern und Zusammenhängen suchen.

Abbildung 2: Funktionsweise von X-KEYSCORE, von E. Snowden veröffentlicht

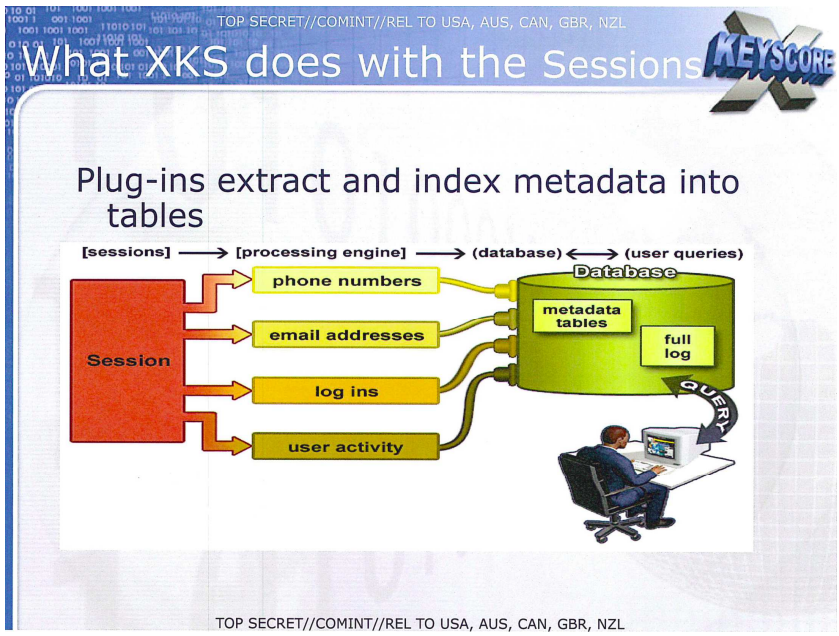
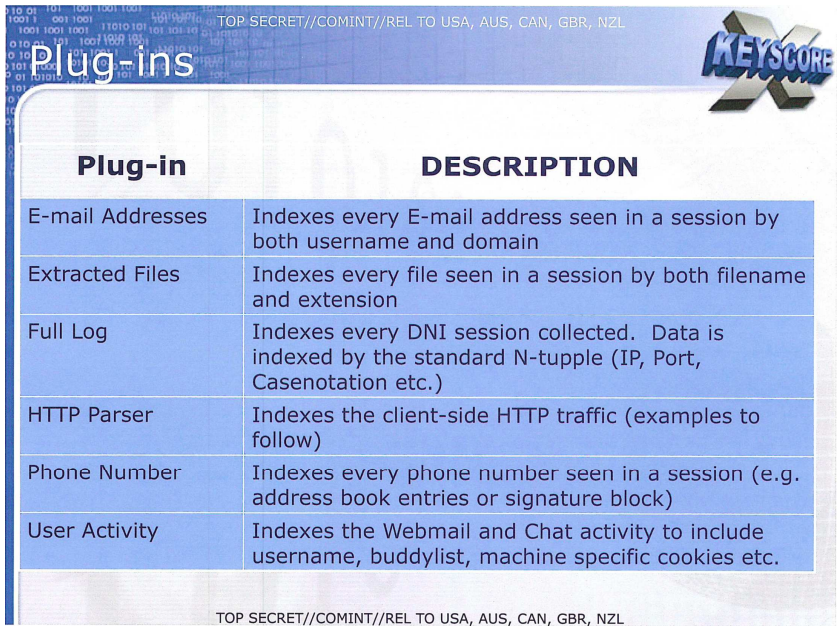


Abbildung 3: Beispiele von Plug-ins für X-KEYSCORE, von E. Snowden veröffentlicht



3.3 Implikationen von „Big Data“

Es gibt viele, insbesondere auch sehr viele positive Anwendungen und Implikationen von Big Data. In diesem Dokument möchte ich jedoch nur auf die Anwendungen und Implikationen von Big Data eingehen, die im Zusammenhang mit der Überwachung entstehen.

Durch die Sammlung und Speicherung umfangreicher Datenbestände, die alle Bereiche des Alltags von Personen betreffen können, und die Möglichkeit zur Analyse dieser Datenbestände steht ein großes und mächtiges Instrumentarium zur Verfügung, das auch gegen die Interessen der Nutzer eingesetzt werden kann. Welche Daten sie von sich preisgeben und zu welchen Zwecken sie jetzt oder künftig genutzt werden, können sie nicht wirklich einschätzen. Der konkrete Verwertungszweck sowie weitere Verwertungsmöglichkeiten der Daten ergeben sich erst aus den jeweiligen konkreten Big-Data-Algorithmen, die die Daten analysieren und verwerten.

Hat die Praxis dieser Datenverwertung Rückwirkungen auf die Handlungen von Menschen, so wird dadurch ihre Freiheit eingeschränkt. Dies impliziert einen Verlust an Selbstbestimmung (z. B. den Verzicht auf eigentlich gewollte, aber für nicht opportun gehaltene Kommunikationsbeziehungen).

Auch die Meinungsfreiheit kann durch die Anwendung von Big Data im Zusammenhang mit Massenüberwachung beeinträchtigt werden. Die Freiheit von Meinungen und Gedanken beinhaltet explizit die Freiheit der freien Informationsbeschaffung und der eigenen Entscheidung, wem gegenüber man seine Meinung äußert und wem man diese zugänglich macht. Das Wissen um Massenüberwachung allgemein und die Kombination mit Big-Data-Technologie im Besonderen kann den informierten Bürger daran hindern, sich frei Informationen zu beschaffen, z. B. aus Angst vor negativen Konsequenzen. Das Internet ist jedoch heute zu einer sehr wichtigen Quelle für die Beschaffung aktueller Information geworden.

Die Anwendung von Big-Data-Algorithmen im Zusammenhang mit der Massenüberwachung kann beispielsweise zu folgenden Konsequenzen führen:

- *Risiken durch falsche Entscheidungen:* Wendet die Massenüberwachung Big-Data-Algorithmen an, dann kann dies für Menschen negative Konsequenzen haben, obwohl sie sich nichts haben zu Schulden kommen lassen. Da Big-Data-Algorithmen ihre Entscheidungen nicht mehr scharf, sondern auf der Basis von Wahrscheinlichkeiten und Vorhersagemodellen treffen, können die Entscheidungen dieser Algorithmen im Einzelfall falsch sein. Mit dem Trend zur „Datafizierung“, bei dem praktisch alle Lebensbereiche digital erfasst werden, genügen bestimmte Übereinstimmungen in den erfassten Daten mit den Daten solcher Personen (z. B. Aufruf derselben Seiten im Internet, ähnliches Konsumverhalten), die nachrichtendienstlich erfasst sind, dass Entscheidungen zur Intervention getroffen werden.
- *Umgehung von Schutzmaßnahmen:* Auch wenn sich Menschen mit heute verfügbaren Mitteln wie z. B. zur Anonymisierung schützen möchten, dann ist es durchaus möglich, dass der Schutz angesichts von mächtigen Big-Data-Anwendungen nicht hinreichend ist. Selbst wenn Daten in Datenbanken anonymisiert werden, dann ist es durchaus möglich, dass Big-Data-Algorithmen mit Zugriffsmöglichkeiten auf andere Datenbanken Zusatzwissen ausnutzen können. Mittels Querbeziehungen lassen sich dann Mengen von potenziell in Frage kommenden Kandidaten so weit aussieben, dass anonymisierte Daten der korrekten Person zugeordnet werden können. Die Deanonymisierung von Einzelfällen kann auch ohne moderne Big-Data-Technologie gelingen, wie ein Fall in den USA gezeigt hat, bei dem in publizierten anonymisierten Tabellen mit Gesundheitsdaten die Daten von William Weld, dem damaligen Gouverneur von Massachusetts, identifiziert werden konnten.[27] Für eine massenhafte Durchführung von Deanonymisierungen ist jedoch eine leistungsfähige Technologie wie Big Data erforderlich.

4. MÖGLICHKEITEN UND GRENZEN VON SICHERHEIT UND PRIVATSPHÄRENSCHUTZ DURCH TECHNIK

Im Folgenden werden einige grundlegende Aspekte von Sicherheit und Privatsphärenschutz durch Technik diskutiert: Kryptographie, Anonymisierungsdienste, Sicherheit von Cloud-Diensten und das allgemeine Problem der System- und Softwaresicherheit.

4.1 Kryptographie

Die Kryptographie stellt Verfahren zur „Nachrichtenvertraulichkeit", also Verschlüsselung, und zur „Nachrichtenintegrität", also zum Erkennen unerlaubter Nachrichtenmanipulationen durch Prüfcodes und digitale Signaturen, bereit. Die Verfahren benötigen hierzu „Schlüssel", die ähnlich wie Passwörter gut und zufällig gewählt und dann geheim gehalten werden müssen.[28] Die Wahl der Schlüssel übernehmen spezielle Algorithmen, die dafür eine nur dem Schlüsselbesitzer zugängliche Quelle von Zufallszahlen benötigen.

Um Kryptographie einzusetzen, muss man mehrere Ebenen betrachten, und jede birgt gewisse Risiken und Angriffspunkte:

- Algorithmen und Standards,
- Vertrauensinfrastrukturen,
- Implementierung und Anwendung.

Ebene der Algorithmen und Standards

Zunächst muss man die Verfahren an sich betrachten, also deren mathematische Beschreibungen z. B. aus wissenschaftlichen Papieren und Standards. Hierzu gehören die Grundalgorithmen (z. B. RSA, AES, Pseudozufallszahlengeneratoren), physikalischen Prozesse zur Zufallszahlenerzeugung sowie die Protokolle, in denen Grundalgorithmen verwendet werden z. B. SSL/TLS und DNSSEC.

Bis Mitte der 1970er-Jahre war die Kryptographie durch Nachrichtendienste, insbesondere durch GCHQ und NSA, dominiert und tatsächlich eine „Geheimwissenschaft". Seither hat sich die Kryptographie grundlegend gewandelt und ist zu einer international stark vernetzten, öffentlich agierenden und sehr aktiven Wissenschaft geworden. In Europa und besonders in Deutschland gibt es eine ganze Reihe exzellenter Forschungsgruppen zur Kryptographie.

Ich gehe davon aus, dass die Nachrichtendienste ihren Wissensvorsprung in der Kryptographie mittlerweile verloren haben. Ein gewisser Ressourcenvorsprung zum Brechen durch „brute force" dürfte unverändert bestehen, wird aber in Empfehlungen für Schlüssellängen berücksichtigt.[29, 30]

Die intensive öffentliche Forschung in der Kryptographie hat dazu geführt, dass veröffentlichte Verfahren meist sehr schnell und gründlich analysiert werden. Dies gilt insbesondere für Verfahren, die für einen baldigen Einsatz gedacht sind, da hier die Chancen, eine erfolgreiche Analyse zu publizieren, sehr hoch sind. Akademische Forscher sind sehr stark durch Publikationen motiviert. Geheim gehaltene Verfahren, wie sie nach wie vor in manchen Sektoren verwendet werden, unterliegen nicht diesem Sicherheitstest durch die Fachöffentlichkeit. Die Nutzer solcher geheimer Verfahren gehen dadurch meines Erachtens ein hohes und völlig unnötiges Risiko ein.[31]

Für die Praxis müssen kryptographische Verfahren in internationale Standards übersetzt werden. Diese Standardisierung erfolgt primär durch das „National Institute of Standards and Technology" (NIST) in den USA und die „Internet Engineering Task Force" (IETF). Beide verfolgen im Prinzip eine Politik der offenen Prozesse. Die Grundalgorithmen AES und SHA3 wurden von NIST in offenen Wettbewerben bestimmt (in beiden Fällen gewannen europäische Forscherteams). Trotz aller Offenheit hat dieser Prozess aber gravierende Schwächen: Zum einen erstreckt sich der Prozess selten auf alle Details eines Standards, und auch kleine Details können in der Sicherheit eine große Rolle spielen. Zum anderen werden Standardisierungsprozesse immer von einzelnen Menschen getrieben, im Fall von Kryptographiestandards meist von Vertretern amerikanischer Firmen und Behörden. Dieser Umstand erlaubte es der NSA beispielsweise, über die dominierend aktive Arbeit in einer NIST-Arbeitsgruppe einen Pseudozufallszahlengenerator mit Hintertür standardisieren zu lassen.[32]

Grundverfahren wie RSA, AES und Protokolle wie SSL/TLS gelten in der Kryptographie derzeit als algorithmisch sicher, ausreichend gute und lange Schlüssel vorausgesetzt.[29] Umgekehrt gelten Grundverfahren mit kurzen Schlüsseln, z. B. 40 Bit oder 64 Bit, als unsicher oder zumindest sehr zweifelhaft.

Während die Internetkommunikation mit SSL/TLS zumindest auf algorithmischer Ebene gut gesichert werden kann, werden in der Mobil- und Satellitenkommunikation mit A5/1 bzw. A5-GMR-1 und A5-GMR-2 häufig Verschlüsselungsverfahren eingesetzt, die bereits gebrochen sind und keinen signifikanten Schutz bieten, weder gegen Einzel- noch gegen Massenüberwachung.[33, 34] Für den Nachfolger von A5/1, A5/3, sind noch keine praktischen Angriffe bekannt, wohl aber theoretische Analysen.[35] Mit einer effektiven Schlüssellänge von 64 Bit gilt A5/3 als unterdimensioniert. Eine Umstellung von Algorithmen ist in der Mobil- und Satellitenkommunikation relativ aufwändig, da die Hardware von Basisstationen und Satelliten geändert werden muss.

Ebene der Vertrauensinfrastrukturen

Fast alle Anwendungen der Kryptographie benötigen eine Vertrauensinfrastruktur: Zu Beginn einer Kommunikationsbeziehung müssen Sender und Empfänger sich irgendwie darauf einigen, welche Schlüssel verwendet werden sollen. Andernfalls ist eine geschützte Kommunikation unmöglich. Kennen sich die beiden noch nicht, brauchen sie dazu die Hilfe einer „Trusted Third Party“ (TTP), eines vertrauenswürdigen Dritten, z. B. einer „Certificate Authority“ (CA) oder eines „Kerberos Servers“.

Kooperiert die gewählte TTP mit dem Angreifer oder wird von diesem korrumpiert, so bricht der Schutz zusammen.[36, 37] Der Angreifer kann dann die Identität des beabsichtigten Kommunikationspartners übernehmen und sich als „Man in the Middle“ unbemerkt in die Kommunikation einklinken. Ähnliche Mechanismen sind in den Snowden-Dokumenten als Teil des Programms BULLRUN angedeutet und für die Einzelüberwachung geeignet.

Im Fall von SSL/TLS im Web (also wenn man Webseiten mit „https://...“ anspricht) übernimmt faktisch der Browser-Hersteller die Entscheidung, welche TTPs als vertrauenswürdig eingestuft sind. Die entsprechende Liste ist in allen gängigen Browsern voreingestellt, und die meisten der z. B. in Firefox voreingestellten derzeit 394 TTPs dürften dem normalen Endnutzer völlig unbekannt sein.[38] Der Endnutzer kann sich zwar die Details der gewählten TTP anzeigen lassen, im Allgemeinen wird er dies aber nicht tun, und falls doch, wird ihm die Information vermutlich sehr wenig sagen. Dieser Ansatz ist damit höchstens so sicher wie die unsicherste der jeweils zugelassenen TTPs. Die Verbesserung dieser Situation wird derzeit intensiv in Forschung und Entwicklung diskutiert.[39]

Im Fall von E-Mail stellt sich den meisten Endnutzern die Frage, welche TTP man verwenden will, überhaupt nicht: Es steht keine zur Auswahl. Mit S/MIME und OpenPGP gibt es zwar Standards zur E-Mail-Verschlüsselung. Aber es existiert keine Vertrauensinfrastruktur, die einen signifikanten Teil der Internetnutzer auch nur Deutschlands abdecken würde.[40]

Die meisten Endnutzer müssen also akzeptieren, dass ihre Nachrichten auf den Servern der E-Mail-Anbieter im Klartext liegen und dort prinzipiell für den E-Mail-Anbieter und für Dritte zugreifbar sind. Das in den Snowden-Dokumenten beschriebene Programm PRISM legt nahe, dass bei manchen US-amerikanischen E-Mail-Anbietern die NSA dies auch zur Massenüberwachung nutzt. Die mittlerweile übliche Verschlüsselung zwischen E-Mail-Servern mittels SSL/TLS schützt lediglich davor, dass E-Mails auf den Leitungen abgehört werden, verhindert aber nicht den Zugriff direkt auf den Servern.

Ebene der Implementierung und Anwendung

Implementierungsnahe Schwachstellen stellen vermutlich das größte Risiko beim Einsatz von Kryptographie dar. Kryptographie muss, wie alle Algorithmen, letztlich in Software und Hardware implementiert, in größere Systeme integriert und dann vom Endnutzer korrekt verwendet werden. All dies sind sehr fehleranfällige Aufgaben, aus denen sich immer wieder Angriffsmöglichkeiten ergeben. Die Implementierung von Kryptographie ist dabei besonders anspruchsvoll und dementsprechend auch besonders fehleranfällig.

Zahlreiche Implementierungen von Kryptographie existieren. Gängige Betriebssysteme enthalten typischerweise wenigstens eine Bibliothek kryptographischer Algorithmen. Für SSL/TLS gibt es mehrere Open-Source-Implementierungen mit OpenSSL als Marktführer. Implementierungen existieren auch für S/MIME, das zudem von vielen E-Mail-Programmen auch direkt unterstützt wird, von OpenPGP, SSH und anderen.

Ein neueres Beispiel für einen technisch trivialen, aber in der Auswirkung fatalen Implementierungsfehler ist der „Heartbleed Bug“ in OpenSSL.[41] Dieses Beispiel zeigte auch, dass „Open Source“ alleine nicht zu mehr Sicherheit führt, sondern auch bei Open-Source-Projekten aktiv an der Qualitätssicherung (Entwicklungsprozesse, automatisiertes Testen, Code Reviews) gearbeitet werden muss. Im Allgemeinen setzt dies eine Finanzierung durch die Nutzer (Industrie, Staat, Crowdfunding) des Projektes voraus. (Im Gegensatz dazu erfolgt die Qualitätssicherung auf der Ebene der Algorithmen durchaus von alleine, wie erwähnt. Hier genügt anscheinend die wissenschaftliche Motivation, algorithmische Schwachstellen und Angriffe publizieren zu können.)

Allgemein sind für SSL/TLS eine ganze Reihe von implementierungsnahen Schwachstellen und Angriffen bekannt,[42] und ähnliche Mechanismen sind in den Snowden-Dokumenten als Teil des Programms BULLRUN angedeutet.

Zusammenfassung

Generell darf man davon ausgehen, dass NSA und GCHQ keinen Wissensvorsprung in der Kryptographie besitzen und auf der algorithmischen Ebene daher weniger Überraschungen drohen. Die heutige Praxis der Standardisierung gibt jedoch insbesondere der NSA sehr viel Einfluss und damit die Möglichkeit, Hintertüren in Standards zu platzieren. Dieser Einfluss muss durch ein stärkeres Europäisches Engagement ausgeglichen werden.

Die Snowden-Dokumente erwähnen, NSA und GCHQ seien in der Lage, insbesondere SSL/TLS zu entschlüsseln. Die technischen Details deuten an, dass hier Angriffe auf die Vertrauensinfrastruktur (gefälschte Zertifikate, gestohlene geheime Schlüssel) und das Ausnutzen von Schwachstellen oder Hintertüren in Implementierungen zum Tragen kommen. Diese Angriffe sind auf Einzelüberwachungen gerichtet.

Festzuhalten bleibt, dass eine durchgängige Ende-zu-Ende-Verschlüsselung, selbst wenn sie nur auf einer vergleichsweise schwachen Vertrauensinfrastruktur aufbaut, einen sehr effektiven Schutz gegen Massenüberwachung darstellen würde. Der Aufwand, eine einzelne weitere Person zu überwachen, würde dadurch zumindest etwas steigen. Aufgrund des Skaleneffektes würde dies genügen, die ökonomische Basis der Massenüberwachung zu zerstören.

4.2 Anonymität im Internet

Das Schutzziel Vertraulichkeit der Kommunikation bezieht sich einerseits auf die Inhaltsdaten und andererseits auf die Metadaten, also z. B. wer wann mit wem wie lange kommuniziert, aber auch auf technische und für die Abrechnung notwendige Daten wie Datenmenge, Bandbreite und Standortdaten.

Verschlüsselung schützt in der Regel nur die Inhaltsdaten. Bei SSL/TLS sind z. B. die Endpunkte, Zeiten und der Umfang der Kommunikation sichtbar. Dasselbe gilt bei den im Telefonverkehr üblichen Verbindungsdaten. Bei Ende-zu-Ende verschlüsselter E-Mails sind Sender und Empfänger E-Mail-Adressen, Größe der Email und selbst die Betreffzeile offen lesbar.[43] Diese Metadaten geben Aufschluss über die sozialen Beziehungen von Menschen und Organisationen, woraus sich wiederum Rückschlüsse über Interessen, Vorlieben und Absichten ziehen lassen. Über „Big Data“ Algorithmen lassen sich massenhaft gesammelte Metadaten sehr schnell analysieren und filtern. Metadaten gelten prinzipiell als aussagekräftig und daher schützenswert.

Das Problem der Metadaten im Internet wird spätestens seit den 1980er-Jahren diskutiert.[44, 45]

Die Metadaten, die bei der Nutzung von relativ statischen Datenbanken – etwa Wikipedia, Tageszeitungen – entstehen, kann man leicht dadurch anonymisieren, dass den Nutzern eine komplette Kopie der Datenbanken – die ganze

Wikipedia, die ganze Tageszeitung – übergeben wird. Die Auswahl erfolgt lokal beim Nutzer, die genauen Interessen und das Verhalten des Nutzers bleiben verborgen. Diesem Ansatz sind natürlich enge praktische Grenzen gesetzt, er zeigt aber, dass oftmals sehr einfach Lösungen existieren.

Anonymisierungsdienste im engeren Sinne sind Dienste, die die Kommunikationsbeziehungen zwischen Internetnutzern verbergen. Statt direkt miteinander zu kommunizieren, tauschen die Kommunikationspartner ihre Nachrichten über bestimmte Server aus. Die Kommunikation zwischen den Teilnehmern und diesen Servern wird verschlüsselt (z. B. mit SSL/TLS). Wird ein Server von sehr vielen Teilnehmern verwendet, so sollte einem Außenstehenden verborgen bleiben, welche beim Server eingehende Nachricht zu welcher ausgehenden gehört, und das Ziel der Anonymisierung wäre dann erreicht.

Die einfachste Variante dieses Dienstes sind „Web Proxies", also einzelne Server, die als „Proxy" Anfragen an Web-Server im Auftrag weiterleiten und die Antwort entsprechend zurückschicken. Die erreichte Anonymität ist allerdings sehr schwach. Die Nutzer müssen dem Proxy vollständig vertrauen, und über den engen zeitlichen Zusammenhang zwischen ein- und ausgehenden Nachrichten kann ein Angreifer, der beispielsweise mit dem ISP des Proxy kooperiert, leicht Rückschlüsse auf die Sender-Empfänger-Beziehung gewinnen.[46] Üblicherweise dienen „Web Proxies" allerdings auch weniger der Anonymisierung als der Umgehung von Zensur und regionalen Zugangsbeschränkungen.

Eine verbesserte Variante dieser Idee wird beispielsweise in „Tor"[47] und dem in Deutschland entwickelten „JonDo"[48] verwendet:[44] Es werden mehrere Proxies, „Mixe" genannt, so hintereinander geschaltet, dass im Prinzip alle Mixe zusammenarbeiten müssten, um eine Nachricht vom Sender zum Empfänger zu verfolgen. Statt allen Mixen zu vertrauen, genügt es also, wenn wenigstens einer der Mixe tatsächlich vertrauenswürdig ist. Die Mixe sollen daher möglichst von unterschiedlichen Organisationen, in unterschiedlichen Ländern und mit unterschiedlichen IT-Systemen betrieben werden.

Die genannten Dienste sind technisch stabil und benutzbar, aber nicht darauf ausgelegt, einen signifikanten Teil des Internetverkehrs zu übernehmen. Hinzu kommt eine Reihe von praktischen Problemen, die gelöst werden müssen: „Die Installation und Verwendung ist relativ kompliziert. Die spezielle Architektur der Systeme ist für Kommunikation mit hohen Anforderungen an Bandbreite und Verzögerungszeiten – wie etwa bei VoIP oder Videoanwendungen – wenig geeignet. Der Zugriff auf Web-Seiten mit eingebetteten dynamischen Inhalten ist problematisch. Eine echte Integration mit anderen Kommunikationsdiensten wird meist nicht unterstützt. Zudem lassen sich diese Dienste relativ leicht durch die Netzbetreiber blockieren."[zitiert nach 40]

„Ein weiteres Problem besteht darin, dass die genannten Dienste unter der Annahme entworfen wurden, eine umfassende Überwachung der Kommunikation sei unmöglich. Andernfalls existieren Korrelationsangriffe, mit denen ein Angreifer statistisch erkennen kann, wer mit wem kommuniziert. Die Überwachungsprogramme von NSA und GCHQ lassen diese Annahme in neuem Licht erscheinen."[zitiert nach 40, 49]

Hinzu kommt, dass Tor und JonDo spezielle Client-Software benötigen und diese im Prinzip Schwachstellen und Hintertüren enthalten könnte. In diesem Zusammenhang wird oft darauf verwiesen, dass Tor aus einem Projekt des „U.S. Naval Research Laboratory" hervorgegangen ist. Konkrete Hinweise auf Hintertüren sind aber nicht bekannt, und das heutige Entwicklerteam von Tor gilt als unabhängig. JonDo geht zurück auf das Projekt „AN.ON", das seit 2000 mit Mitteln der DFG und des BMWi gefördert wurde.

Zusammenfassung

Zusammenfassend kann man feststellen, dass Systeme wie Tor und JonDo einen eher mäßigen Schutz gegenüber Nachrichtendiensten wie NSA und GCHQ darstellen. Ein breiter Einsatz könnte eine massenhafte Erfassung von Metadaten zwar stark erschweren, scheitert aber noch an der mangelnden Leistungsfähigkeit und Einsatzbreite der Systeme. Ein gezielter Einsatz für manche Dienste ist möglich und

sinnvoll, kann einem gezielten Angriff durch einen Nachrichtendienst aber kaum standhalten.

4.3 Sichere Dienste und „Cloud Computing“

Die IT-Dienstleistungen in einem Unternehmen oder einer Behörde bestehen aus einer Reihe von Servern, die Speicher und Rechenleistung zur Verfügung stellen, und darauf laufenden Anwendungen. Durch „Cloud Computing“ kann ein im Prinzip beliebig großer Teil dieser IT-Dienstleistungen durch einen Dritten, den „Cloud Provider“, erbracht werden. Realer Speicher wird durch Cloud Speicher ersetzt, reale Maschinen durch virtuelle Maschinen. Vormals lokale Anwendungen werden auf diese virtuelle Infrastruktur migriert oder durch standardisierte Cloud-Angebote ersetzt. Durch Spezialisierung, Standardisierung und Skaleneffekte entstehen Kosteneinsparungen, die dieses Modell für beide Seiten, Cloud Provider und Cloud Nutzer, ökonomisch attraktiv machen.

Nach heutigem Stand der Technik hat ein Cloud Provider vollen Zugriff auf alle bei ihm gespeicherten oder verarbeiteten Daten. Prinzipiell sind diese Daten ein inhaltlich sehr wertvolles Ziel sowohl für die Massenüberwachung (z. B. durch die Analyse von E-Mails, Text-Dokumenten, Bildern usw.) als auch für gezielte Angriffe (z. B. auf einen Software-Hersteller, der in der Cloud das nächste Produkt entwickelt oder testet).

Daten, die in der Cloud nur gespeichert, aber nicht verarbeitet werden, können im Prinzip durch Verschlüsselung vor dem Zugriff durch den Cloud-Provider geschützt werden. Entsprechende Angebote und Entwicklungen existieren bereits, werden allerdings in der Praxis nicht breit eingesetzt. Der Schutz von Daten während der Verarbeitung vor dem Cloud-Provider ist noch Gegenstand der Forschung.[40]

4.4 System- und Softwaresicherheit

Die digitale Überwachung Einzelner oder großer Gruppen beruht zu einem erheblichen Teil auf der mangelhaften Sicherheit der heutigen Informationstechnologie. Das Internet ist vergleichsweise einfach abhörbar (Abschnitt 2), Rechner – Server, PCs, Smartphones, Smart TVs, intelligente Autos usw. – sind vergleichsweise einfach korrumpierbar.

Kommunikation ließe sich mit richtig entworfener und umgesetzter Ende-zu-Ende-Verschlüsselung gegen Abhören der Inhaltsdaten absichern. Fehlerfreie und für den Endnutzer gut bedienbare Hardware, Betriebssysteme und Anwendungen wären gegen die heute üblichen Angriffe weitestgehend immun. Die umfassende und überzeugende Kontrolle des Herstellungs- und Betreiberprozesses könnte den Einbau von Hintertüren bei Herstellern und Anbietern von Cloud-Diensten massiv erschweren.

Die heutige Informationstechnologie ist von diesem Zustand jedoch weit entfernt. Laut „BITKOM“ haben 39 % der Unternehmen und mehr als die Hälfte der Privatnutzer in Deutschland bereits Angriffe auf ihre Systeme erlebt.[50] Laut „Corporate Trust“ waren 54 % aller Unternehmen nachweislich oder vermutlich Opfer von Wirtschaftsspionage.[51]

Angreifer auf die IT kombinieren meist verschiedene Elemente zu komplexeren Angriffen. Für sehr komplexe Angriffe, bei denen oft mehrere Opfer angegriffen werden, um den eigentlichen, letzten Angriff durchzuführen, hat sich der Begriff „Advanced Persistent Threat“ (APT) eingebürgert. Viele der in den Snowden-Dokumenten beschriebenen Programme sind technisch gesehen APTs. Ausgenutzt werden meist vier Typen von Gefahren.

Gefahr 1: Innentäter

Angriffe involvieren sehr häufig Innentäter, also Nutzer, die rechtmäßig einen privilegierten Zugriff auf das angegriffene IT-System haben, z. B. als Administrator. „Corporate Trust“ schätzt, dass mehr als die Hälfte aller Fälle von Wirtschaftsspionage durch Innentäter ermöglicht wurde. Organisatorische Regeln wie das Vier-Augen-Prinzip oder Rollen-Konzepte und deren Durchsetzung durch IT können das Problem lindern. Verhindern kann man solche Angriffe jedoch letztlich nicht, man kann sie höchstens mithilfe entsprechender Überwachungssysteme erkennen.

Gefahr 2: „Social Engineering"

Eine weitere Gefahr droht durch „Social Engineering", also das Ausnutzen menschlicher Schwächen und Eigenschaften. „Corporate Trust" schätzt, dass dies in etwa einem Viertel aller Wirtschaftsspionagefälle eine Rolle spielt. Nutzer verraten etwa ihr Passwort einem vermeintlichen Administrator am Telefon; sie öffnen E-Mail-Anhänge von vermeintlich vertrauenswürdigen Sendern und führen damit Schadcode aus; sie ignorieren Sicherheitsrichtlinien und speichern vertrauliche Daten in öffentlichen Clouds; oder sie speichern alle persönlichen Daten, die man zum Zurücksetzen ihrer Passwörter braucht, in ihrem Facebook-Profil ab. Als Maßnahme gegen „Social Engineering" werden meist Aufklärung und Schulung angeführt. Mindestens genauso wichtig ist jedoch die Verbesserung der Nutzbarkeit („Usability") von Informationstechnologie. Statt den Menschen an die IT anpassen zu wollen, ist es die Aufgabe der Informatikforschung, menschentaugliche Sicherheitstechnologien zu entwickeln.

Gefahr 3: Schwachstellen, „Vulnerabilities"

Die dritte Gefahr droht durch Schwachstellen, „Vulnerabilities", also Entwurfs-, Programmier- und Konfigurationsfehler in Systemen und Software. Erfahrungsgemäß verbergen sich in großen Softwarepaketen (z. B. Betriebssystemen, Verwaltungssystemen, Datenbanken) hunderte bis tausende Fehler, die für Angriffe ausgenutzt werden können. Die meisten davon sind unbekannt, können aber im Prinzip jederzeit von Angreifern gefunden und ausgenutzt werden.

Wird eine dem Hersteller und Anwender unbekannte Schwachstelle ausgenutzt, so spricht man von einer „Zero-Day Vulnerabillity". Offensichtlich sind diese für die Endnutzer besonders gefährlich. Die NSA hat indirekt bestätigt, dass sie solche Schwachstellen sammelt und unter Umständen auch nutzt.[52] Diese Praxis gilt in der IT-Branche, Wirtschaft wie Wissenschaft, als höchst gefährlich, da sie alle Endnutzer der entsprechenden Systeme gefährdet. Kennt die NSA eine Schwachstelle, so muss man davon ausgehen, dass auch andere Organisationen diese kennen oder finden. Viele IT-Hersteller lehnen die Meldung von Schwachstellen an staatliche Stellen ab, da sie einen Missbrauch der gemeldeten Schwachstellen fürchten.

Für das Finden von Schwachstellen hat sich eine eigene Forschungsgemeinschaft herausgebildet, die sich regelmäßig auf Konferenzen wie „BlackHat" und „DefCon" trifft. Wettbewerbe wie „Pwn2Own" zeigen, dass ungeschützte Standardsysteme oftmals innerhalb von Minuten korrumpierbar sind. In einem kontrollierten Feldversuch demonstrierte Felix Lindner, wie er innerhalb von nur zwei Tagen in das auf übliche Weise abgesicherte System der Stadtwerke Ettlingen eindringen konnte.[53]

Gefahr 4: Gezielte Angriffe auf Komponenten und Lieferketten

Sehr mächtige Angreifer verfügen über die Möglichkeit, physisch in die Herstellungs- und Lieferketten von Informationstechnologie einzugreifen.

„Trojanische Pferde" in Hardware und Software können mit Kooperation der Hersteller schon während der Herstellung eingebaut werden und sind dann, insbesondere in Hardware, kaum zu finden.

Durch spezielle Maßnahmen – etwa wie im Katalog der „Tailored Access Operations" (TAO) der NSA beschrieben[54] – können diese auch während oder nach der Auslieferung und ohne Kooperation der Hersteller eingebaut werden. Hersteller können ihre Systeme gegen solche Manipulationen in Grenzen absichern (etwa durch digitales Signieren aller Softwarekomponenten und Einsatz von Trusted Computing Technologie). Gegen einen Angreifer, der zu einem physischen Angriff bereit ist, kann es aber letztlich keinen Schutz geben.

Gründe für mangelhafte Cybersicherheit

Die scheinbar inhärente Unsicherheit heutiger Informationstechnologie wird oft wie ein Naturgesetz dargestellt. Tatsächlich ist der heutige Zustand einfach das Resultat der Entwicklung der Informationstechnologie. Das Internet und die Grundprinzipien moderner Computer entstanden Mitte des 20. Jahrhunderts. Die Komplexität von Hard- und Software ist seither dramatisch angestiegen. Aus vormals isoliert aufgestellten und dementsprechend

recht gut zu sichernden Großrechnern wurden global vernetzte Computer und „smart things". Während Unternehmen ihre IT-Dienste früher aus dem eigenen Rechenzentrum bezogen und Endnutzer ihre Daten auf der eigenen Festplatte ablegten, ist das Modell der Zukunft die Cloud. Die IT-Systeme sind dort nur noch virtuell einem Unternehmen oder einem privaten Nutzer zugeordnet, die realen IT-Systeme in den Cloud-Rechenzentren werden von allen Nutzern gemeinsam genutzt. Eine klare Grenze zwischen den eigenen und allen anderen IT-Systemen ist nicht mehr festzustellen. Genau auf der Existenz einer solchen Grenze beruhten aber die meisten der bislang üblichen, vorwiegend reaktiven Ansätze zur IT-Sicherheit.

Strategie für bessere Cybersicherheit

Eine technische Strategie für Cybersicherheit hat stets einen reaktiven und einen proaktiven Teil.

Der reaktive Teil sorgt dafür, dass Angriffe an einer passenden „Grenze" erkannt und zumindest teilweise blockiert werden können. „Firewalls", „Anti-Virus", „Intrusion Detection", „Anomaly Detection" usw. erkennen bekannte Angriffsmuster und eigenartiges Verhalten, also Anomalien, und erzeugen Alarme. Manche Alarme können automatisiert behandelt werden (z. B. werden bekannte Viren gelöscht oder zumindest nicht ausgeführt). „Patches" von Software beseitigen erkannte Schwachstellen, hoffentlich bevor sie durch Angreifer ausgenutzt wurden. Die reaktive Sicherheit funktioniert gut gegenüber bekannten Angriffen. Unbekannte Angriffe eines sehr fähigen Angreifers sind jedoch schwer zu erkennen und zu stoppen.

Der proaktive Teil sorgt dafür, dass durch geeignete Entwurfs-, Produktions- und Managementprozesse erst gar keine Schwachstellen entstehen, die für Angriffe ausgenutzt werden können. Sofern man Schwachstellen nicht vermeiden kann, sollen diese zumindest vor Auslieferung an den Anwender gefunden oder durch geeignete, mehrschichtige Schutzkonzepte maskiert werden. Dieser Ansatz ist insbesondere in Europa unter dem Namen „Security by Design" bekannt und wird intensiv in dem vom BMBF geförderten Kompetenzzentren für Cybersicherheitsforschung EC SPRIDE erforscht.[55]

Ursprünglich verfolgte man in der IT-Sicherheit vorwiegend proaktive Ansätze. Der rasanten allgemeinen Entwicklung der Informationstechnologie konnte jedoch die IT-Sicherheit zunächst nicht folgen; Forschung und die IT-Sicherheitsbranche konzentrierten sich seit den 1980er-Jahren auf die reaktive Sicherheit. Seit etwa 10 Jahren, ungefähr mit dem Start des „Trustworthy Computing" Programms von Microsoft, hat sich die Erkenntnis durchgesetzt, dass man beide Ansätze kombinieren muss. Studien zeigen, dass die proaktive Vermeidung von Schwachstellen um ein bis zwei Größenordnungen kostengünstiger ist als die reaktive Abwehr, wodurch sich auch in der Wirtschaft ein wachsender Fokus auf proaktive Sicherheit herausbildet. Die seit 2011 vom BMBF geförderten Kompetenzzentren für Cybersicherheitsforschung in Darmstadt, Karlsruhe und Saarbrücken vertreten in sehr prominenter Weise diesen Ansatz.

In Fachkreisen wird vermutet, dass sich ca. 80 % aller Angriffe durch den Einsatz von Standardtechniken bei Entwurf und Betrieb hätten vermeiden lassen (z. B. die Verwendung von E-Mail-Verschlüsselung, den Einsatz bekannter Verfahren zum Testen von Software auf Schwachstellen). Sowohl in der Wirtschaft als auch im privaten Bereich herrscht also ein sehr großer Nachholbedarf. Auch wenn Angreifer für viele der dann geschlossenen Lücken Ersatz fänden, könnte man das Sicherheitsniveau doch deutlich verbessern.

Das ultimative Ziel der Sicherheitsforschung ist, unbedingt sichere Systeme zu entwickeln. Hierzu gibt es eine Reihe von Initiativen, die sich diesem Ziel annähern wollen. Drei davon seien beispielhaft genannt:

- Einen sehr pragmatischen und vielversprechenden Ansatz verfolgen die Entwickler des Mikrokernsystems „L4", für das sich eine Reihe von Sicherheitseigenschaften mathematisch beweisen lässt und das den Aufbau einfacher, sicherer Plattformen erlaubt.[56, 57] L4 wurde ursprünglich in Deutschland entwickelt, liegt als Open Source vor und wird in einer Reihe von Produkten deutscher und anderer Hersteller genutzt.
- Einen anderen, umfassenderen Ansatz für eine sichere Plattform verfolgt das System

„SGX“ von Intel, mit dem sich in der Cloud isolierte Rechnerumgebungen realisieren lassen sollen.[58] SGX liegt allerdings noch nicht vor und Intel wird die Details der Implementierung vermutlich nicht für eine öffentliche Überprüfung freigeben.

- Einen radikalen Neuanfang auf Hardware- und Software-Ebene verfolgt der „Clean-slate“ Ansatz, der mit Finanzierung durch DARPA und Google prominent von SRI International (USA) und Univ. of Cambridge (UK) verfolgt wird.[59, 60] Dieser Ansatz ist wissenschaftlich sehr vielversprechend und wird öffentlich entwickelt, ist von einer Umsetzung in Produkten aber noch sehr weit entfernt.

Zusammenfassung

Viele der in den Snowden-Dokumenten beschriebenen Programme nutzen die mangelhafte System- und Softwaresicherheit von Informationstechnologie aus.

Möchte ein Nachrichtendienst wie die NSA oder eine ähnlich gut ausgestattete Organisation einen einzelnen Internet-Nutzer überwachen und ist auch zu physischen Manipulation an der IT bereit, so wird man sie durch informationstechnische Maßnahmen alleine nicht daran hindern können.

Dennoch rentiert sich eine Verbesserung der IT-Sicherheit. Zum einen sollte man über die Sorge um die nachrichtendienstliche Überwachung nicht die vielen anderen Angriffe übersehen, denen Internet-Nutzer heute ausgesetzt sind. Zum anderen erhöhen sinnvolle Verbesserungen stets den Aufwand für den Angreifer. Konsequente Ende-zu-Ende-Verschlüsselung erhöht den Aufwand je Opfer und macht so die Massenüberwachung unbezahlbar. Bessere Systemsicherheit kann Angriffe wie im ANT-Katalog beschrieben zwar nicht verhindern, aber verteuern und so dafür sorgen, dass diese Art der Überwachung nur in Einzelfällen zum Tragen kommen kann.

5. EMPFEHLUNGEN

Gegenüber Angreifern mit fast unbegrenzten Möglichkeiten ist perfekte Sicherheit nicht erreichbar. Diese durchaus wahre Erkenntnis hat oft einen paralysierenden Effekt – die Lage wird als hoffnungslos betrachtet. Dies ist aber ein gefährlicher Trugschluss. Auch die Budgets der mächtigsten Angreifer sind begrenzt, und selbst kleine Verbesserungen der Sicherheit können die Kosten für einen Angreifer so weit erhöhen, dass der Angriff nicht mehr finanzierbar ist oder sich zumindest im Vergleich zum Nutzen nicht mehr lohnt.[61]

Dies gilt insbesondere für Massenangriffe. Solche Angriffe setzen voraus, dass nach einer Anfangsinvestition die Angriffskosten für jeden zusätzlich Anzugreifenden praktisch „Null“ sind. Schon kleine Sicherheitsverbesserungen können diese Kosten leicht erhöhen und damit so viel „Sand“ in das Getriebe der Angreifer streuen, dass die Angriffskosten explodieren.

Dieser Abschnitt formuliert eine Reihe von Empfehlungen, insbesondere für Bundestag und Bundesregierung, die praktisch umsetzbar sind und das aktuelle Sicherheitsniveau deutlich erhöhen würden.

5.1 Vertrauliche Ende-zu-Ende-Kommunikation

Empfehlung: **Gesetzgeber und Regierung sollten den Aufbau und den Betrieb Ende-zu-Ende-gesicherter Kommunikationsdienste aktiv fördern. Betreiber von Kommunikationsdiensten sollten dazu verpflichtet werden, entsprechende Angebote zu schaffen. Die dafür erforderlichen Infrastrukturen sollten wie z. B. das Straßennetz als öffentliche Infrastrukturen betrachtet und gefördert werden.**

Die Entwicklung der Kommunikationstechnik hat dazu geführt, dass heute ein bunter Strauß von Kommunikationstechnologien nebeneinander existiert. Die Digitalisierung von Nachrichten und die Anwendung von Digitaltechnik zur Nachrichtenübertragung ermöglichen es, dass beliebige Inhalte mittels verschiedener Netzwerktechnologien übertragen werden können. Der Ausbau der Kommunikationsnetze in den vergangenen Jahren mit ihren hohen Transportkapazitäten in den Anschluss- und Weitverkehrsbereichen und die Möglichkeit der Verbindung von verschiedenen Netzen zu einem Netz haben dazu geführt, dass eine

Nachricht bei ihrer Übertragung zwischen Sender und Empfänger durch verschiedene Netze mit unterschiedlichen Netzwerk- und Übertragungstechnologien geleitet wird. Verschiedene Nachrichten zwischen denselben Kommunikationspartnern können darüber hinaus über verschiedene Wege versendet werden, wobei hier sowohl Übertragungsressourcen verschiedener Betreiber wie auch verschiedene geographische Wege in Anspruch genommen werden können (s. Abschnitt 2).

Durch die Integration von verschiedenen Kommunikationsdiensten und Anwendungen in modernen Netzen werden heute z. B. synchrone Kommunikation wie Sprachtelefonie und asynchrone Kommunikation wie E-Mail über die selben Kommunikationsnetze versendet. Auf dem Weg zwischen Sender und Empfänger können je nach benötigter bzw. verfügbarer Kommunikationsressourcen unterschiedliche Technologien und Routen verwendet werden (z. B. Glasfaser, Richtfunk, Satellitenfunk), was hinsichtlich der Angreifbarkeit und des Gefährdungspotenzials unterschiedliche Implikationen mit sich bringt. So können Angreifer beispielsweise auf bestimmte Knoten einfacher zugreifen als auf andere, wenn diese sich außerhalb ihres Zugriffsbereichs befinden. Darüber hinaus bringen bestimmte Netze bzw. Übertragungstechnologien bereits standardmäßig Funktionen zur Verschlüsselung auf bestimmten Übertragungsstrecken (z. B. GSM-Kommunikation auf der Luftschnittstelle), wohingegen andere Übertragungsstrecken keine Schutzfunktionen bieten (z. B. der stationäre Teil des GSM-Netzes, die Sprachtelefonie im Festnetz). Sind Verschlüsselungsfunktionen in Netzwerkstandards enthalten, dann kann deren Einsatz optional sein (z. B. Internet Protocol v6). Werden Verschlüsselungsfunktionen in bestimmten Netzwerken standardmäßig verwendet, dann ist hier nochmal zu betrachten, ob die verwendeten Algorithmen hinreichend stark sind. Selbst wenn starke Verschlüsselungsfunktionen in bestimmten Netzstandards vorgesehen sind, dann können diese Sicherungen immer nur innerhalb dieser Netze gelten. Bei Übergängen zwischen verschiedenen Netzwerkstandards sind die Nachrichten an den Netzübergangsknoten vor dem Zugriff von solchen Akteuren ungeschützt, die sich Zugang zu den Netzknoten verschaffen können. Hinzu kommt, dass Angreifer auf die Auswahl von Wegen (Routing), entlang derer Nachrichten durch ein Netz geschickt werden, Einfluss nehmen können, so dass Nachrichten zwangsweise an den Knoten entlang geleitet werden, an denen sie einen geeigneten Zugriff haben.

Da die Nachrichten von Kommunikationsteilnehmern bei der Übertragung über Kommunikationsnetze durch die Netze also nicht hinreichend geschützt sind, sollte die Sicherung direkt bei Sender und Empfänger ansetzen und somit nicht den Sicherungsfunktionen eines Netzes überlassen werden. Deshalb ist eine Sicherung an den Endpunkten einer Kommunikationsbeziehung erforderlich, also Ende-zu-Ende. Die Nachrichten sollten vor der Übertragung vom Sender verschlüsselt und erst beim Empfänger entschlüsselt werden. Diese Sicherung der Daten muss unabhängig von den für die Übertragung verwendeten Netzen stattfinden.

Damit das gelingen kann, müssen entsprechende Verschlüsselungsfunktionen in verschiedene Kommunikationsanwendungen und -dienste (z. B. Sprachtelefonie, Datenkommunikation) integriert werden. Zusätzlich ist ein authentischer Austausch von Schlüsseln notwendig, wozu der Aufbau einer Infrastruktur („Public Key Infrastructure“, PKI) erforderlich ist.

Für die Einführung von sicherer Ende-zu-Ende-Kommunikation sollten die entsprechenden Infrastrukturen aufgebaut werden. Anbieter von Kommunikationsdienstleistungen sollten dazu verpflichtet werden, entsprechende Dienste in ihr Portfolio aufzunehmen.

Es sollte Aufgabe des Staates sein, die Bedingungen dafür zu schaffen, dass Ende-zu-Ende-gesicherte Kommunikationsdienste zur Verfügung stehen.

5.2 Sichere Nutzung von Diensten

Empfehlung: **Der Gesetzgeber und die Regierung sollten die Voraussetzungen dafür schaffen, dass sichere Dienste zur Verfügung stehen. Betreiber sollten verpflichtet werden, zu jedem Dienst stets auch die nach Stand der Technik sicherste Dienstnutzungsvariante anzubieten.**

IT-Leistungen wie Speicher, Rechenleistung und Software werden heute als Cloud-Dienste über das Internet angeboten. Solche Dienste haben für private wie auch gewerbliche Nutzer viele Vorteile, wie etwa Kostenreduktion, Zeit- und Effizienzgewinne. Aufgaben, die Nutzer ohne diese Dienste selbst erledigen müssten, können auf spezialisierte Anbieter verlagert werden. Dadurch können Nutzer sich besser auf ihre eigenen Aufgaben konzentrieren und müssen nicht spezielle IT-Kompetenzen aufbauen. Für die Wirtschaft bieten solche Dienste die Möglichkeit, die Investitionsrisiken zu reduzieren. Die kurzen Innovationszyklen in der IT-Branche führen zu einem andauernden Modernisierungsdruck, dem ein ebenso andauernder Druck zur Kostensenkung gegenübersteht.

Durch die Nutzung von Diensten kommt es zwangsläufig zu einer Auslagerung von Daten und Prozessen in die Cloud. Dadurch kommt es wiederum zu neuen Abhängigkeiten und Gefahren, sowohl für Unternehmen als auch für Privatpersonen. Dies gilt praktisch für alle Dienstmodelle, also unabhängig davon, welche konkreten IT-Ressourcen im Rahmen eines Dienstes genutzt werden. Auch wenn Daten bei der Übertragung zu einem Dienstanbieter geschützt sein mögen, so sind diese nach der Übertragung meist ungeschützt, so dass der Dienstanbieter oder andere Akteure, die sich Zugang auf die IT-Ressourcen von Dienstanbietern verschaffen können, Zugriff auf diese Daten haben. Wie im Rahmen der Berichterstattung bekannt wurde, konnten Geheimdienste auf Daten bei verschiedenen Diensten zugreifen.[62]

Die Lösung der IT-Sicherheitsprobleme im Cloud Computing ist daher von zentraler Bedeutung. Für Unternehmen wie für Privatpersonen ist es wichtig, dass die eigenen Daten vertraulich und gegen unerwünschte Veränderungen oder Verlust geschützt gespeichert und verarbeitet werden.

Um Privatpersonen und Unternehmen eine sichere Dienstnutzung zu ermöglichen, sind erforderlich:

- *Forschung und Entwicklung:* Zur Erforschung und Entwicklung sicherer Dienste sind entsprechende Fördermaßnahmen notwendig. Neue Technologien für sichere Dienste zur Nutzung unterschiedlicher Typen von IT-Ressourcen sollten entwickelt werden. Es sind Lösungen erforderlich, mit denen Betreiber sichere Dienstangebote schaffen können. Für Dienstangebote, die nicht sicher sind, sind Lösungen zu entwickeln, die Nutzer in Kombination mit bestehenden unsicheren Dienstangeboten verwenden können, um die Sicherheit dieser Dienste zu erhöhen.
- *Bereitstellung und Betrieb:* Unternehmen und Privatpersonen sollten sichere Dienste nutzen können. Es sollte sichergestellt werden, dass die an einen Dienst zur Speicherung oder Verarbeitung übergebenen Daten weder vom Dienstanbieter noch von anderen Parteien in Erfahrung gebracht werden können. Werden im Rahmen der Diensterbringung informationstechnische Ressourcen verwendet, die nicht sicher sind, dann sind technische Erweiterungen notwendig, mittels welcher die entsprechenden Sicherheitsziele erreicht werden können. Durch die Kombination mit einer entsprechenden technischen Erweiterung können Benutzer selbständig das Sicherheitsniveau für die Dienstnutzung erhöhen.

5.3 Verbesserung des Datenschutzes durch Technik

Empfehlung: **Um Massenüberwachung durch Unternehmen verhindern zu können, müssen Lösungen entwickelt werden, mittels derer der Fluss von Daten zu unberechtigten Dritten aktiv unterbunden werden kann. Der Gesetzgeber und die Regierung sollten die Entwicklung solcher Lösungen unterstützen und einen Rahmen schaffen, innerhalb dessen diese Lösungen angeboten bzw. als Infrastruktur aufgebaut und betrieben werden.**

Massenüberwachung wird heute nicht nur von Geheimdiensten betrieben. Viele technische Lösungen werden bewusst so entwickelt, dass sie Daten der Nutzer erfassen und sie ohne deren Kenntnis an Dritte weitergeben, mit denen Verbraucher weder willentlich noch bewusst in Verbindung treten. Bei den hierbei erfassten

Daten handelt es sich oftmals um Metadaten, welche den Empfängern Auskunft über Aktionen und das Verhalten von Nutzern geben und aus denen sich z. B. Gewohnheiten, Interessen, Vorlieben oder Aufenthaltsorte ableiten lassen.[24] Das Spektrum von Produkten und Anwendungen, die über entsprechende Funktionen verfügen, ist sehr breit. Hierzu zählen z. B.:

- Web-Anwendungen, bei denen mittels Web-Tracking im Hintergrund Informationen über aufgerufene Webseiten zu dritten Parteien fließen,
- Smartphone Apps, die per App-Tracking Informationen zur App-Nutzung oder andere Daten an Dritte versenden,
- Smart-TV, die Informationen über das Zuschauerverhalten an Dritte senden.

Die technischen Rahmenbedingungen zur Erfassung von Daten werden sich mit der fortschreitenden Einführung des „Internets der Dinge“ immer weiter entwickeln. Mit der Anwendung von Informationstechnologie in verschiedenen Geräten des täglichen Gebrauchs und deren Fähigkeit, Netzwerkverbindungen aufzubauen, werden immer mehr Informationen über Nutzer erfasst und versendet, so dass immer mehr personenbezogene Daten aggregiert werden.

Die im Hintergrund gewonnenen Daten zu Nutzern können miteinander in Beziehung gesetzt werden, so dass umfangreiche Datensammlungen entstehen, über die sich Profile von Personen bilden lassen. Diese Daten werden heute hauptsächlich für Marketingzwecke verwertet, jedoch ist ihre Verwertung nicht darauf beschränkt. Für die Betroffenen sind die möglichen Nachteile nicht abzusehen, die sich aus einer Verwertung dieser personenbezogenen Daten durch Dritte ergeben könnten.

Vor diesem Hintergrund muss es darum gehen, dass sich Nutzer entsprechend schützen können. Zur Eindämmung dieser Form der Massenüberwachung besteht ein großer Bedarf. Hierzu muss sichergestellt werden, dass Metadaten und Daten zur Dienstnutzung nicht von Dritten ohne informierte Zustimmung der Benutzer in Erfahrung gebracht werden können. Damit dies gelingen kann, müssen technische Schutzmechanismen geschaffen und angeboten werden. In Abhängigkeit der Daten, die gegenüber Dritten vertraulich bleiben sollen, müssen diese auf unterschiedlichen technischen Ebenen ansetzen:

- *Netzwerkebene:* Auf dieser Ebene geht es darum, dass Nutzer Metadaten zur Kommunikation wie z. B. Kommunikationspartner oder Zieladresse gegenüber Dritten geheim halten können. Hierzu ist der Aufbau und Betrieb einer Infrastruktur erforderlich, durch die entsprechende Metadaten gegenüber Dritten geschützt werden können, z. B. Anonymisierungsnetze (s. Abschnitt 4.2).
- *Anwendungsebene:* Auf Anwendungsebene sind Lösungen erforderlich, mit denen Nutzer sicherstellen können, dass keine Metadaten zu unberechtigten Dritten fließen können. Wenn Anwendungen versuchen, entsprechende Daten zu versenden, so sollen Schutzmechanismen auf Nutzerseite den Datenaustausch mit Dritten unterbinden.

Einige Lösungen auf Netzwerk- und Anwendungsebene existieren zwar bereits, jedoch müssen Nutzer die entsprechenden Komponenten heute zusätzlich installieren oder konfigurieren. Um eine benutzerfreundliche Lösung zu haben, sollten Schutzmechanismen einfacher zu nutzen sein, z. B. sollten sie möglichst standardmäßig voreingestellt sein. Für bestimmte Anwendungsbereiche sind hingegen noch keine Lösungen vorhanden, z. B. für die Unterbindung von Datenflüssen bei Smartphone-Apps. Hier sollte die Forschung und Entwicklung weiter vorangetrieben werden. Das Angebot von Lösungen auf der Netzwerkebene erfordert den Aufbau einer Infrastruktur, an deren Betrieb sich verschiedene Akteure beteiligen müssen. Werden zukünftig neue Produkte im Rahmen von neuen Anwendungen eingeführt, die ein Potenzial für neue Massenüberwachung haben, z. B. im Rahmen von Innovationen für das Internet der Dinge, dann sollten die entsprechenden Abwehrmaßnahmen frühzeitig entwickelt und zur Verfügung gestellt werden.

In diesem Zusammenhang ist ein spezielles Monitoring notwendig, um erkennen zu können, wann entsprechende Abwehrmaßnahmen erforderlich sind.

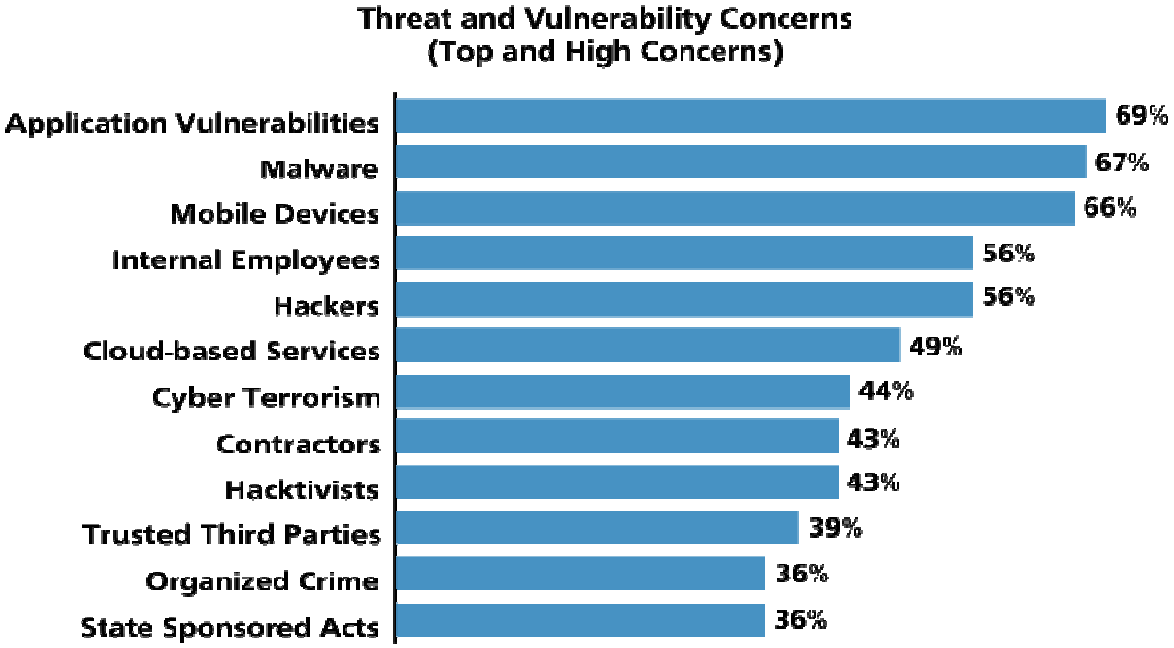
5.4 „Security and Privacy by Design“

Empfehlung: **Der Gesetzgeber und die Regierung sollten die Weiterentwicklung und Umsetzung des Paradigmas „Security and Privacy by Design“ in der IT-Industrie fördern. Dies sollte zunächst die Forschung zur Entwicklung entsprechender Werkzeuge und Prozesse umfassen. Forschungs- und Innovationsprojekte, in denen Informationstechnologie entwickelt oder angewendet wird, sollten verpflichtet werden, die Fragen der IT-Sicherheit in angemessenem Maße zu berücksichtigen.**

Die Sicherheit von Anwendungen und Systemen, die informationstechnische Komponenten verwenden, ist abhängig von der IT-Sicherheit informationstechnischer Komponenten. Dies gilt gleichermaßen für Komponenten aus Hardware und Software. Zur Absicherung von informationstechnischen Systemen mit ihren rein funktionalen Anwendungskomponenten wurden in den vergangenen Jahren oftmals dedizierte Sicherheitskomponenten verwendet, z. B. Wrapper oder Firewalls. Beim Entwurf und der Entwicklung der funktionalen Komponenten steht in der Regel die Funktion im Vordergrund, so dass Sicherheitsaspekte dort nicht oder nur unzureichend berücksichtigt werden. Das führt oftmals zu Sicherheitslücken in informationstechnischen Systemen, die sich durch zusätzliche Sicherheitskomponenten nicht schließen lassen. Häufig ist den für die Entwicklung der Sicherheitskomponenten verantwortlichen Sicherheitsexperten gar nicht bekannt, welche Sicherheitslücken in den funktionalen Komponenten enthalten sind. Sicherheitslücken in Produkten bleiben dann trotz aller Sicherheitskomponenten bestehen. Eine Folge dieser Praxis sind Angriffe auf Systeme und Anwendungen, wie sie inzwischen fast schon täglich den Nachrichtenmeldungen zu entnehmen sind. Weitere Folgen sind Bedrohungen und Risiken für Anwender bzw. die ganze Gesellschaft im Fall von kritischen Infrastrukturen sowie Reputationsverluste und hohe Kosten zur Beseitigung von Sicherheitslücken. Manche Sicherheitslücken in Software können durch Patches geschlossen werden, Sicherheitslücken in Hardware erzwingen jedoch den Austausch von Bauteilen.

Die Nichtberücksichtigung von IT-Sicherheit bei der Anwendungsentwicklung wird für die Sicherheit als kritischste Ursache eingeschätzt (Abbildung 4). Hinzu kommt, dass mehr

Abbildung 4: Quellen von IT-Sicherheitsbedrohungen[63]



als 90 % der Sicherheitslücken in Anwendungen hätten leicht vermieden werden können, da sie vom Typ her seit langer Zeit bekannt waren und zu ihrer Vermeidung genügend Wissen vorhanden ist. Diese Erkenntnis legt nahe, dass IT-Sicherheit bei der Entwicklung von Anwendungskomponenten, Systemen und Lösungen berücksichtigt werden muss. Um die Sicherheit IT-basierter Produkte zu erhöhen, muss es also einen Paradigmenwechsel geben, der mit „Security and Privacy by Design" bezeichnet wird (siehe Abschnitt 4.4).[64] Dieser Paradigmenwechsel wird umso wichtiger, wenn man bedenkt, dass Informationstechnologie heute bereits branchenübergreifend der wichtigste Treiber von Innovation ist und zukünftig immer stärker auch in solche Produkte diffundieren wird, die klassisch keine Informationstechnologie verwenden.

Das Paradigma „Security and Privacy by Design" baut sich hauptsächlich auf zwei Säulen auf, welche die folgenden Bereiche betreffen:

- *Prozesse:* Bei der Entwicklung von informationstechnischen Produkten muss es einen Sicherheitsentwicklungsprozess geben, der bereits in der Entwurfsphase beginnt und der sich über den gesamten Lebenszyklus des informationstechnischen Produkts erstreckt.
- *Werkzeuge:* Heutige Softwaredesigner und -entwickler sind hauptsächlich durch die Funktionalität von Produkten getrieben und haben nicht das erforderliche IT-Sicherheitsfachwissen, um die erforderlichen IT-Sicherheitsanforderungen umzusetzen. Das Hinzuziehen von Experten für Sicherheitstests nach der Softwareentwicklung ist zwar effektiv, es verlangsamt den Entwicklungsprozess jedoch erheblich und ist somit nicht optimal für den schnellen Marktzugang und die Wettbewerbsfähigkeit. Nur auf solches Personal zu setzen, welches zusätzlich zu dem jeweiligen Domänenfachwissen noch in IT-Sicherheit geschult wurde, ist auf lange Sicht nicht realistisch, da Hersteller mit ihrem verfügbaren Personal möglichst schnell sichere Produkte auf den Markt bringen wollen. Um dieses Personal bei der Entwicklung von sicheren Produkten zu unterstützen, können Werkzeuge eingesetzt werden, die in die Entwicklungsumgebungen integriert sind und die Sicherheitslücken direkt bei der Entwicklung erkennen und ggf. Vorschläge zur Vermeidung dieser Lücken machen. Diese Werkzeugunterstützung gilt für die Entwicklung von Software und Hardware, da z. B. integrierte Schaltungen wiederum mit Software entworfen werden.

Neben der Steigerung der Sicherheit durch „Security and Privacy by Design" hat dieses Paradigma weitere wichtige Vorteile für Hersteller von informationstechnischen Produkten. Die Entwicklung der Kosten zur Beseitigung von Sicherheitslücken in Software zeigt: Je später im Lebenszyklus eines Produktes Sicherheitslücken erkannt werden, desto teurer wird dies für den Hersteller. Bei Sicherheitslücken in Hardware steigen die Kosten nochmals dramatisch an, da dann physische Bauteile nachproduziert, ausgeliefert und ausgetauscht werden müssen. Die Ausschöpfen dieses Potenzials zur Kostenreduktion hat sowohl Vorteile für Hersteller als auch für Anwender: Für Hersteller ergibt sich daraus ein Wettbewerbsvorteil, für Anwender führt „Security and Privacy by Design" zu reduzierten Kosten bei verbesserter Qualität und höherer Sicherheit.

Wegen der vielfältigen Bedrohungen einerseits und des großen Potenzials des Paradigmas „Security and Privacy by Design" andererseits stellt die künftige, stärkere Berücksichtigung bzw. Anwendung dieses Paradigmas den Kern einer Empfehlung für die staatliche Steuerung im Rahmen von Forschungs- und Innovationsförderung dar.

5.5 Prüfung von IT-Sicherheit

Empfehlung: **Der Gesetzgeber und die Regierung sollten die Voraussetzungen dafür schaffen, dass IT-Produkte hinsichtlich ihrer Sicherheitseigenschaften überprüft werden können. Die Ergebnisse der Überprüfung sollten Anwendern vollständig zugänglich sein. Für Produkte, die in sicherheitskritischen Umgebungen eingesetzt werden, sollten solche Überprüfungen verpflichtend sein, d. h. Produkte sollten nicht eingesetzt werden dürfen, wenn kein der Produktklasse entsprechendes positives Prüfergebnis vorliegt.**

Mit der massiven Diffusion von Informationstechnologie in den Alltag vieler Organisationen und Privatpersonen sind Verletzlichkeit und Risiken für Gesellschaft und Wirtschaft stark gestiegen. Bedrohungen entstehen nicht nur durch die massenhafte Überwachung von Einzelpersonen und deren Kommunikation, wie diese beispielsweise im Rahmen von PRISM durch die NSA geschehen ist, sondern auch durch Wirtschaftsspionage und die Manipulation von informationstechnischen Systemen in Unternehmen und kritischen Infrastrukturen.

Sind informations- und kommunikationstechnische Anwendungen und Systeme nicht hinreichend sicher, dann ergeben sich Ansatzpunkte für Angriffe und somit für Gefahren und Risiken. In der Vergangenheit sind bestimmte informationstechnische Produkte und Systeme entweder von Herstellern oder von Dritten bewusst mit Hintertüren versehen worden, um Anwender besser ausspionieren zu können.[65, 66]

IT-Sicherheitslücken in informations- und kommunikationstechnischen Produkten können zu Schäden von beträchtlichem Ausmaß führen, wenn sie in Beziehung zu großen Werten von Anwendern stehen, z. B. wenn sie in kritischen Infrastrukturen eingesetzt oder von vielen Anwendern verwendet werden.

Heute werden informations- und kommunikationstechnische Produkte und Dienste oftmals in Zusammenhang mit Faktoren angewendet, die kritisch für den Erfolg von Organisationen oder für das Wohlergehen der Gesellschaft sind, ohne dass Aussagen zur Sicherheit dieser Systeme vorliegen.[51] Hier wäre es wünschenswert, wenn informations- und kommunikationstechnische Produkte oder Dienste vor der Beschaffung hinsichtlich ihrer IT-Sicherheit überprüft werden könnten. Die Ergebnisse dieser Überprüfungen sollten dann bei der Produktauswahl berücksichtigt werden können. Diese Überprüfungen sollten durchgeführt werden können, ganz unabhängig davon, wo und von welchem Hersteller die entsprechenden Produkte oder Dienste stammen. Darüber hinaus kann es nützlich sein, wenn die Herstellungsprozesse von Produkten oder Prozesse der Diensterbringung überprüft werden. Ist das Überprüfungsergebnis positiv, kann dies entsprechend dokumentiert und zertifiziert werden. Die Überprüfungsergebnisse sollten für Anwender sichtbar sein.

Bei der Überprüfung von Produkten und Diensten auf Sicherheitslücken oder von Herstellungs- und Diensterbringungsprozessen hinsichtlich ihrer Eignung für IT-Sicherheit sollte es sich um leichtgewichtige Vorgehensweisen handeln. Die Überprüfungen müssen sowohl schnell als auch zu niedrigen Kosten durchgeführt werden können. Es geht dabei nicht in erster Linie darum, die Sicherheit von bestimmten Produkten zu beweisen, sondern darum, bekannte Fehler und Fehlerklassen auszuschließen. Wie die Erfahrung zeigt, liegen den meisten der gefundenen IT-Sicherheitslücken seit langem bekannte Fehlermuster zugrunde, die leicht hätten vermieden werden können.[67] Wenn solche Schwachstellen ausgeschlossen werden können, dann ist für die Cybersicherheit bereits viel erreicht. Wenn es um das Finden von typischen Fehlern geht, lassen sich diese effizient mittels Software-Unterstützung identifizieren. Sind die Überprüfungsprozesse standardisiert, dann können Hersteller diese Prüfroutinen bereits bei der Entwicklung einsetzen, wodurch sich das Sicherheitsniveau bereits bei der Entwicklung verbessern lässt.

Im Zusammenhang mit der Sicherheitsüberprüfung von IT-Produkten werden verschiedene Maßnahmen vorgeschlagen:

- Aufbau und Betrieb einer europäischen Prüfeinrichtung für IT-Sicherheit und Sichtbarmachung ihrer Prüfergebnisse in der Öffentlichkeit;
- Forschung und Entwicklung von effektiven und effizienten Prüfmethoden für IT-Sicherheit, die von der Prüfeinrichtung (und anderen) angewendet werden;
- europaweite Verpflichtung für staatliche Einrichtungen, nur solche informations- und kommunikationstechnischen Produkte einzusetzen, die positiv überprüft wurden.

5.6 Unterstützung von Verbrauchern

Empfehlung: **Um die Cybersicherheit von Verbrauchern zu verbessern, sollten Gesetzgeber und Regierung eine Organisation zum**

Verbraucherschutz im Zusammenhang mit Cybersicherheit schaffen, die Verbraucher aktiv darin unterstützt, ihre eigene Sicherheit zu verbessern. Die Arbeit dieser Organisation sollte durch die anwendungsorientierte Forschung begleitet werden.

Im privaten Alltag spielen Informations- und Kommunikationstechnologien eine große Rolle. Beispielsweise pflegen Menschen damit Kontakte zu ihrem sozialen Umfeld oder kommunizieren mit Ämtern und Behörden, nutzen sie zur Anfertigung von Steuererklärung oder zur Durchführung von Bankgeschäften von zu Hause aus, zum Einkaufen, zur Beratung in verschiedenen Lebensfragen oder einfach nur zur Unterhaltung. Einige Anwendungen haben für Verbraucher einen hohen Schutzbedarf, weshalb die verwendete Hardware und Software entsprechende Sicherheitsanforderungen erfüllen müssen. Nutzen Anwendungen weitere Internetdienste, dann ist auch die Sicherheit dieser Dienste für die Verbraucher wichtig. Darüber hinaus sind für Verbraucher auch die Geschäfts- und Datenschutzbedingungen relevant; diese sollten Verbrauchern helfen zu verstehen, unter welchen Bedingungen und zu welchem Zweck die eigenen Daten an welche Parteien gegeben werden.

Für Verbraucher ist die Nutzung von Informations- und Kommunikationstechnologie sehr komplex. Angriffe und deren Vorbereitung sind für Verbraucher meist unsichtbar. Um Ereignisse und eigene Handlungen korrekt einordnen und erkennen zu können, welche Implikationen bestimmte Entscheidungen und Aktionen mit sich bringen, braucht man als Verbraucher viel Wissen und die Fähigkeit zur Bewertung der großen Menge von Informationen, die fast täglich über die Medien zu den Verbrauchern gelangen. Die meisten Verbraucher sind im Alltag überfordert und können nicht adäquat reagieren. Die Nutzung vieler Anwendungen geht jedoch davon aus, dass die Systeme auf der Seite des Verbrauchers bestimmte Sicherheitsanforderungen erfüllen. Verbraucher sind jedoch mit der Herstellung eines Zustands, der die Sicherheitsanforderungen hinreichend erfüllt, alleine gelassen. Die meisten Schwachstellen werden von Verbrauchern heute erst dann erkannt, wenn sie von Hackern ausgenutzt wurden.

Verbrauchern ist oftmals gar nicht klar, wie weit bestimmte Schutzmaßnahmen gehen und wo deren grundsätzliche Grenzen liegen. Es kann und darf nicht die Lösung sein, dass sich Verbraucher selbst die notwendigen Hintergrundinformationen erarbeiten, um ihre IT-Ausstattung hinreichend sicher zu halten. Es ist davon auszugehen, dass ein durchschnittlicher Verbraucher, der nicht über informationstechnisches Spezialwissen verfügt, dies nicht alleine leisten kann. Dies gilt insbesondere auch deshalb, weil die Entwicklungsdynamik im Bereich der Informations- und Kommunikationstechnologie sehr hoch ist. Die Innovationszyklen sind in diesem Bereich so kurz, dass man als durchschnittlicher Verbraucher das hierfür relevante Wissen praktisch nicht alleine aktuell halten kann. Ohne effektive Lösung dieses Problems wird eine angemessene Erhöhung des Sicherheitsniveaus in der IT-Infrastruktur von Verbrauchern illusorisch sein.

Zur Verbesserung der Rahmenbedingungen für die Cybersicherheit von Verbrauchern sind an den folgenden Stellen Handlungen erforderlich:

- *Verbraucherorganisation für Cybersicherheit:* Es sollte eine Verbraucherorganisation für Cybersicherheit aufgebaut und betrieben werden, die sich um alle relevanten Belange der Cybersicherheit aus der Perspektive der Verbraucher kümmert. Dies umfasst alle Fragen zur Cybersicherheit für Software, Hardware, Netze, Dienste und sicherheits- und privatsphärenbezogene Bedingungen zur Nutzung von Diensten. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterstützt im Rahmen von „BSI für Bürger“ bereits Verbraucher, was sehr begrüßenswert ist. Der Schwerpunkt von „BSI für Bürger“ liegt im Bereich der Aufklärung und Beratung von Verbrauchern. Die hier vorgeschlagene Verbraucherorganisation sollte hingegen weitergehen und auch Beratung auf der Ebene von Produkten vornehmen, z. B. welche Produkte verwendet werden sollen und wie diese für bestimmte Schutzziele zu konfigurieren sind. Die Verbraucherorganisation sollte auf europäischer oder nationaler Ebene angesiedelt sein. Sie sollte Verbraucher hinsichtlich Cybersicherheit be-

raten und konkrete Empfehlungen geben. Die Empfehlungen sollten über typische Produktvergleiche hinausgehen und ggf. auch Anleitungen zur Konfiguration von Produkten für bessere Sicherheitseigenschaften anbieten. Die Verbraucherorganisation sollte gegenüber Technologieherstellern und Dienstanbietern die Interessen von Verbrauchern vertreten. Eine internationale Verbraucherorganisation könnte für Dienste standardisierte Geschäfts- und Datenschutzbedingungen erarbeiten, die von Dienstanbietern übernommen werden können und mit technischer Unterstützung automatisiert abgeglichen werden können.

- *Forschung:* Um die Cybersicherheit für Verbraucher weiter verbessern zu können, ist weitere Forschung erforderlich. Hierbei sollte es um Erforschung von Problemen und Entwicklung von Lösungen gehen, die sowohl in die Wirtschaft (z. B. Software-Hersteller, Dienstanbieter) als auch in die praktische Arbeit einer Verbraucherorganisation für Cybersicherheit transferiert werden sollten. Beispielsweise sollten Lösungen erarbeitet werden, wie IT-Produkte sicherer und privatsphärenfreundlicher gestaltet werden können, ohne dass dies für Verbraucher als zusätzliche Last wahrgenommen wird.

5.7 Standardisierungssouveränität

***Empfehlung:* Auf europäischer Ebene sollte eine Organisation identifiziert oder aufgebaut werden, die für eine eigenständig europäische, mittelfristig internationale Standardisierung im Bereich der Cybersicherheit verantwortlich ist.**

Die international einflussreichsten Standards zur Cybersicherheit werden heute vorwiegend vom US-amerikanischen „National Institute of Standards and Technology" (NIST) entwickelt. NIST spielt in der Strategie der US-amerikanischen Regierung eine wichtige Rolle. Allein für das Jahr 2015 sieht der US-amerikanische Haushalt für NIST ein Budget von US-$ 680 Millionen vor.[68]

Diese international führende Rolle des NIST ist ein klarer Wettbewerbsvorteil für die US-amerikanische Wirtschaft, da deren Interessen von NIST mit höherer Priorität berücksichtigt werden. Umgekehrt herrscht durch die NSA-Affäre ein gewisses Misstrauen gegenüber den besonders regierungsnah entstandenen Cybersicherheitsstandards des NIST (siehe Abschnitt 4.1).

Europa sollte auf diese Situation mit einer eigenen, souveränen Standardisierungsstrategie für Cybersicherheit reagieren. Hierzu muss eine entsprechende Organisation entstehen oder ausgewählt werden. Voraussetzung für den Erfolg ist eine realistisch gewählte Roadmap und ein offener, wissenschaftlich begleiteter und über jeden Verdacht der nachrichtendienstlichen Beeinflussung erhabener Standardisierungsprozess.

5.8 Technologische Souveränität

***Empfehlung:* Auf europäischer Ebene sollten die Voraussetzungen dafür geschaffen werden, dass in Europa marktführende Hersteller von Informationstechnologie und IT-Sicherheitstechnologie entstehen.**

Europa und Deutschland verfügen über eine sehr große Kompetenz im Bereich der IT und IT-Sicherheit. Es gibt exzellente Universitäten und hervorragend ausgebildete Mitarbeiterinnen und Mitarbeiter. Weltweit nehmen Europäer führende Positionen in Forschung und Entwicklung ein. Der Markt für IT und IT-Sicherheit wird aber von Herstellern außerhalb Europas dominiert, insbesondere aus den USA und Asien, insbesondere China. Trotz der sehr kurzen Innovationszyklen in der IT-Industrie gibt es nur sehr wenige globale IT-Anbieter in Europa. Im IT-Sicherheitsbereich ist die europäische Unternehmenslandschaft sehr mittelständisch und eher nationalstaatlich geprägt.

Dieser Mangel kann sich insbesondere angesichts der NSA-Enthüllungen sehr negativ bemerkbar machen: Die NSA-Enthüllungen haben in Europa und anderen Regionen zu einem Vertrauensverlust gegenüber US-amerikanischen Anbietern geführt,[69] ähnlich zu dem bereits zuvor bestehenden Misstrauen gegenüber Anbietern aus anderen Regionen. Mangels alternativer IT-Anbieter hat die Wirtschaft jedoch keine Wahl. Technischen Innovationen

wird aber misstraut, sie werden daher verlangsamt angenommen, die Wettbewerbsfähigkeit in Europa leidet.[70] Auf staatlicher wie wirtschaftlicher Ebene herrscht die Sorge, IT könnte Hintertüren enthalten und im Zweifel gegen ihren Nutzer eingesetzt werden.

Angesichts dieser Situation mag man sich eine vollständige IT-Unabhängigkeit Europas und Deutschlands von den USA und anderen Regionen wünschen. Angesichts globaler Märkte und global vernetzter Unternehmen und Privatpersonen ist eine solche Unabhängigkeit allerdings weder realistisch noch wirklich wünschenswert. Niemand wird ernsthaft Europa von der technologischen Entwicklung im Rest der Welt abkoppeln wollen.

Ein Teil der Antwort auf diese Situation muss daher der schon erwähnte Aufbau von technischen und rechtlichen Maßnahmen zum Überprüfen und sicheren Integrieren von IT-Produkten und Dienstleistungen sein, unabhängig von deren Herkunft (Empfehlungen 4 und 5).

In einzelnen Bereichen ist aber auch eine echte Unabhängigkeit, also der Aufbau von großen europäischen Herstellern, sinnvoll und möglich. Welche Bereiche dies sind, sollte Gegenstand einer strategischen Analyse sein. Zwei Handlungsstränge erscheinen sinnvoll: Aufbau eines globalen IT-Herstellers in Europa für zentrale Bereiche, z. B. für die Infrastruktur, sowie Aufbau eines globalen auf IT-Sicherheit spezialisierten Herstellers in Europa.

Es ist anzunehmen, dass eine solche Aktivität auf positiven Zuspruch in der Gesellschaft und europäischen Wirtschaft stoßen würde. Gute Chancen für eine positive wirtschaftliche Entwicklung scheinen vorhanden.[71] In den Segmenten, in denen es bereits Alternativen zu US-Anbietern gab, haben deutsche und europäische Unternehmen entsprechende positive Marktreaktionen wahrnehmen können.[72]

Neben der gewonnenen Unabhängigkeit könnten industriepolitische Maßnahmen dieser Art auch indirekt, über den steigenden Konkurrenzdruck auf US-amerikanische Anbieter, zu positiven Änderungen in der heutigen Praxis der Massenüberwachung führen. Selbst Anbieter von Produkten, für welche es heute noch keine echte europäische Konkurrenz gibt, merken die Auswirkungen des mangelnden Kundenvertrauens deutlich in ihren Geschäftszahlen.[73, 74]

5.9 Cybersicherheitsforschung in Deutschland

Empfehlung: **Der Gesetzgeber und die Regierung sollten einen strategischen und finanziellen Rahmen zur Förderung der Cybersicherheitsforschung in Deutschland schaffen. Der Umfang der nationalen Forschungsförderung sollte deutlich erhöht werden. Deutschland sollte sich intensiv für ein gezieltes Forschungsprogramm zur Cybersicherheit auf europäischer Ebene einsetzen. Die Politik der Bildung nationaler, auf Dauer angelegter und an Exzellenz auf internationalem Niveau ausgelegter Kompetenzzentren für Cybersicherheitsforschung sollte fortgesetzt und ausgebaut werden. Cybersicherheit ist ein Querschnittsthema und sollte als solches bei allen öffentlich geförderten Innovationsprojekten zwingend Berücksichtigung finden.**

Aufgrund der weiter fortschreitenden Verbreitung von Informations- und Kommunikationstechnologie und der damit einhergehenden steigenden Verletzlichkeit kommt der Cybersicherheitsforschung eine weiter wachsende Bedeutung zu. Die Behandlung von Fragen der Cybersicherheit ist für Freiheit und Demokratie, Gesellschaft, Wirtschaft und Wohlstand von großer Relevanz. Die rasante Weiterentwicklung von Informations- und Kommunikationstechnologie auf der einen Seite und die fast täglichen Meldungen von Sicherheitslücken und stattgefundenen Angriffen legen nahe, dass es noch viele Probleme in der Cybersicherheit gibt, die gelöst werden müssen. Hier ist die Forschung gefragt. Deutschland und Europa sollten auf dem Gebiet der Cybersicherheitsforschung Vorreiter sein. Cybersicherheit spielt heute branchenübergreifend in allen Produkten eine Rolle, die Informations- und Kommunikationstechnologie verwenden. Bei den kurzen Innovationszyklen in der Informations- und Kommunikationstechnologie ist es für die Wettbewerbsfähigkeit der Wirtschaft wichtig, die Forschungsexpertise zur Cybersicherheit vor

Ort zu haben. Darüber hinaus kann eine exzellente Cybersicherheitsforschung die Politik in Fragen beraten, die von hohem nationalem Interesse sind.

Bund und Länder müssen die Voraussetzungen dafür schaffen, dass sich die Cybersicherheitsforschung in Deutschland entsprechend positiv entwickeln kann. Das Ziel muss es sein, dass mit den eingesetzten Mitteln Ergebnisse erarbeitet werden, die für Wirtschaft und Gesellschaft von hohem Nutzen sind.

Dies umfasst zunächst die anwendungsorientierte Forschung, die sich mit den Fragen zu beschäftigen hat, wie sie heute von Politik, Wirtschaft und Gesellschaft an die Forschung herangetragen werden, z. B. Sicherheit von Industrie 4.0, Smartphone-Sicherheit oder Privatsphärenschutz in sozialen Netzen. Ebenso wichtig ist die Grundlagenforschung, die Wissen und Vorschläge zur Lösung der Cybersicherheitsprobleme von morgen erarbeitet wie z. B. zum Clean-Slate-Design für sichere Systeme oder zur voll-homomorphen Verschlüsselung zur Durchführung von Datenverarbeitungsoperationen auf verschlüsselten Daten.

Zur Gestaltung des Rahmens zur Cybersicherheitsforschung in Deutschland sollten Strukturen geschaffen bzw. ausgebaut werden, bei denen insbesondere die folgenden Aspekte berücksichtigt werden sollten:

- *Nationale Cybersicherheitsstrategie:* Die Cybersicherheitsstrategie für Deutschland und die Cybersicherheitsforschung in Deutschland sollten eng verzahnt sein.[75] Exzellente Wissenschaftler der Cybersicherheitsforschung in Deutschland beraten die Politik im Hinblick auf die Cybersicherheitsstrategie. Die Cybersicherheitsstrategie gibt wichtige Themen vor, die von nationalem Interesse sind, und steuert somit die Cybersicherheitsforschung in Deutschland. In dieser Cybersicherheitsstrategie sollten inhaltliche und strukturelle Ziele festgeschrieben sein. Daraus ergeben sich die Leitlinien für die Cybersicherheitsforschung. Darüber hinaus sollte die Cybersicherheitsstrategie Maßnahmen zur Erreichung von Cybersicherheitszielen enthalten. Bei der Erarbeitung dieser Maßnahmen sollte die Politik von anerkannten Vertretern der deutschen Cybersicherheitsforschung unterstützt werden. Die Strategie sollte kontinuierlich fortgeschrieben werden. Aktivitäten auf Landesebene sollten in Abstimmung mit der nationalen Cybersicherheitsstrategie erfolgen.
- *Zentrumsbildung:* Ein wesentlicher Bestandteil der Cybersicherheitsstrategie ist die Bündelung der wissenschaftlichen Arbeiten in thematisch fokussierten Forschungszentren. Diese Forschungszentren sollten neben der heute existierenden universitären und außeruniversitären Forschung bestehen. Die längerfristige Konzentration der eingesetzten Mittel auf wenige ausgewählte Zentren hat viele positive Effekte auf die Cybersicherheitsforschung. Es entstehen dadurch Forschungseinrichtungen, die in Größe und Schlagkraft mit den großen Forschungseinrichtungen international, insbesondere in den USA, konkurrenzfähig sind. Durch Zentrumsbildung kann eine kritische Masse erreicht werden, welche die neuen Zentren attraktiv für exzellente Wissenschaftler macht. So können herausragende Köpfe für Deutschland zurückgewonnen werden, die früher ins Ausland gegangen sind. Das Bundesforschungsministerium hat mit der Einrichtung seiner Kompetenzzentren für Cybersicherheitsforschung bereits im Jahr 2011 die Weichen in diese Richtung gestellt, mit positiven Ergebnissen: Es konnten damit in Deutschland Leuchttürme international anerkannter Spitzenforschung aufgebaut werden, mittels derer exzellente Wissenschaftler für Deutschland gewonnen und wichtige neue Themen der Cybersicherheitsforschung positioniert werden konnten. Forschungsfördermittel können in einem Zentrum sehr viel koordinierter und strategischer in Forschung investiert werden. Die Strategie der Zentrumsbildung des Bundes sollte weiter verfolgt werden, indem die bestehenden Zentren langfristig ausgebaut werden.
- *Verzahnung von Grundlagenforschung und anwendungsorientierter Forschung:* Die Verzahnung verschiedener Ausrichtungen in der Cybersicherheitsforschung ist wichtig für praktisch relevante Forschung, die auf Exzellenz ausgerichtet ist und dadurch mit den

weltbesten Forschungseinrichtungen für Cybersicherheit wettbewerbsfähig ist. Durch die enge Verzahnung erzielen Grundlagenforschung und anwendungsorientierte Forschung Synergieeffekte, indem die anwendungsorientierte Forschung auf Ergebnisse der Grundlagenforschung zurückgreifen kann und die Grundlagenforschung über die anwendungsorientierte Forschung die für die Praxis relevanten Grundlagenfragen erhält. Damit die Cybersicherheitsforschung von möglichst hohem Nutzen für Wirtschaft und Gesellschaft sein kann, muss sie sich an den wichtigen anwendungsorientierten Forschungsfragen orientieren.

- *Finanzrahmen:* Cybersicherheit ist ein Thema, welches für Gesellschaft und Wirtschaft von zentraler Bedeutung ist. Das Thema ist sowohl für Anwender als auch für Hersteller relevant, deren Wettbewerbsfähigkeit durch Produkte mit entsprechenden IT-Sicherheitseigenschaften gestärkt wird. Auf der anderen Seite investieren staatliche Organisationen wie Geheimdienste oder Unternehmen weltweit erhebliche Summen, um IT-basierte Anwendungen oder Systeme angreifen zu können. Allein für das Jahr 2013 hatte der US-amerikanische Geheimdienst NSA ein Budget von US-$ 52,6 Milliarden nur für sein Crypto-Cracking-Programm reserviert.[76] Das Forschungsbudget des Department of Homeland Security hat allein für die Forschung und Entwicklung des Intrusion Detection-Systems Einstein im Jahr 2015 ein Budget von US-$ 549 Millionen vorgesehen.[77] Hinzu kommen viele andere Vorhaben, die sich auf Cybersicherheit beziehen und für die große Budgets reserviert sind. Die hohen Summen belegen die große Bedeutung der Cybersicherheit für die US-Regierung. Die Cybersicherheitsforschung in Deutschland sollte entsprechend der Aktivitäten in anderen Ländern weiter gestärkt werden. Die Forschung und Entwicklung im Bereich der Cybersicherheit sollte mit adäquaten Finanzmitteln ausgestattet sein.
- *Cybersicherheit für Innovationsprojekte:* In vielen Innovationsprojekten wird die eigentliche Innovation durch Informationstechnologie getrieben. In diesen Projekten werden fertige Produkte und Dienste oder Prototypen als Vorstufe wirtschaftlich verwertbarer Ergebnisse entwickelt. Haben diese Ergebnisse Sicherheitslücken, entstehen neue Ansatzpunkte für Angriffe. Um das Verletzlichkeitspotenzial durch diese Innovationen möglichst gering zu halten, sollte Cybersicherheit bei der Entwicklung von Innovationen eine Rolle spielen. Die Berücksichtigung von Cybersicherheit sollte in öffentlich geförderten Innovationsprojekten durchgesetzt werden, z. B. indem in jedem öffentlich geförderten Innovationsprojekt, bei dem Informationstechnologie angewendet wird, Fragen der Cybersicherheit adäquat behandelt werden.

Bundesregierung und einige Landesregierungen haben in den vergangenen Jahren – und dies auch schon vor den Enthüllungen von Edward Snowden – viel unternommen, um die IT-Sicherheitsforschung in Deutschland zu fördern. Es bleibt festzuhalten, dass Deutschland hier auf einem guten Weg ist. Die Cybersicherheitsforschung in Deutschland muss jedoch weiter gestärkt werden. Hierfür ist ein entsprechender Rahmen zur Forschungsförderung zu schaffen.

5.10 Verzahnung von Rechts- und Technikgestaltung

***Empfehlung:* Um die Rechts- und Technikgestaltung besser miteinander verzahnen zu können, sollten die Verträglichkeit des Rechts- und Technikrahmens kontinuierlich überwacht werden, die Techniktrends hinsichtlich ihrer Relevanz für den Rechtsrahmen möglichst früh analysiert werden, Betroffene möglichst früh über die relevanten Implikationen neuer gültiger Rechtsgestaltung empfängeradäquat informiert und Vorschläge für juristische Diskussionen und neue Rechtsrahmen ggf. vor ihrer Verabschiedung im Rahmen von Simulationsstudien geprüft werden.**

Anwendung und Gestaltung von Technik auf der einen Seite und Recht auf der anderen Seite sollten eng miteinander verbunden sein. Der bestehende Rechtsrahmen gibt vor, wie

vorhandene Technologie angewendet werden kann. Jedoch entwickelt sich Technologie typischerweise weiter, wodurch sich auch neue Anwendungen ergeben. Die neuen Anwendungen können dann verträglich mit dem bestehenden Rechtsrahmen sein oder sie können ihm widersprechen. Die dritte Möglichkeit besteht darin, dass der bestehende Rechtsrahmen keine bzw. keine deutliche Aussage zu der neuen Anwendung der Technologie gibt. In diesem Fall muss dann im Zuge der Rechtsgestaltung der Rechtsrahmen weiterentwickelt werden.

Wenn der Rechtsrahmen der neuen technischen Entwicklung folgt, dann ist es wichtig, dass der neue Rechtsrahmen möglichst schnell zur Verfügung steht. Das Fehlen eines Rechtsrahmens schafft Unsicherheit im Positiven wie im Negativen. Beispielsweise kann das Fehlen eines Rechtsrahmens bedeuten, dass Unternehmen nicht wissen, wie sie reagieren und investieren sollen. Haben Unternehmen bereits in neue Anwendungen investiert, die laut neuem Rechtsrahmen nicht mehr rechtskonform sind, dann drohen zwangsläufig Verluste. Gegebenenfalls können dann getätigte Investitionen nicht mehr länger genutzt werden und Geschäftsmodelle müssen geändert werden. Wird der Rechtsrahmen in einem anderen Land schneller angepasst, dann haben die dort ansässigen Unternehmen eine größere Rechtssicherheit für ihre Investitionen. So lange der Rechtsrahmen der Technik nicht folgt, können rechtsfreie Räume ausgenutzt werden, z. B. auch gegen die Interessen von Verbrauchern, wie dies bei der Verzögerung in der Umsetzung der e-Privacy-Direktive der EU in Deutschland der Fall ist.

Wird ein Rechtsrahmen weiterentwickelt, dann ist es von Vorteil, wenn er bereits die weitergehende technologische Entwicklung vorwegnimmt und berücksichtigt, so dass damit bereits für zukünftige Anwendungen ein passender Rechtsrahmen besteht. Hierfür sollte man die Trends in der Anwendung von Informations- und Kommunikationstechnik identifizieren und erfassen, damit diese frühzeitig bei der Rechtsgestaltung berücksichtigt werden können.

Es kommt zuweilen jedoch auch vor, dass der Rechtsrahmen sich weiterentwickelt, der neue Rechtsrahmen für die potenziellen Anwender jedoch nicht hinreichend klar ist, so dass sie nicht wissen, wie weit sie gehen können, um sich noch rechtssicher zu bewegen. Ein Beispiel hierfür ist der sogenannte Hackerparagraph (StGB § 202 a Ausspähen von Daten, § 202 b Abfangen von Daten, § 202 c Vorbereiten des Ausspähens und Abfangens von Daten), der im Jahr 2007 eingeführt wurde. Bei der hier bestehenden Dual-Use-Problematik wurde der Aspekt, der zum gesellschaftlichen Wohlergehen beiträgt, nicht angemessen berücksichtigt, so dass hier zunächst Nachteile entstanden sind. Der Hackerparagraph schreibt vor, dass sich Personen strafbar machen, wenn sie Werkzeuge herstellen, die dazu verwendet werden können, Daten auszuspähen oder abzufangen. Um reale Software sicherer machen zu können, ist es jedoch häufig notwendig, Werkzeuge zu entwickeln, um Sicherheitslücken in Software zu erkennen, so dass in einem nächsten Schritt Lücken in der Software geschlossen werden können. Die Entwicklung von Hacking-Werkzeugen dient in diesem Fall dann dazu, dass Anwendungssoftware sicherer gemacht werden kann. Ohne die Verwendung von solchen Hacking-Werkzeugen ist die Verbesserung der Sicherheit von Anwendungssoftware praktisch nicht möglich. Andererseits können entwickelte Werkzeuge dazu verwendet werden, reale Softwaresysteme anzugreifen und Anwendern dieser Systeme damit zu schaden. Die Einführung des Hacker-Paragraphen hatte damals zu einer starken Verunsicherung auf der Seite der Entwickler geführt. Die Hersteller von Hacking-Werkzeugen hatten die Sorge, dass sie sich strafbar machen, auch wenn sie nicht die Absicht hatten, anderen Parteien zu schaden. Dadurch hat der Hacker-Paragraph dann dazu geführt, dass andere Anwendungssoftware zunächst nicht so gesichert werden konnte, da Hacker vor der Entwicklung bzw. Anpassung von Hacking-Werkzeugen aus Gründen potenzieller Strafbarkeit zurückgeschreckt sind. Auch wenn es bei dem Hackerparagraphen eigentlich darum ging, die Bedingungen für IT-Sicherheit zu verbessern, haben sich dadurch die Bedingungen für IT-Sicherheit zunächst einmal verschlechtert. Um solche Situationen zu vermeiden, wäre es von Vorteil, wenn bei der Verabschiedung neuer Gesetze entsprechende Hinter-

grundinformationen vorliegen würden, anhand derer die Entwickler die Rechtssituation besser einschätzen könnten.

Situationen wie nach der Verabschiedung des Hackerparagraphen hätten ggf. vermieden werden können, wenn alle Seiten frühzeitig eingebunden gewesen wären. Jedoch bietet eine solche Einbindung keine Garantie dafür, dass die verschiedenen Aspekte bei der Rechtsgestaltung in dem Sinne abgewogen werden, wie sie für das Wohlergehen der Gesellschaft den besten Rahmen bieten. Oftmals ist der Sachverhalt sehr komplex und es lässt sich im Vorfeld nur sehr schwierig abschätzen, zu welchen Konsequenzen bestimmte Entscheidungen führen und ob Entscheidungen für das Wohlergehen der Gesellschaft die optimalen Voraussetzungen bieten. Ein Beispiel hierfür ist die gerade in der Diskussion befindliche Idee, ob man Betreiber und Anbieter von Informations- und Kommunikationstechnologie verpflichten sollte, dass diese die bekannt gewordenen Schwachstellen frühzeitig melden bzw. öffentlich machen müssen. Auf der einen Seite bringt eine solche Transparenzverpflichtung einen Vorteil für Kunden, Anwender und andere Betreiber bzw. Anbieter desselben Produkts, andererseits kann eine Veröffentlichung auch dazu führen, dass das Bekanntwerden einer Sicherheitslücke Hacker erst auf die Lücke aufmerksam macht, so dass die Lücke erst dadurch ausgenutzt werden kann. Welche Lösung hier die bessere ist, ist offen. Dennoch sollten solche Fragen möglichst schnell beantwortet und Entscheidungen zur Rechtsgestaltung zügig getroffen werden. Hierfür können Instrumente wie Simulationsstudien hilfreich sein, bei denen Vertreter aus Recht und Technik die Auswirkungen von potenziellen Regelungen analysieren und überprüfen, ob bzw. wie hilfreich bestimmte Regelinstrumente sind.

Um die Rechts- und Technikgestaltung enger verzahnen zu können, sollen folgende Themen behandelt werden:

- *Monitoring der Verträglichkeit von Rechts- und Technikrahmen und Abgleich:* Es sollte in geeigneten Intervallen überprüft werden, ob Rechts- und Technikrahmen noch im Einklang sind. Hierzu müssen reale Entwicklungen der Technikanwendung gegen den bestehenden Rechtsrahmen geprüft werden. Hierzu ist eine anwendungsorientierte und interdisziplinäre Forschung unter Einbeziehung der Fachgebiete Informatik, insbesondere Cybersicherheit, und Recht, insbesondere IT-Recht, erforderlich. Die Ergebnisse dieser Forschung sollten in die Rechtsgestaltung einfließen.
- *Erfassung und Analyse von Trends für Technologie und Anwendungen:* Technologische Trends und die damit potenziell möglichen Anwendungen sollten möglichst früh erfasst werden und der Rechtsgestaltung zugeführt werden.
- *Angebot von Hintergrundinformationen bzgl. Rechtsgestaltung:* Wenn ein neuer Rechtsrahmen mit Relevanz für IT-Sicherheit geschaffen wird, dann sollte dieser mit allen relevanten Hintergrundinformationen, z. B. alle seinen konkreten Rückwirkungen auf die Technik und deren Anwendung, möglichst vielen Betroffenen kurzfristig mitgeteilt werden. Hierbei ist es wichtig, dass diese Hintergrundinformationen gerade für diejenigen verständlich dargestellt werden, die von den Änderungen betroffen sind.
- *Durchführung von Simulationsstudien:* Simulationsstudien bieten ein Instrument, um bei Themen und Sachverhalten, bei denen es noch keine Urteile aus der Praxis gibt, Argumente für die juristische Diskussion zu liefern. Diese lassen sich auf einen geltenden wie auch auf einen vorgeschlagenen Rechtsrahmen anwenden und liefern somit Erkenntnisse für die Rechtsgestaltung.

PROF. DR. MICHAEL WAIDNER

Direktor der Forschungszentren EC SPRIDE und CASED an der Technischen Universität Darmstadt, www.ec-spride.de / www.cased.de;
Institutsleiter des Fraunhofer-Instituts für Sichere Informationstechnologie (SIT), Darmstadt, www.sit.fraunhofer.de;
michael.waidner@sit.fraunhofer.de

ANMERKUNGEN

* Dieser Text wurde zuerst veröffentlicht unter http://www.bundestag.de/bundestag/ausschuesse18/ua/1untersuchungsausschuss/-/280848. Er wird hier mit freundlicher Genehmigung des Verfassers abgedruckt.

1 Jacob Appelbaum et. al.: Der geheime Werkzeugkasten der NSA; Der Spiegel, 30. Dezember 2013 (http://www.spiegel.de/netzwelt/netzpolitik/neue-dokumente-der-geheime-werkzeugkasten-der-nsa-a-941153.html)

2 Glenn Greenwald: No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State; Metropolitan Books, New York, Mai 2014

3 Kim Zettler: How a Crypto „Backdoor" Pitted the Tech World Against the NSA; Wired, 24. September 2013 (http://www.wired.com/2013/09/nsa-backdoor/all/)

4 Anja Feldmann: Current Trends in the Internet Architecture; Keynote; Networked Systems, Stuttgart 2013 (http://www.netsys2013.de/keynotes.html)

5 Cisco Visual Networking Index: Forecast and Methodology, 2013-2018; (http://www.cisco.com/c/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.pdf)

6 The National Security Agency: Missions, Authorities, Oversight and Partnerships; NSA, 9. August 2013 (http://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf)

7 Global Internet Phenomena Report: 1H 2014; Sandvine, 2014 (https://www.sandvine.com/downloads/general/global-internet-phenomena/2014/1h-2014-global-internet-phenomena-report.pdf)

8 Jim Cowie: The New Threat: Targeted Internet Traffic Misdirection; renesys, 19. November 2013 (http://www.renesys.com/2013/11/mitm-internet-hijacking)

9 The NSA Archive; American Civil Liberties Union (https://www.aclu.org/nsa-documents-search)

10 Haya Shulman, Michael Waidner: Towards Forensic Analysis of Attacks with DNSSEC; Intl. Workshop on Cyber Crime at the IEEE Symp. On Security and Privacy; San Jose 2014 (www.ieee-security.org/TC/SPW2014/papers/5103a069.PDF)

11 Datenverkehr am DE-CIX erreicht neuen Spitzenwert von 2 Terabit pro Sekunde; Pressemitteilung, DE-CIX, Frankfurt a.M., 21. September 2012 (http://presse.de-cix.net/uploads/media/PM_DE-CIX_2Tbitps-Peak_DT_FINAL.pdf)

12 NSA: Inside the FIVE-EYED VAMPIRE SQUID of the INTERNET; The Register, 5. Juni 2014 (http://www.theregister.co.uk/Print/2014/06/05/how_the_interenet_was_broken)

13 Vodafone: Sustainability Report 2013/14. http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html

14 Telekom bastelt am „Deutschland-Net"; Süddeutsche Zeitung, 12. Oktober 2013 (http://www.sueddeutsche.de/digital/reaktion-auf-nsa-ueberwachung-telekom-bastelt-am-deutschland-net-1.1793247)

15 Matthias Meisner: Die Grenzen der Freiheit: Wenn Deutsche nicht in die USA dürfen; Der Tagesspiegel, 27. Dezember 2013 (http://www.tagesspiegel.de/politik/einreiseverbot-die-grenzen-der-freiheit-wenn-deutsche-nicht-in-die-usa-duerfen/9266368.html)

16 Peter Blechschmidt: Der gesperrte Himmel. Süddeutsche Zeitung, 17. Mai 2010 (http://www.sueddeutsche.de/reise/usa-ueberflugsrechte-der-gesperrte-himmel-1.172848)

17 Doug Laney: 3D Data Management, Controlling Data Volume, Velocity and Variety; META Group, Stamford, CT, 2001 (http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf)

18 Krystal Temple: What Happens In An Internet Minute?; Intel InsideScoop, 13. März 2012 (http://scoop.intel.com/what-happens-in-an-internet-minute)

19 Viktor Mayer-Schönberger, Kenneth Cukier: Big Data. Redline-Verlag, 2013

20 1 Exabyte (EB) ≈ 103 Petabyte (PB) ≈ 106 Terabyte (TB) ≈ 109 Gigabyte (GB) ≈ 1018 Byte (B)

21 Rich Miller: Facebook Builds Exabyte Data Centers for Cold Storage; Date Center Knowledge, 18. Januar 2013 (http://www.datacenterknowledge.com/archives/2013/01/18/facebook-builds-new-data-centers-for-cold-storage/)

22 Andreas J Peters, Lukasz Janyst: Exabyte Scale Storage at CERN; 2011 J. Phys.: Conf. Ser. 331 052015 (http://iopscience.iop.org/1742-6596/331/5/052015)

23 James Bamford: Who's in Big Brother's Database?; New York Times, 5. November 2009. (http://www.nybooks.com/articles/archives/2009/nov/05/whos-in-big-brothers-database)

24 Markus Schneider, Matthias Enzmann, Martin Stopzcynski: Web-Tracking-Report 2014. Fraunhofer SIT Technical Report SIT-TR-2014-01, März 2014 (https://www.sit.fraunhofer.de/reports)

25 Hierbei geht es darum, Daten für die Datenverarbeitung aufzubereiten, die in gesprochener Sprache vorliegen. Dies geschieht entweder durch Annotierung, bei der zentrale Schlüssel- oder Kategorisierungsbegriffe verschriftlicht werden, oder durch die vollständige Verschriftlichung von Audiodaten. Dadurch werden Daten verarbeitbar, z.B. ist dann die Suche nach einem bestimmten Begriff möglich.

26 Bei Stilometrie geht es um die Untersuchung von Ausdrucksweisen, Sprech- und Schreibstilen durch Verwendung statistischer Hilfsmittel. Sie erlaubt Rückschlüsse auf den Verfasser von Dokumenten.

27 Nate Anderson: „Anonymized" Data Really isn't – And Here's Why Not. Ars Technica, 8. September 2009 (http://arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin)

[28] Zur Vermeidung von Missverständnissen: Auch in der „public key" Kryptographie gibt es „secret keys", die geheim gehalten werden müssen, z.B. Signier- und Entschlüsselungsschlüssel.

[29] Kryptographische Verfahren: Empfehlungen und Schlüssellängen; BSI TR-02102-1, Bundesamt für Sicherheit in der Informationstechnik, Bonn, 10. Februar 2014 (https://www.bsi.bund.de/ SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102_pdf.html)

[30] Nigel P. Smart (ed.): Algorithms, Key Sizes and Parameters Report; ENISA, Kreta, 29. Oktober 2013 (http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report/at_download/fullReport)

[31] Dieser Gedanke ist in der Kryptographie als das „Kerkhoffs'sche Prinzip" bekannt.

[32] Kim Zettler: How a Crypto „Backdoor" Pitted the Tech World Against the NSA; Wired, 24. September 2013 (http://www.wired.com/2013/09/nsa-backdoor/all/)

[33] Benedikt Driessen et. al.: Don't Trust Satellite Phones: A Security Analysis of Two Satphone Standards; IEEE Symposium on Security & Privacy 2012 (http://gmr.crypto.rub.de/paper/paper-1.pdf)

[34] GSM Security Country Report: Germany; Security Research Labs, Berlin, Mai 2014; (http://gsmmap.org/assets/pdfs/gsmmap.org-country_report-Germany-2014-05.pdf)

[35] Orr Dunkelman et. al.: A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony; CRYPTO 2010; Springer-Verlag, Heidelberg 2010 (http://www.ma.huji.ac.il/~nkeller/Crypt-jour-Kasumi.pdf)

[36] John Leyden: French Gov Used Fake Google Certificate to Read its Workers' Traffic; The Register, 10. Dezember 2013 (http://www.theregister.co.uk/2013/12/10/french_gov_dodgy_ssl_cert_reprimand)

[37] Mistrust Authority; The Economist, 10. September 2011 (http://www.economist.com/node/21528601)

[38] Mozilla Included CA Certificate List, Stand vom 15. Juni 2014 (http://www.mozilla.org/en-US/about/governance/policies/security-group/certs/included/)

[39] Siehe beispielsweise „Perspectives" (http://perspectives-project.org/) oder „Public Key Pinning" (http://www.ietf.org/id/draft-ietf-websec-key-pinning-14.txt)

[40] Michael Herfert, Michael Waidner: Trend- und Strategiebericht „Privatsphärenschutz und Vertraulichkeit im Internet", SIT-TR-2013-03, 2013 (https://www.sit.fraunhofer.de/reports)

[41] Der GAU für Verschlüsselung im Web: Horror-Bug in OpenSSL; Heise, 8. April 2014 (http://heise.de/-2165517)

[42] Kenny Paterson: TLS Security – Where Do We Stand?; RHUL, 2013 (http://www.cl.cam.ac.uk/research/security/seminars/archive/slides/2013-10-15.pdf)

[43] Siehe hierzu auch das Projekt „Immersion" (https://immersion.media.mit.edu)

[44] David Chaum: Untracable Electronic Mail, Return Addresses, and Digital Pseudonyms; Communications of the ACM, 1981

[45] Andreas Pfitzmann, Michael Waidner: Networks Without User Observability – Design Options; Eurocrypt '85, LNCS 219, Springer-Verlag, Berlin 1986, 245-253

[46] https://www.privacy-handbuch.de/handbuch_22b2.htm, Abruf am 12.6.2014

[47] https://www.torproject.org/

[48] https://www.anonym-surfen.de/jondo.html

[49] Bruce Schneier: Attacking Tor: How the NSA Targets Users' Online Anonymity; The Guardian, 4. Oktober 2013 (http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity)

[50] Vertrauen und Sicherheit im Netz; BITKOM, Berlin 2012 (http://www.bitkom.org/files/documents/Vertrauen_und_Sicherheit_im_Netz.pdf)

[51] Industriespionage 2012, Corporate Trust, München 2013 (http://corporate-trust.de/pdf/CT-Studie-2012_FINAL.pdf)

[52] „When NSA decides to withhold a vulnerability for purposes of foreign intelligence, then the process of mitigating risks to US and allied systems is more complex." – Michael S. Rogers, Schriftliche Stellungnahme vom 11. März 2014, US Senate Committee on Armed Services, (http://www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf)

[53] Christiane Grefe: Blackout; Die Zeit, 17. April 2014 (http://www.zeit.de/2014/16/blackout-energiehacker-stadtwerk-ettlingen/komplettansicht)

[54] Jacob Appelbaum et.al.: Der geheime Werkzeugkasten der NSA; Der Spiegel, 30. Dezember 2013 (http://www.spiegel.de/netzwelt/netzpolitik/neue-dokumente-der-geheime-werkzeugkasten-der-nsa-a-941153.html)

[55] In den USA spricht man oft auch von „Build in Security" (BSI) bzw. vom Gegensatzpaar „Built-in Security" = proaktiv vs. „Bolt-on Security" = reaktiv. (https://buildsecurityin.us-cert.gov/)

[56] Hermann Härtig: The L4 Microkernel; ARTIST Summer School in Europe 2010 (http://os.inf.tu-dresden.de/papers_ps/artist2010_presentation.pdf)

[57] L4HQ.org Projektseiten (http://l4hq.org)

[58] Matthew Hoekstra: Intel SGX for Dummies (Intel SGX Design Objectives); 26. September 2013 (https://software.intel.com/en-us/blogs/2013/09/26/protecting-application-secrets-with-intel-sgx)

[59] John Markoff: Profiles in Science „Peter G. Neumann": Killing the Computer to Save It; New York Times, 29. Oktober 2012 (http://www.nytimes.com/2012/10/30/science/rethinking-the-computer-at-80.html)

[60] University of Cambridge (UK) & SRI International: CTSRD – Rethinking the Hardware-Software Interface for Security (https://www.cl.cam.ac.uk/research/security/ctsrd)

[61] Siehe hierzu Fußnote 54 und die dort exemplarisch genannten Kosten für manipulierte Hardware für maßgeschneiderte Angriffe, sogenannte „Tailored Access Operations".

[62] Google und Facebook distanzieren sich von Überwachungsprogramm; Süddeutsche Zeitung, 8. Juni 2013 (http://www.sueddeutsche.de/digital/nsa-programm-prism-google-und-facebook-distanzieren-sich-von-ueberwachungsprogramm-1.1691690)

[63] Michael Suby: The 2013 (ISC)² Global Information Security Workforce Study; Frost & Sullivan in partnership with Booz Allen Hamilton for ISC, 2013

[64] Michael Waidner, Michael Backes, Jörn Müller-Quade, Eric Bodden, Markus Schneider, Michael Kreutzer, Mira Mezini, Christian Hammer, Andreas Zeller, Dirk Achenbach, Matthias Huber, Daniel Kraschewski: Entwicklung sicherer Software durch Security by Design; SIT-TR-2013-01, Darmstadt 2013 (https://www.sit.fraunhofer.de/reports).

[65] Heise: NSA-Skandal: Cisco beschwert sich über manipulierte Postsendungen; 15. Mai 2014 (http://www.heise.de/newsticker/meldung/NSA-Skandal-Cisco-beschwert-sich-ueber-manipulierte-Postsendungen-2190470.html)

[66] Lisa Hemmerich: Nortel: Hacker kannten Passwörter von Top-Managern – Telekomausrüster jahrelang ausgespäht; Netzwelt, 14. Februar 2012 (http://www.netzwelt.de/news/90847-nortel-hacker-jahrelang-zugang-zentralen-dokumenten.html)

[67] Steve Christley: CWE//SANS Top 25 Most Dangerous Software Errors, SANS 2011 (http://cwe.mitre.org/top25)

[68] Executive Office of the President of the United States: Fiscal Year 2015 Budget of the U.S. Government. 2014. (http://www.whitehouse.gov/sites/default/files/omb/budget/fy2015/assets/budget.pdf)

[69] Daniel Castro: How Much Will PRISM Cost the U.S. Cloud Computing Industry?, 5. August 2013 (http://www2.itif.org/2013-cloud-computing-costs.pdf)

[70] Heise Online: Bitkom: PRISM-Spähskandal erschüttert Vertrauen der Internetnutzer, 25. Juli 2013 (http://www.heise.de/newsticker/meldung/Bitkom-PRISM-Spaehskandal-erschuettert-Vertrauen-der-Internetnutzer-1923732.html)

[71] James Staten: The Cost of PRISM Will Be Larger Than ITIF Projects, 15. August 2013 (http://www.forbes.com/sites/forrester/2013/08/15/the-cost-of-prism-will-be-larger-than-itif-projects)

[72] Handelsblatt: Deutsche E-Mail-Anbieter profitieren von NSA-Affäre, 25. August 2013 (http://www.handelsblatt.com/unternehmen/it-medien/medienbericht-deutsche-e-mail-anbieter-profitieren-von-nsa-affaere/v_detail_tab_print/8690072.html)

[73] Heise: Technische Probleme und schwache Nachfrage: Cisco schwächelt; 13. Februar 2014 (http://www.heise.de/newsticker/meldung/Technische-Probleme-und-schwache-Nachfrage-Cisco-schwaechelt-2112133.html)

[74] Heise: Cisco wird weniger Netzwerk-Technik los; 15. Mai 2014 (http://www.heise.de/netze/meldung/Cisco-wird-weniger-Netzwerk-Technik-los-2190026.html)

[75] Siehe die aktuelle Cyber-Sicherheitsstrategie für Deutschland unter http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile

[76] Michael Mimoso: NSA Budget Doc Reveals Investment in Crypto-Breaking, Hacking, 30. August 2013 (http://threatpost.com/nsa-budget-doc-reveals-investment-in-crypto-breaking-hacking)

[77] Executive Office of the President of the United States: Fiscal Year 2015 Budget of the U.S. Government, 2014 (http://www.whitehouse.gov/sites/default/files/omb/budget/fy2015/assets/budget.pdf)