PRO PRIVACY

Abschlussbericht des Fraunhofer SIT

Verbundprojekt ProPrivacy - Technische und rechtliche Untersuchung von Privatheit unterstützenden Technologien

Gefördert durch das Bundesministerium für Bildung und Forschung (BMBF)

Förderkennzeichen 16KIS0092K

Tobias Hahn, Michael Herfert, Benjamin Lange

Fraunhofer SIT

09.09.2015

Inhalt

1. Einleitung

Beginnend im Juni 2013 veröffentlichten The Guardian, DER SPIEGEL, The Washington Post und andere Medien zahlreiche Details über Abhörprogramme der amerikanischen National Security Agency (NSA) und die britischen Government Communications Headquarters (GHCQ).[1] Damit wurde unter dem Begriff der „NSA-Affäre" eine Debatte in Gang gesetzt, die auf politischer, juristischer und technischer Ebene geführt wird.[2] Die von Edward Snowden zur Verfügung gestellten Dokumente zeichnen das Bild eines weltweiten Netzes von Spionagesystemen, das von der NSA und ihren Partnerdienste für eine umfassende Überwachung jeder Form der elektronischen Kommunikation genutzt wird.[3] Bekanntgeworden ist auch eine Beteiligung des Bundesnachrichtendienstes (BND) an Programmen der NSA in Form von Nutzung entsprechender Daten und Auskünfte auf Anfragen der NSA.[4] Verdachtsunabhängig werden in großem Umfang Daten des internationalen Internet-Verkehrs erfasst, ausgewertet und auf unbestimmte Zeit zentral gespeichert. Dies umfasst sowohl Inhaltsdaten von Kommunikation, als auch Bestands- und Nutzungsdaten und damit auch massenweise personenbezogene Daten. Zusätzlich wird auf privilegierte Weise auf Daten zugegriffen, die sich auf den Servern von US-Anbietern in den USA befinden. Genannt werden Apple, AOL, Google, Facebook, Microsoft, Skype, Yahoo und Youtube. Ziel der umfassenden NSA-Überwachung ist die Kontrolle aller digitalen Kommunikationsinhalte und Kommunikationsmetadaten im gesamten Internet.[5]

Die Spähaktionen greifen in die Grundrechte aller Internetnutzer ein und gefährden deren Privatheit.[6] Die von den Geheimdiensten gesammelten und ausgewerteten Daten bewegen sich dabei auf mehreren Ebenen und durchdringen viele Bereiche des täglichen Lebens.

Das Abhören von Internettelefonie mit HAMMERCHANT[7] und das Abfangen von E-Mails und SMS über TEMPORA, RAMPART-A[8] und DISHFIRE[9] betrifft die ***Kommunikationsinhalte*** und greift damit in das Fernmeldegeheimnis aus Art. 10 GG ein. Das Ausspähen von Kommunikationsinhalten stellt grundsätzlich einen tiefen Eingriff in die Privatsphäre der Nutzer dar. Obwohl der Grad der Beeinträchtigung nicht abstrakt bestimmt werden kann, können aus Kommunikationsinhalten insbesondere die Informationen bekannt werden, die durch gesetzliche Vorschriften besonders geschützt sind. Dies umfasst Angaben über die Gesundheit, politische Meinungen, sowie religiöse und philosophische Überzeugungen und damit Daten, die durch § 3 Abs. 9 BDSG besonders geschützt sind. Auch Daten,

[1] Spiegel 2013; Greenwald & MacAskill 2013; Greenwald 2014; Rosenbach & Stark 2014.
[2] Hoffmann-Riem 2014; Roßnagel, Jandt & Richter 2014; Hansen 2014; Saeltzer 2014; Waidner 2014.
[3] Siehe Greenwald 2014; vgl. auch die Zusammenfassungen zur NSA-Spähaffäre bei http://www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal; http://www.heise.de/thema/NSA.
[4] Leyendecker & Mascolo 2014; Mascolo 2015.
[5] Rosenbach & Stark 2014.
[6] Siehe für eine begriffliche Diskussion von „Privatheit": Forum Privatheit 2014.
[7] HAMMERCHANT dient zur Überwachung von VoIP-Gesprächen, siehe Gallagher & Greenwald 2014.
[8] TEMPORA und RAMPART-A sammeln alle Daten, die über transatlantische Glasfaserkabel gesendet werden, siehe Rosenbach & Stark 2014.
[9] Mit DISHFIRE werden täglich Millionen von SMS abgegriffen und ausgewertet, siehe Ball 2014.

die wegen strafrechtlichen Berufsgeheimnispflichten (z. B. für Ärzte, Anwälte und Sozialarbeiter) gemäß §§ 203, 355 StGB geschützt sind, oder Betriebs- und Geschäftsgeheimnissen gemäß Art. 12 und 14 GG, sind von der Überwachung betroffen.

Die Erhebung von Verkehrs-, Bestands- und Nutzungsdaten über PRISM[10] und das Erstellen von Profilen über XKEYSCORE[11] werten die gesammelten ***Verbindungsdaten*** aus, die auch als Verkehrsdaten (§ 3 Nr. 30 TKG) bezeichnet werden. Dies sind alle Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet und genutzt werden, insbesondere die Anschlusskennung von Sender und Empfänger der Nachricht – Telefonnummer oder IP-Adresse – sowie Beginn, Ende, Datum und Uhrzeit der Verbindung. Zu den bei der E-Mail-Kommunikation anfallenden Verbindungsdaten gehören ferner die Adressen von Empfänger und Sender, der Betreff und die Sendezeit. Durch eine Analyse dieser Daten können soziale Gruppen erkannt und Beziehungsgraphen erstellt werden. Eine Analyse dieser Datensätze kann umfangreiche Aufschlüsse über die Kommunikationsbeziehungen der von der Ausspähung Betroffenen geben und ist damit geeignet, einen durch das Fernmeldegeheimnis geschützten Bereich der privaten Kommunikation massiv zu beeinträchtigen. Auch die Intensität der Beziehungen zu den Kontakten kann anhand der Häufigkeit der Kommunikation abgeschätzt werden.

Ein besonderer Fall von Verkehrsdaten sind ***Positionsdaten***, wie sie insbesondere bei Mobilfunkkommunikation anfallen. Da ein Mobiltelefon immer in eine Basisstation eingebucht sein muss, kann hierüber die ungefähre Position des Nutzers bestimmt werden, da die Basisstationen eindeutig identifizierbar sind und deren Position bekannt ist.[12] Darüber hinaus weisen mittlerweile die meisten mobilen Endgeräte die Möglichkeit der Positionsbestimmung über weitere Technologien, wie z. B. GPS oder WLAN auf. Werden Daten dieser Art über einen längeren Zeitraum erfasst, können genaue Bewegungsprofile des Nutzers erstellt werden. Anhand bestimmter Bewegungs-Muster wiederum kann direkt auf das Verhalten des Nutzers geschlossen werden.[13] Indem die so erstellten Bewegungsprofile vieler Nutzer in eine große Datenbank zusammengeführt werden, lassen sich auch bisher noch unbekannte Verbindungen zwischen Nutzern erkennen, z. B. wenn diese sich über einen bestimmten Zeitraum auf den gleichen Wegen befinden. Dieses Verfahren wird von der NSA im Rahmen des CO-TRAVELER Programms[14] eingesetzt, wobei zusätzlich zur Bewegung noch weitere Auswahlkriterien zum Einsatz kommen können. Auch dieses ist geeignet, zahlreiche Rückschlüsse auf die Persönlichkeit der Nutzer zu ziehen und private Belange aufzudecken.

[10] Über PRISM werden Google, Apple, Microsoft und andere gezwungen, Nutzerdaten herauszugeben, siehe Greenwald 2014.
[11] Mit XKEYSCORE können aus den riesigen Datenbanken der NSA in einem Such- und Analyseverfahren Profile zu einzelnen Personen angelegt werden, siehe Greenwald 2014.
[12] Genauigkeit in Großstädten bis zu 200 Meter bei einzelner Messung.
[13] Biermann 2011; vgl. http://www.zeit.de/digital/datenschutz/2011-02/vorratsdaten-malte-spitz.
[14] Electronic Frontier Foundation, https://www.eff.org/deeplinks/2013/12/meet-co-traveler-nsas-cell-phone-location-tracking-program.

Zunehmend werden Haushalte und die Geräte im und am Haus vernetzt und damit an das Internet angeschlossen. Diese Entwicklung wird unter dem Begriff „***Smart Home***“ zusammengefasst. Damit sind auch Daten aus privaten Haushalten als dem Inbegriff der Privatsphäre im räumlichen Sinne den großflächigen Ausspähprogrammen der Geheimdienste ausgesetzt. Der Schutz der durch Art. 13 GG gewährleisteten räumlichen Privatsphäre kann somit massiv beeinträchtigt werden. Viele private Haushalte spannen heute schon ihr eigenes privates Netzwerk auf, meist durch den Anschluss eines DSL-Modems, das mehrere LAN-Geräte bedienen kann und gleichzeitig ein WLAN-Zugangspunkt ist. Die Nutzung des eigenen Netzwerks wird sehr stark zunehmen, wenn die Industrie immer mehr Geräte anbietet, die netzwerkfähig sind. Smart-TV, Smart-Metering, eBook-Lesegeräte und vernetzte Spielekonsolen sind erst der Anfang. Die Analyse der Kommunikationsdaten im „Smart Home“ kann zu einer detaillierten Beschreibung der Lebensgewohnheiten der in ihm lebenden Personen führen.

Der massiven Bedrohung der Privatsphäre in diesen vier Bereichen (Kommunikationsinhalte, Verbindungsdaten, Positionsdaten, Daten im Smart Home) stehen Privatpersonen häufig hilflos gegenüber. Es existieren technische Maßnahmen, die Schutz vor Ausspähung der über das Internet übermittelten Daten bieten können. Sie werden allerdings zögernd eingesetzt, obwohl sich die Bürger mitunter gegenüber der bekannt gewordenen Bedrohung durch Geheimdienste zunehmend unsicher fühlen. Diese Spannung kann als eine Form des „Privacy-Paradoxon“ angesehen werden[15], bei dem Nutzer angeben sich Sorgen um ihre Datensicherheit zu machen, aber gleichzeitig ihre eigenen Daten auf z. B. Facebook veröffentlichen. Es ergeben sich aufgrund des NSA-Skandals zahlreiche Fragen in Bezug auf die Gefährdung und Möglichkeiten zum Schutz der Privatsphäre. Dies umfasst sowohl die Frage nach dem genauen Bedrohungspotential der Ausspähung in diesen Bereichen, die Frage nach verfügbaren Schutzmaßnahmen und deren technischer Bewertung, die Verbreitung solcher Schutzmaßnahmen und Gründen für eine mangelnde Nutzung sowie schließlich die Fragen nach nutzungsfördernden Konzepten und neuen Technologien.

Diese Fragen werden in dem vorliegenden Abschlussbereich des Projektes „ProPrivacy“ aufgegriffen und behandelt. Dabei wird für jeden der oben genannten Bereiche jeweils ein Überblick über den aktuellen technischen Stand und das tatsächliche Bedrohungspotential für die Privatsphäre gegeben. Ferner werden die gegenwärtig verfügbaren Schutzmaßnahmen zusammengestellt und bezüglich ihrer Schutzwirkung und Verbreitung analysiert. Die Analyse erfolgt zunächst durch einen Überblick über die in jedem Bereich verorteten Techniken und wird jeweils in einem Analyseschwerpunkt anhand einer exemplarischen Technologie konkretisiert. Für Kommunikationsinhalte bildet die Analyse von E-Mail-Kommunikationsinhalten den Schwerpunkt, während die Untersuchung von Verbindungsdaten am Beispiel von Internet-Kommunikationsdaten untersucht wird. Techniken zur Positionsbestimmung werden schwerpunktmäßig anhand der bei der Nutzung von Mobiltelefonen anfallenden Daten analysiert, während im Bereich Smart Home die exemplarische Behandlung anhand von Smart-TV-Geräten erfolgt. Für jeden der vier un-

[15] Kramer & Utz 2009.

tersuchten Bereiche werden neben der Darstellung derzeit verfügbarer Schutzmaßnahmen gegen eine Ausspähung der Daten Gründe für deren tendenziell geringe Verbreitung analysiert. Daraus werden nutzungsfördernde Kriterien abgeleitet und neue Technologien vorgeschlagen, die sowohl hinsichtlich Schutzwirkung als auch Nutzerfreundlichkeit einen flächendeckenden Schutz versprechen und Gegenstand von zukünftigen Entwicklungen sein sollten.

Der vorliegende Bericht gliedert sich in vier Kapitel, die den vier behandelten Bereichen entsprechen. Aufgrund der Diversität der behandelten Bereiche und der jeweils behandelten Probleme und Techniken werden die wesentlichen Ergebnisse und Implikationen am Schluss jedes Kapitels in einem eigenen Fazit zusammengefasst.

2. Kommunikationsinhalte

Kommunikationsinhalte sind alle Inhalte, die bei schriftlicher oder mündlicher Kommunikation über die verschiedensten Kommunikationskanäle wie Telefonfestnetz, Mobilfunk oder Internet ausgetauscht werden. Dabei kommt eine Vielzahl an Kommunikationsformen zum Einsatz: Neben klassischen Kommunikationsformen wie Telefon und Brief wird die tägliche Kommunikation in zunehmendem Maße über SMS und Handygespräche, sowie über internet-basierte Dienste wie E-Mail, Messagingdienste, Chat/Voice-Chat und soziale Netzwerke geführt. Gerade die neueren elektronischen Kommunikationsformen haben zu einer starken Steigerung an ausgetauschten Nachrichten und Gesprächen sowie zu einem geänderten Kommunikationsverhalten insgesamt geführt, bei dem sich punktueller und gezielter Informationsaustausch immer mehr in Richtung einer kontinuierlichen und von Multitasking geprägten Alltags-Kommunikation verschiebt.[16] Dementsprechend aussagekräftig sind auch die über die verschiedensten Kommunikationsformen ausgetauschten Kommunikationsinhalte, anhand derer sich nicht nur das Leben einer Person detailliert nachvollziehen lässt, sondern die auch Lebensgewohnheiten, Einstellungen, Lebensumstände, Beziehungen bis hin zu den intimsten Details preisgeben. Diese Zunahme an alltäglicher Kommunikation und Aussagekraft über einzelne Personen steht gerade vor dem Hintergrund massenhafter Überwachung in auffälligem Missverhältnis zu den zahlreichen Angriffsmöglichkeiten auf die Kommunikationsinhalte und führt zu einem Bedarf an Schutzmöglichkeiten, um die Vertraulichkeit der Kommunikation sicher zu stellen.

In diesem Kapitel werden nach einer kurzen Einführung in Verschlüsselungsmethoden zu den gängigsten Kommunikationsformen jeweils die Angriffsmöglichkeiten und die derzeit verfügbaren Techniken zum Schutz der Kommunikationsinhalte dargestellt. Ein besonderer Schwerpunkt sind dabei E-Mail-Kommunikationsinhalte. Daran schließt sich eine Evaluierung der Verbreitung der genannten Schutzmaßnahmen, deren Potential zum Schutz der Vertraulichkeit von Kommunikation sowie eine Übersicht über Möglichkeiten an, die geeignet sind, einen flächendeckenden Einsatz von Schutzmaßnahmen zu ermöglichen.

2.1. Überblick über Techniken der Kommunikation und mögliche Schutzmaßnahmen der Kommunikationsinhalte

Dieser Abschnitt gibt einen Überblick über die am häufigsten verwendeten Kommunikationskanäle und –techniken. Ferner werden derzeit verfügbare Schutzmaßnahmen kategorisiert und im Hinblick auf ihre Schutzwirkung und Verwendbarkeit analysiert. Da Verschlüsselung in den allermeisten Fällen das wirksamste Mittel für den Schutz von Kommunikationsinhalten darstellt,[17] beginnt die Darstellung mit einer Erläuterung der grundlegenden Verschlüsselungsmechanismen.

[16] Meier 2012.
[17] Gaycken 2014; Waidner 2014.

2.1.1. Grundbegriffe der Verschlüsselung

Der wirksamste Schutz von Kommunikationsinhalten besteht in einer Verschlüsselung der Inhalte. Dabei werden zwei Formen der Verschlüsselung unterschieden:

Transportverschlüsselung: Diese besteht in einer verschlüsselten Übermittlung von Kommunikationsinhalten auf verschiedenen Teilstrecken der Kommunikation. An Zwischenstationen werden die Inhalte entschlüsselt und für die nächste Teilstrecke neu verschlüsselt. Die Inhalte sind damit auf den Transportwegen verschlüsselt, liegen jedoch ungeschützt an allen Zwischenstationen vor. Transportverschlüsselung kommt häufig bei der Verschlüsselung von E-Mails durch SSL bzw. TLS zum Einsatz.

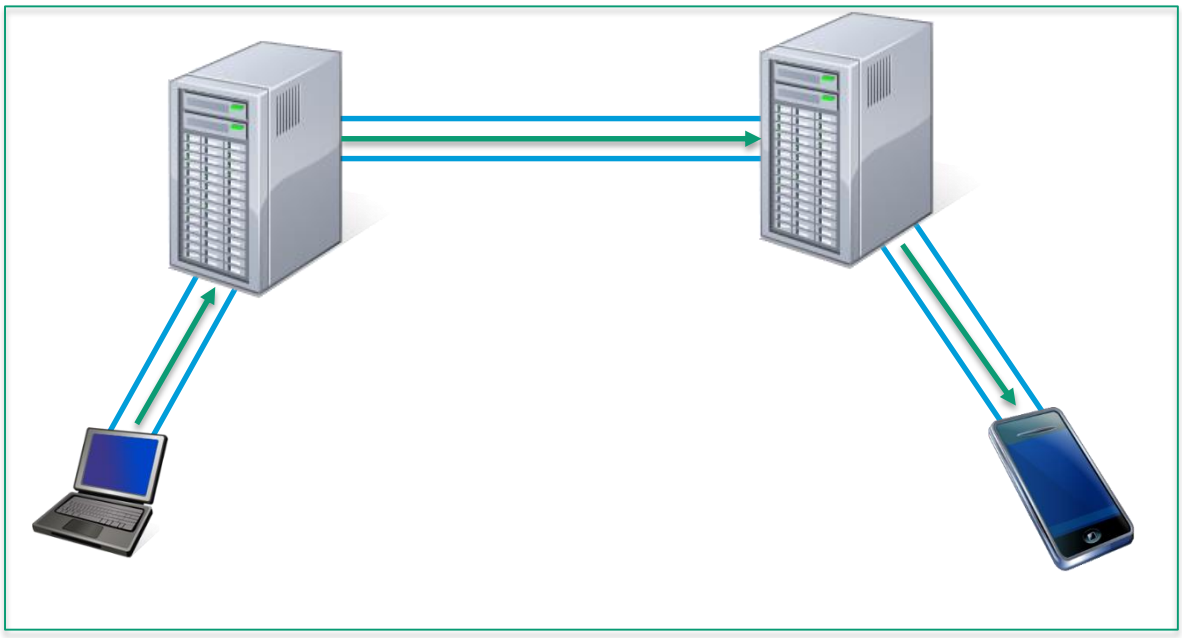

Abb. 1: Transportverschlüsselung

Ende-zu-Ende-Verschlüsselung: Diese besteht im Gegensatz zu Transportverschlüsselung in einer Verschlüsselung der übertragenen Inhalte über alle Zwischenstationen hinweg, so dass die Inhalte nur beim Absender und Empfänger entschlüsselt vorliegen. Die dazu notwendigen Schlüssel sind nur dem Absender und Empfänger bekannt. Ende-zu-Ende-Verschlüsselung kann durch die Verschlüsselung von E-Mails mit PGP oder S/MIME (siehe Abschnitt 2.2.3) erreicht werden.

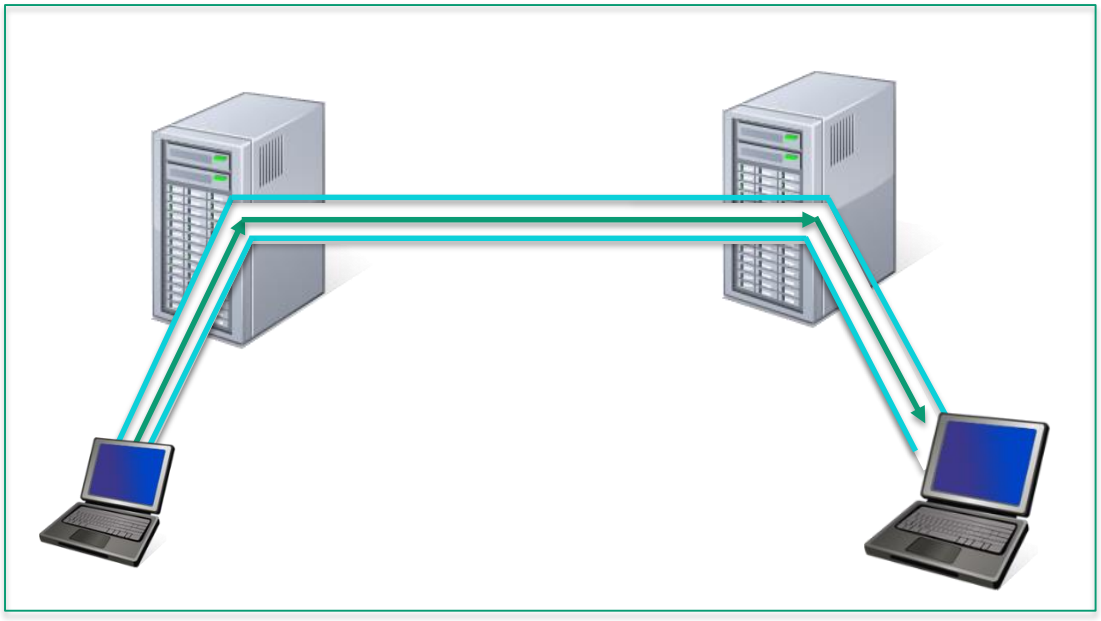

Abb. 2: Ende-zu-Ende-Verschlüsselung

Neben Transportverschlüsselung und Ende-zu-Ende-Verschlüsselung gibt es zahlreiche Kombinationsmöglichkeiten beider Verfahren.

Verschlüsselung setzt das Vorhandensein von geheimem Schlüsselmaterial bei Absender und Empfänger voraus. Dabei wird zwischen zwei unterschiedlichen Arten von Verschlüsselungsverfahren unterschieden:

Symmetrische Verschlüsselung: Absender und Empfänger verfügen über denselben geheimen Schlüssel, der nur ihnen bekannt ist. Nachrichten werden mit diesem Schlüssel verschlüsselt und wieder entschlüsselt. Ein bekanntes symmetrisches Verschlüsselungsverfahren ist der „Advanced Encryption Standard“, auch bekannt als AES.

Asymmetrische Verschlüsselung: Absender und Empfänger verfügen jeweils über ein Schlüsselpaar. Dieses besteht aus einem geheimen Schlüssel, der nur dem Besitzer selbst bekannt ist, und einem öffentlichen Schlüssel, der öffentlich bekannt und dem Besitzer zugeordnet ist. Nachrichten werden stets mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und können nur mit dem geheimen Schlüssel des Empfängers wieder entschlüsselt werden. Ein bekanntes asymmetrisches Verschlüsselungsverfahren ist RSA, benannt nach seinen drei Erfindern (Rivest, Shamir, Adleman).

Sowohl symmetrische wie asymmetrische Verschlüsselungsverfahren setzen voraus, dass Schlüssel zwischen Absender und Empfänger ausgetauscht werden müssen. Durch die Verwendung von öffentlichen Schlüsseln ist der Schlüsselaustausch bei asymmetrischen Verfahren einfacher, allerdings sind diese deutlich langsamer als vergleichbare Sicherheit bietende symmetrische Verfahren. In der Praxis werden daher die beiden Verfahren häufig miteinander kombiniert (hybride Verschlüsselung).

2.1.2. Telefon-Kommunikation

Telefonkommunikation beschreibt gesprochene Kommunikation über Telefon oder Mobiltelefon. Diese kann entweder über Festnetz, Mobilfunk oder VoIP (Voice-over-IP) übermittelt werden.

Festnetz

Die Übertragung von Telefongesprächen über Festnetz erfolgt grundsätzlich unverschlüsselt. Das Mitverfolgen und Mitschneiden von Telefonkommunikation durch den Telefonanbieter ist technisch sehr leicht möglich, gesetzlich jedoch nicht zulässig. Für Auslandsgespräche liegt eine Gefährdung der Vertraulichkeit der Kommunikation durch ausländische Geheimdienste vor.[18] Die über Kabel oder Satellit übermittelten Gespräche werden umfassend von Geheimdiensten mittels Software gefiltert und überwacht.[19] Für Inlandsgespräche liegt die größte Gefahr von abgehörten Telefongesprächen darin, dass Telefonleitungen gezielt von Unbefugten angezapft und abgehört werden können. Dies ist bereits mit einfachen technischen Mitteln möglich, sofern ein Zugang zur Telefonleitung besteht. Privatpersonen können sich nur unzureichend gegen die Überwachung von Telefonaten über Festnetz schützen. Spezielle Lösungen durch Verschlüsselung der Gespräche durch Gateways oder eigens dafür konzipierten Telefongeräten ist oftmals mit hohen Kosten verbunden.[20]

Voice-over-IP (VoIP)

Größere Gefahren für die Vertraulichkeit der Kommunikationsinhalte ergeben sich, sofern Telefongespräche nicht analog sondern digital über Voice over IP (VoIP) übertragen werden. In diesem Fall werden die Gespräche als digitale Datenpakete über das Internet übertragen und sind damit anfällig für Angriffe in IP-Datennetzen wie etwa *Spoofing* oder *Sniffing*.[21]

VoIP bezeichnet das Telefonieren über das Internet. Die akustischen Signale werden dabei digitalisiert und als Datenpakete über das Internet übertragen. VoIP wird sowohl über Internettelefone, die an einen Router angeschlossen sind, verwendet, als auch über kostenlose Voice-Chat-Dienste (z. B. Skype, Google Talk, iChat; siehe dazu Abschnitt 2.1.5). Ferner werden für Auslandsgespräche häufig sog. „Billig-Vorwahlnummern“ verwendet, die das Gespräch per VoIP über das Internet leiten.

Telefongespräche finden in den letzten Jahren vermehrt über VoIP statt: Von 2008 auf 2009 stieg das VoIP-Gesprächsvolumen um 40%; von 2009 auf 2010 erhöhte sich der

[18] Siehe etwa „NSA kann alle Telefonate eines Landes abhören“, Süddeutsche Zeitung vom 18.03.2014, verfügbar unter http://www.sueddeutsche.de/digital/internet-ueberwachung-nsa-kann-alle-telefonate-anderer-staaten-abhoeren-1.1916436

[19] Rosenbach & Stark 2014.

[20] Vgl. z. B. die Lösungen von Securstar (http://www.securstar.de/abhoersicher-telefonieren.html).

[21] Vgl. die entsprechende Warnung des BSI: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05012.html

Nutzer um 18% auf 10,3 Millionen regelmäßige Nutzer. [22] Von 2010 auf 2011 stieg die Anzahl der Nutzer erneut um 13,5% auf 11 Millionen Nutzer. [23] Von 2011 bis 2013 ist das Marktvolumen von VoIP-Lösungen ebenfalls stetig gestiegen. Diese Steigerung wird sich nach Prognosen fortsetzen.[24]

Als Sicherheitslösung besteht die Möglichkeit, die Daten per Secure Real-Time Transport Protocol (SRTP) zu verschlüsseln. Dieses Verfahren wird vom BSI empfohlen,[25] wird jedoch aus verschiedenen Gründen unzureichend genutzt:

- Nicht alle Anbieter von Internettelefonie unterstützen SRTP
- Die Endgeräte der Gesprächsteilnehmer müssen SRTP unterstützen
- Die Verschlüsselung kann die Sprachqualität beeinträchtigen
- Sowohl die Anfälligkeit von VoIP für Angriffe als auch die Möglichkeit der Verschlüsslung mittels SRTP sind nur unzureichend bekannt

Alternativen zu SRTP sind Verschlüsselung mittels TLS oder spezielle Lösungen von Internettelefonie-Anbietern. Dabei bestehen grundsätzlich dieselben Probleme wie bei der Verwendung von SRTP.

Mobilfunk

Mobilfunkkommunikation wird weltweit hauptsächlich mittels des GSM-Standards übertragen. In Deutschland wird dabei auch standardmäßig verschlüsselt. Dabei wird eine symmetrische Verschlüsselung (A5/1) mit kurzer Schlüssellänge (64Bit) verwendet. Diese bereits 1987 entwickelte Verschlüsselung gilt jedoch als unsicher und kann in Echtzeit unter Verwendung eines üblichen PCs gebrochen werden.[26] Im Rahmen der NSA-Affäre wurde bekannt, dass die NSA umfassend Handy-Gespräche abhört und die Verschlüsselung von GSM gebrochen hat.[27] Mehr Sicherheit verspricht der Nachfolgestandard zur GSM-Verschlüsselung A5/3 mit Schlüssellängen von 128 Bit. Die Netze der deutschen Telekom wurden bereits Ende 2013 auf den neuen Standard umgestellt,[28] während bei anderen Dienstanbietern noch der alte Standard verwendet wird.

---

[22] Presseinformation BITKOM vom 6.4.2010, http://www.bitkom.org/files/documents/BITKO-_Presseinfo_VoIP_06_04_2010.pdf.
[23] Vgl. http://www.trendsderzukunft.de/internettelefonie-im-trend-voip-telefonie-hat-mehr-als-11-millionen-nutzer/2011/02/02/.
[24] Siehe http://www.experton-group.de/research/ict-news-dach/news/article/auch-im-ucc-zeitalter-waechst-der-voip-markt.html.
[25] Siehe https://www.bsi-fuer-buerger.de/BSIFB/DE/SicherheitImNetz/Verschluesseltkommunizieren/Einsatzbereiche/einsatzbereiche_node.html.
[26] Nohl & Paget 2010. Vgl. ferner Nohl 2010.
[27] Siehe http://www.heise.de/newsticker/meldung/Zeitung-NSA-kann-auf-breiter-Front-Handys-abhoeren-2065990.html.
[28] Siehe http://www.wiwo.de/unternehmen/it/datenschutz-telekom-fuehrt-neue-verschluesselungstechnik-fuer-handygespraeche-ein/9180638.html.

Neben dem Brechen der Verschlüsselung können Handy-Gespräche von Geheimdiensten auch über IMSI-Catcher dazu angewiesen werden, die Kommunikation unverschlüsselt abzuwickeln.[29] Daneben können Handy-Gespräche auch durch einfache Spionage-Apps abgehört werden, sofern der Angreifer einmalig Zugriff auf das ausspionierte Gerät hatte.[30]

Sicherheit für die vertrauliche Übertragung von Mobilfunkgesprächen bietet hier nur eine sichere Ende-zu-Ende-Verschlüsselung. Verschlüsselung von Gesprächen oder SMS über Smartphones kann durch Verwendung von Apps wie den folgenden erreicht werden:[31]

- Silent Phone[32] ist eine App der Firma *Silent Circle*, die Verschlüsselung von Handy-Kommunikation zur Verfügung bietet. Die Kommunikation (SMS, Telefonate) verläuft dabei nicht über GSM, sondern über ein VPN von Silent Circle via VoIP, also datenbasiert (3G- oder WLAN-Verbindung). Verwenden beide Gesprächspartner Silent Phone, so wird über das VPN eine verschlüsselte Kommunikation hergestellt. Der Schlüsselaustausch erfolgt dabei automatisch über die Server von Silent Circle.
- RedPhone[33] ist eine Open-Source Android-App, die Gespräche über VoIP überträgt. Die Verschlüsselung erfolgt mit AES und ist nur möglich, wenn beide Gesprächsteilnehmer RedPhone nutzen. Der Schlüsselaustausch erfolgt dabei automatisch.

2.1.3. SMS

SMS werden wie Mobilfunkgespräche über die GSM-Verschlüsselung A5/1 bzw. A5/3 verschlüsselt. Um sich vor den Sicherheitslücken in der unsicheren Verschlüsselung A5/1 zu schützen, können SMS durch die Verwendung spezieller Apps verschlüsselt übertragen werden. Verschlüsselte Kommunikation per SMS bieten etwa die folgenden Apps:

- Silent Phone (s.o.)
- TextSecure: Die App kann sowohl als Messenger als auch zu Verschlüsselung von SMS verwendet werden. Um SMS verschlüsselt zu übertragen, muss sowohl der Absender als auch der Empfänger die App installiert haben. Der Schlüsselaustausch erfolgt dann automatisch. Im Betriebssystem CyanogenMod[34] wird die Verschlüsselung über die Server von TextSecure standardmäßig implementiert und kann über

[29] Vgl. http://www.spiegel.de/netzwelt/netzpolitik/gsm-verschluesselung-die-nsa-kann-fast-alle-handy-gespraeche-abhoeren-a-939049.html.
[30] Entsprechende Tools umfassen z. B. mSpy, Flexyspy, Stealthgenie.
[31] Siehe http://www.abendzeitung-muenchen.de/inhalt.angst-vorm-abhoeren-ueberwachen-orten-mitlesen-was-ihr-handy-ueber-sie-verraet.html.
[32] Siehe www.silentcircle.com.
[33] Siehe https://play.google.com/store/apps/details?id=org.thoughtcrime.redphone&hl=de
[34] CyanogenMod ist ein freies mobiles Betriebssystem und stellt ein Derivat von Android dar.

jede beliebige SMS-App genutzt werden, sofern auch das Gerät des Empfängers Verschlüsselung über TextSecure unterstützt.[35]

Weitere Alternativen zur verschlüsselten Übertragung von Kurznachrichten stehen zur Verfügung, wenn Kurznachrichten nicht über Mobilfunk (GSM), sondern IP-basiert (z. B. WLAN, 3G) unter Verwendung von Messaging-Diensten übermittelt werden.

2.1.4. Messaging-Dienste

Die Kommunikation über SMS wird zunehmend durch Messaging-Dienste (z. B. WhatsApp, Viber, Google Hangouts, Skype, etc.) ersetzt.[36] Alleine der Marktführer WhatsApp hat weltweit 400 Millionen aktive Nutzer, davon 30 Mio. in Deutschland. Weltweit werden täglich 18 Milliarden Nachrichten inkl. Bilder, Videos und Sprachnachrichten versandt.[37]

WhatsApp verlangt umfangreiche Rechte (u. a. Zugriff auf alle persönlichen Kontakte, Bilder, Standort sowie auf das Mikrofon). Was genau mit den Daten, auf die WhatsApp Zugriff hat, geschieht, ist nicht transparent und unklar. WhatsApp steht schon länger in der Kritik, das Adressbuch des Nutzers und andere Daten auf amerikanischen Servern zu speichern.[38]

Die Kommunikationsinhalte sind bei den meisten Messanger zwar durch Verschlüsselung geschützt, dabei wird jedoch selten Ende-zu-Ende-Verschlüsselung verwendet, so dass die Nachrichten auf den Servern der Betreiber im Klartext vorliegen. Keine Ende-zu-Ende-Verschlüsselung verwenden etwa Viper, Google Hangouts, Snapchat, iMessage. Wird eine Verschlüsselung verwendet, kommen dabei häufig unsichere Algorithmen zum Einsatz.[39] Messenger-Apps mit Ende-zu-Ende-Verschlüsselung bieten dagegen WhatsApp, Threema, Surespot, ChatSecure, Telegram, Text Secure oder Whistle.[40]

2.1.5. Chat und Voice-Chat

Es lassen sich zwei Arten des Chats unterscheiden: IRC (Internet Relay Chat) und IM (Instant Messaging). Beispiele für ersteres sind Chat-Rooms im Internet, die entweder öffentlich zugänglich oder privat sein können. Beispiele für letzteres sind IM-Systeme wie AOL IM, ICQ, MSN oder der Yahoo-Messenger.

---

[35] Siehe http://www.golem.de/news/android-distribution-cyanogenmod-versendet-sms-verschluesselt-1312-103278.html.
[36] Braun 2014a.
[37] Vgl. https://www.focus.de/digital/internet/messenger-auf-dem-vormarsch-whatsapp-attackiert-facebook-der-kampf-um-das-mobile-internet-1_id_3548922.html.
[38] Vgl. http://www.wdr.de/tv/markt/sendungsbeitraege/2013/1202/whatsapp.jsp.
[39] Braun 2014b.
[40] Janssen 2014 und http://www.test.de/WhatsApp-und-Alternativen-Datenschutz-im-Test-4675013-0/

Sicherheitsprobleme beim Chat sind nach Ansicht des BSI[41] vor allem:

- Unverschlüsselte Übertragung der Daten über das Internet: Da keine Verschlüsselung verwendet wird, können die Kommunikationsinhalte von allen Vermittlungsrechnern mitgelesen werden.
- Verwendung von Skripten: Viele IM-System bieten die Anpassung von Funktionen über selbst erstellte Skripte an. Diese Möglichkeit kann von Angreifern dazu verwendet werden, Kommunikationsinhalte mitzulesen.
- Mangelhafter Kennwortschutz: Da die Verwaltung von Zugangskennwörter nicht gesichert ist, können Accounts gehackt und die protokollierten Kommunikationsinhalte eingesehen werden.
- Datenschutz: Die Datenschutzbestimmungen von vielen IM-Systemen erlauben es den Anbietern, die Kommunikationsinhalte einzusehen oder sogar beliebig weiterzuverwenden (z. B. durch Veröffentlichung).

Maßnahmen zur sicheren und vertraulichen Übertragung von Kommunikationsinhalten sind:

- Verschlüsselung: Einige Chat-Anbieter verwenden verschlüsselte Übertragung (z. B. Skype, Jitsi).[42] Dies schützt teilweise vor Zugriff durch unbefugte Dritte. Eine Überwachung durch den Anbieter oder Ermittlungsbehörden, ist allerdings teilweise immer noch gegeben. So ist Microsoft als Betreiber von Skype dazu in der Lage, auf den Klartext der verschlüsselt übertragenen Nachrichten zuzugreifen.[43]
- Off-the-record-Verschlüsselung (OTR): OTR ist eine Ende-zu-Ende-Verschlüsselung, die unter anderem von den Chat-Clients Psi, Miranda IM, Pidgin und Adium unterstützt wird. Die Kommunikationsinhalte werden damit vor dem Zugriff durch Dritte geschützt, selbst wenn alle Kommunikationsdaten vom Anbieter gespeichert werden.
- Mit dem Browser-Addon BlockPRISM[44] können Facebook-Chats verschlüsselt werden, sofern beiden Kommunikationsteilnehmer über das Addon verfügen. Die Verschlüsselung erfolgt mit einem asymmetrischen Verfahren, das Addon erzeugt für den Nutzer ein Schlüsselpaar, und führt mit allen anderen Kommunikationsteilnehmern den Schlüsselaustausch durch.

[41] https://www.bsi-fuer-buerger.de/BSIFB/DE/SicherheitImNetz/KommunikationUeberInternet/ChatAberSicher/Sicherheitsrisiken/sicherheitsrisiken_node.html.
[42] Jendrian 2014.
[43] Fakten und Spekulationen zu Skypes ominösen Link-Checks, http://heise.de/-1865370.
[44] BlockPRISM-Addon: https://chrome.google.com/webstore/detail/blockprismorg-encrypted-f/.

Eine andere Möglichkeit, Kommunikationsinhalte zu schützen ist die Verwendung von Virtual Private Networks (VPNs). Diese bieten zwar die Möglichkeit, Daten zwischen Teilnehmern eines VPN-Netzwerkes sicher zu übertragen, jedoch müssen sich alle Kommunikationspartner im VPN befinden.

Voice-Chat-Dienste bieten neben einer Chat-Funktion zusätzlich die Möglichkeit der VoIP-Telefonie. Da die Kommunikationsdaten bei VoIP als Datenpakete durch das Internet geleitet werden, sind sie damit auch anfällig für verschiedene Arten von Angriffen (Phishing, ARP-Spoofing, Denial-of-Service, VoIP-Spam, Phreaking).

Kommunikationsinhalte sind optimal gesichert, sofern eine Ende-zu-Ende-Verschlüsselung verwendet wird. Die meisten Voice-Chat-Dienste verwenden gar keine Verschlüsselung oder Verschlüsselung mittels SSL bzw. TLS, wobei die Kommunikationsdaten auf den Servern der Anbieter im Klartext vorliegen.

2.1.6. Soziale Netzwerke

In sozialen Netzwerken geben Nutzer freiwillig persönliche Informationen preis und übermitteln Nachrichten an Andere. Die Kommunikationsinhalte müssen damit über den Kreis der Adressaten geschützt werden.

2.1.7. Internetkommunikation (Surfen)

Bei der Internetkommunikation können die abgerufenen Webseiten entweder im Klartext, oder verschlüsselt zwischen Server und Nutzer übertragen werden. Dabei werden die Protokolle HTTP für Klartext-Übertragung, bzw. HTTPS für verschlüsselte Übertragung verwendet.[45] Inhalte vieler Websites werden nach wie vor unverschlüsselt übertragen. Mit speziellen Addons, wie dem von der EFF entwickelten „HTTPS-Everywhere“[46] für Firefox, kann zumindest für solche Server, die HTTPS bereitstellen, eine verschlüsselte Verbindung erzwungen werden.

Bei Seiten, die standardmäßig HTTPS verwenden, gibt es große Unterschiede in der Qualität der verwendeten Verschlüsselung:

- Viele Seiten verwenden bei der Verschlüsselung den Algorithmus RC4, der seit dem NSA-Skandal als unsicher gilt.
- Nicht alle Browser unterstützten den aktuellsten Verschlüsselungsstandart TLS 1.2.
- Nur wenige Webseiten verwenden Diffie-Hellman-Schlüsselaustausch (Forward Secrecy).
- Bei den Zertifikaten gibt es große Qualitätsunterschiede.[47]

[45] HTTP(S): Hyper Text Transfer Protocol (Secure).
[46] HTTPS Everywhere, schaltet automatisch auf gesicherte Verbindung um, falls verfügbar. https://www.eff.org/de/https-everywhere.
[47] Bager & Schmidt 2014.

- Einige Webseiten sind anfällig für bekannte Attacken (z. B. BEAST, Lucky Thirteen, etc.).

2.2. Schwerpunkt: Schutz von E-Mail-Kommunikationsinhalten

In diesem Abschnitt wird der Schutz von Kommunikationsinhalten am Beispiel von E-Mail-Kommunikation behandelt. Nach einer Analyse des bestehenden Schutzniveaus von E-Mails werden Anbieter und Technologien zum Schutz von E-Mails analysiert sowie mögliche Verbesserungen und neuartige Technologien vorgestellt.

2.2.1. Zustandsanalyse

Eine E-Mail nimmt ihren Weg vom Gerät (PC oder mobiles Gerät) des Absenders zunächst zum Mail-Server des Absenders (siehe Abbildung 3). Von dort wird sie zum Mail-Server des Empfängers weitergeleitet und dort vom Empfänger heruntergeladen. Um E-Mail-Kommunikationsinhalte vor unbefugtem Zugriff zu schützen, muss eine E-Mail daher sowohl auf dem Transportweg sowie auf den Mail-Servern von Absender und Empfänger sicher vor dem Zugriff Unbefugter sein.

Für deutsche E-Mail-Anbieter sind E-Mail-Inhalte auch auf den Servern der Anbieter durch das Briefgeheimnis geschützt. Eine Gefährdung der Inhalte liegt dann vor, wenn sich Hacker, Geheimdienste oder andere Unbefugte Dritte Zugriff auf die meist gut geschützten Server verschaffen. Bei ausländischen E-Mail-Anbietern sind Geheimdienste unter Umständen dazu befugt, Zugriff auf E-Mail-Postfächer zu erhalten.

Nach Nutzerumfragen aus dem Jahr 2013 werden von deutschen Nutzern vorwiegend deutsche E-Mail-Provider verwendet: Mit 56,7% hat United Internet (WEB.de mit 26,1%, GMX mit 26,3% und 1&1 mit 4,3%) die meisten Nutzer bei den deutschen E-Mail-Providern, gefolgt von T-Online (9,1%) und Freenet (3,8%). Bei den internationalen E-Mail-Providern hat Microsoft (7,7%) den größten Anteil, gefolgt von Google (6,5%), Vodafone (4,6%), Yahoo (3,9%) und anderen (3,3%).[48] Damit werden bei ca. 70% der deutschen Nutzer deutsche E-Mail-Anbieter verwendet, die E-Mails sind daher auf dem Server des Anbieters durch deutsche Gesetze geschützt. Da eine E-Mail jedoch sowohl den E-Mail-Server des Absenders wie auch des Empfängers durchläuft, liegt bei vielen der möglichen Kommunikationspaare aus Absender und Empfänger eine versendete E-Mail dennoch auf einem ausländischen E-Mail-Server.

Ebenso wichtig wie der Schutz der E-Mail auf den durchlaufenen E-Mail-Servern ist der Schutz der E-Mail auf den Transportwegen. Dieser wird bestimmt vom schwächsten Glied in der Kette: Wird eine E-Mail nur auf einem Teilstück des Transportweges nicht verschlüsselt, können die Inhalte trotz Verschlüsselung auf den anderen Teilstrecken leicht

[48] Siehe http://blog.inxmail.de/studien-und-trends/beliebtesten-e-mail-provider-in-deutschland/ Stand: Sept. 2013.

im Klartext durch Dritte mitgelesen werden. Waren noch 2013 Schätzungen zu Folge nur 15% des deutschen E-Mail-Verkehrs auf allen Transportwegen verschlüsselt,[49] haben in Folge des NSA-Skandals die meisten E-Mail-Anbieter standardmäßig auf eine Transportverschlüsselung zwischen Nutzer und E-Mail-Server sowie zwischen den E-Mail-Servern der Anbieter untereinander umgestellt.[50] Damit ist der Anteil der durchgehend transportverschlüsselten E-Mails deutlich gestiegen. Der größte Teil der deutschen E-Mail-Provider verwenden ab 2014 die Sicherheitsstandards der *E-Mail made in Germany* (siehe dazu Abschnitt 2.2.3). Unter den E-Mail-Providern bestehen dennoch Unterschiede hinsichtlich der Güte der verwendeten Verschlüsselungsalgorithmen und –parameter.

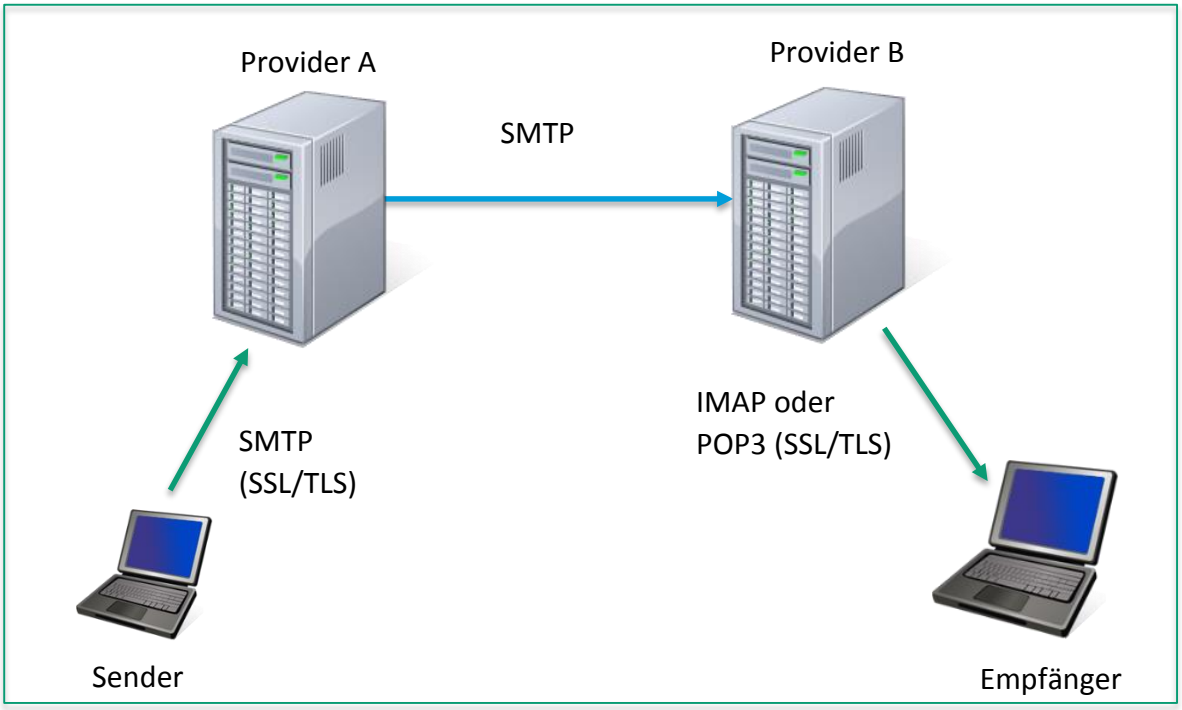

Abb. 3: E-Mail-Kommunikation

Wird die E-Mail-Kommunikation direkt über den Browser geführt (Webmail-Szenario), wird von allen größeren E-Mail-Provider standardmäßig SSL-Verschlüsselung (über HTTPS-Verbindung) verwendet,[51] so dass die E-Mails zwischen Benutzer und Web-Server des E-Mail-Providers verschlüsselt übertragen werden (dennoch liegt die E-Mail beim Mail-Server des Absenders sowie beim Mail-Server des Empfänger im Klartext vor, sofern keine Ende-zu-Ende-Verschlüsselung verwendet wird). Die dabei eingesetzte SSL-Verschlüsselung weist jedoch häufig Mängel auf oder entspricht nicht aktuellen Sicherheitsstandards. Mit Web.de, T-Online, Outlook und GMX wird für ca. 70% der deutschen E-

[49] Schätzung von United Internet Vorstandsmitglied Jan Oetjen gegenüber Zeit-Online, siehe http://www.zeit.de/digital/datenschutz/2013-08/email-telekom-gmx-verschluesselt.
[50] Mansmann 2014.
[51] Yahoo hatte dies als letzter der großen E-Mail-Provider im Januar 2014 umgesetzt, siehe http://www.computerbase.de/news/2013-01/yahoo-mail-unterstuetzt-nun-auch-ssl/.

Mail-Accounts eine HTTPS-Verbindung mit unzureichender Sicherheit verwendet.[52] So wird zur Verschlüsselung häufig noch der Algorithmus RC4 verwendet, der nach den technischen Richtlinien des BSI erhebliche Sicherheitsschwächen aufweist und nicht mehr eingesetzt werden sollte.[53] Ferner verwenden viele E-Mail-Provider veraltete Versionen der SSL-Verschlüsselung oder verzichten auf *Perfect Forward Secrecy*.[54]

Wird anstelle des Browsers ein Mail-Client verwendet, so muss der Benutzer selbst einstellen, ob zur Verbindung zum eigenen E-Mail-Provider SSL- bzw. TLS-Verschlüsselung verwendet werden soll. T-Online stellt als erster der großen E-Mail-Provider 2014 standardmäßig auf SSL-Verschlüsselung um, so dass E-Mails über einen Mail-Client nicht mehr unverschlüsselt übertragen werden können.[55] Bei der SSL-Verschlüsselung zwischen Mail-Client und E-Mail-Provider wird jedoch häufig auf schlechte Sicherheitsstandards zurückgegriffen. Wie beim Browser-basierten Zugang zum E-Mail-Server verwenden viele E-Mail-Provider auch beim Abrufen und Versenden von E-Mails mittels eines Mail-Clients[56] veraltete SSL- und TLS-Verschlüsselungen, teilweise unter Verwendung von RC4. So wird etwa TLS-Verschlüsselung mit guten Sicherheitsstandards nur von Anbietern mit sehr geringem Marktanteil (Freenet, Mail-de, Arcor, Posteo, Mailbox; Marktanteil zusammen unter 7%) angeboten.[57] Der überwiegende Teil der in Deutschland genutzten Mail-Provider unterstützt TLS-Verschlüsselung nur unzureichend oder gar nicht.[58] Verschlüsselte Kommunikation mit ausreichenden Sicherheitsstandards zwischen verschiedenen Mail-Servern ist damit häufig nur unzureichend umgesetzt.

2.2.2. Angriffsmöglichkeiten

Um Kommunikationsinhalte über E-Mail zu schützen, ist ein Schutz auf verschiedenen Ebenen sinnvoll. Diese müssen sowohl den Schutz der E-Mail auf den E-Mail-Servern von Absender und Empfänger wie auch den Schutz auf dem Transportweg mit einbeziehen. Insgesamt ergeben sich die folgenden Angriffsmöglichkeiten:

1. **Angriff auf den persönlichen Computer**
   Dies stellt die grundlegendste Form des Angriffes dar, die alle anderen Angriffsformen erübrigt. Hat ein Angreifer Zugriff auf den Computer, so ist damit auch bei Verwendung von Laufwerk- oder E-Mail-Verschlüsselung ein Mitlesen der gesamten E-

[52] Bager & Schmidt 2014.
[53] BSI 2013a; Bager & Schmidt 2014.
[54] SSL-Verschlüsselungen mit Perfect Forward Secrecy verwenden für jede Sitzung einen eigenen Sitzungsschlüssel. Wird ein Sitzungsschlüssel kompromittiert, kann nur ein Teil der verschlüsselten Kommunikation (und nicht die gesamte Kommunikation über mehrere Sitzungen hinweg) entschlüsselt werden.
[55] Siehe http://www.t-online.de/computer/id_66268354/ssl-verschluesselung-bei-t-online-de-das-sollten-e-mail-nutzer-wissen.html.
[56] Zur Kommunikation zwischen Mail-Client und Server werden die Protokolle IMAP bzw. POP zum Abrufen, und SMTP zum Versenden von E-Mails verwendet.
[57] Vgl. Bager & Schmidt 2014.
[58] Siehe http://www.golem.de/news/e-mail-provider-luecken-in-der-verschluesselungskette-1307-100429.html; Test von Juli 2013.

Mail-Kommunikation möglich. Durch Key-Logger können Passwörter ausgelesen werden und somit auch passwortgeschützte geheime Schlüssel ausgelesen werden. Präventiven Schutz gegen Angriffe auf den eigenen Computer bietet ein umsichtiges Surfverhalten im Internet,[59] der Einsatz einer Firewall, und regelmäßige Aktualisierungen aller verwendeten Programme. Zusätzlich dazu kann im Fall eines Befalls durch Trojaner oder Malware ein Virenscanner zur schnellen Detektion eingesetzt werden, um Schaden früh zu begrenzen oder sogar im Moment des Befalls abzuwehren.

2. **Angriff auf den Server eines E-Mail-Anbieters**
   Bei diesem Angriff versucht ein Angreifer, Zugriff auf den Server eines E-Mail-Anbieters zu bekommen, um Zugriff auf eine Anzahl von E-Mail-Postfächern zu erhalten. Je nach Art des Angriffes und der verwendeten Schutzmaßnahmen können dem Angreifer damit sämtliche auf dem Server befindliche E-Mails eines einzelnen Nutzers in die Hände fallen. Der Angriff kann entweder über das Internet oder durch physischen Zugriff auf die Server erfolgen. Einem solchen Angriff begegnen große E-Mail-Anbieter mit umfangreichen Schutzmaßnahmen, so dass ein erfolgreiches Eindringen in der Praxis nur selten vorkommt.

3. **Zugriff auf Kommunikationsinhalte oder geheimer Schlüssel durch Systemadministratoren**
   Im Gegensatz zum Angriff auf E-Mail-Server von außen verfügt hier der Angreifer über Rechte, die ihm den Zugang zu den Kommunikationsinhalten der Nutzer gestattet. Der Angriff stellt damit einen Missbrauch dieser Rechte dar und ist mit deutlich weniger Aufwand zu bewerkstelligen, als der Angriff von außen.

4. **Zugriff auf Kommunikationsinhalte durch staatliche Behörden**
   Der Zugriff durch staatliche Behörden kann nur zur Strafverfolgung oder Verbrechensprävention und nur aufgrund richterlicher Anordnung geschehen. Dabei können entweder Postfächern mit Kommunikationsinhalten aus der Vergangenheit beschlagnahmt werden, oder durch eine Quick-Freeze-Schnittstelle kann die Kommunikation für einen bestimmten Zeitraum mitverfolgt werden.

5. **Großflächige Überwachung von Netzwerkkommunikation**
   Dieser Angriff erfolgt nicht zielgerichtet auf einzelne Kommunikationsinhalte, sondern gefährdet die Inhalte durch großflächiges Abschöpfen an wichtigen Internetknotenpunkten. Sind die E-Mails unverschlüsselt, kann damit auf leichte Weise eine große Zahl von Kommunikationsinhalten abgeschöpft und automatisiert ausgewertet werden. Ferner können die Inhalte gespeichert und zu einem späteren Zeitpunkt gezielt verwendet werden.

[59] Siehe hier die vom BSI empfohlenen Maßnahmen auf der Internetseite www.bsi-fuer-buerger.de.

2.2.3. Techniken zur Verschlüsselung

Verschiedene Techniken ermöglichen die Verschlüsselung der E-Mail-Kommunikation auf allen Teilstrecken zwischen Absender und Empfänger. Im Unterschied zu Ende-zu-Ende-Verschlüsselung liegt die E-Mail jedoch an den Zwischenstationen (z. B. E-Mail-Server) unverschlüsselt vor. Verschlüsselte Kommunikation unter Verwendung von SSL wird durch die folgenden Techniken ermöglicht:

E-Mail made in Germany

Die deutschen E-Mail-Provider GMX, WEB.de und T-Online verwenden seit 2014 im Zuge Standardisierung der *E-Mail made in Germany*[60] nur noch verschlüsselte Kommunikation vom Benutzer zum Mail-Server und zwischen den Mailservern von GMX, WEB.de und T-Online. Damit werden zwei Drittel des deutschen E-Mail-Verkehrs zwischen den Servern der Mail-Provider verschlüsselt übertragen. Gegenüber gänzlich unverschlüsselter Kommunikation werden damit die Kommunikationsinhalte in E-Mails weitestgehend durch unbefugte Zugriffe durch Dritte geschützt.[61] Eine potentielle Schwachstelle ist jedoch dadurch gegeben, dass die E-Mails bei allen beteiligten E-Mail-Providern selbst unverschlüsselt vorliegen, und nur auf den Wegen zwischen E-Mail-Servern und Benutzern verschlüsselt werden. Bei den E-Mail-Servern selbst werden die E-Mails gescannt (Malware- oder Spamerkennung) und sind sowohl deutschen Sicherheitsbehörden als auch den Administratoren der Server zugänglich. Ferner ist die Verschlüsselung der *E-Mail made in Germany* unwirksam, sofern ein Provider in der Kommunikation involviert ist, der keine verschlüsselte Übertragung zwischen den E-Mail-Servern unterstützt.[62] Die Kommunikationsinhalte werden zudem auch dann ungesichert übertragen, sofern der Empfänger die E-Mails bei seinem E-Mail-Provider unverschlüsselt abruft. Ein umfassender Schutz der per E-Mail verschickten Kommunikationsinhalte ist durch *E-Mail made in Germany* daher nicht möglich.[63] Der Standard ist jedoch ein wichtiger Schritt dahin, auf den Transportwegen zwischen E-Mail-Providern untereinander sowie zwischen Nutzer und E-Mail-Provider standardmäßig verschlüsselte Übertragungen zu verwenden.[64]

De-Mail

De-Mail ist ein auf der E-Mail basierendes Verfahren zur vertraulichen Kommunikation, bei der sich Absender und Empfänger zudem gegenseitig authentisieren können. Auf der Grundlage des De-Mail-Gesetzes können sich E-Mail-Provider als De-Mail-Anbieter akkreditieren lassen, wenn sie die gesetzlichen Vorgaben erfüllen. De-Mail wird von Telekom, Mentana-Claimsoft und der United Internet AG (1&1, GMX.de, Web.de) angeboten. Die besonderen Stärken der De-Mail liegen darin, dass Absender und Empfänger sich gegenseitig authentisieren können und damit eine rechtsgültige elektronische Kommunikation (z. B. gegenüber Behörden) ermöglicht wird. In Bezug auf die Verschlüsselung zum Schutz

[60] Vgl. http://www.e-mail-made-in-germany.de/Verschluesselung.html. Siehe auch https://www.bsi.bund.de/DE/Themen/EGovernment/DeMail/DeMail_node.html.
[61] Gerling 2014.
[62] Dies betrifft häufig nur kleinere deutsche oder ausländische Provider, vgl. hierzu den „Sicherheitsreport 2015“ von mailbox.org unter https://mailbox.org/sicherheitsreport.
[63] Vgl. auch Bleich 2014.
[64] Gerling 2014.

der Kommunikationsinhalte ist De-Mail vergleichbar mit *E-Mail made in Germany*: Die De-Mails werden nur auf den Transportwegen zwischen den Providern verschlüsselt übertragen und liegen auf den Servern der beteiligten De-Mail-Anbieter im Klartext vor. Zum umfassenden Schutz der Kommunikationsinhalte ist De-Mail daher ungeeignet. Ein wesentlicher praktischer Nachteil besteht darin, dass De-Mail ein sich geschlossenes System ist. Es beruht zwar auf der herkömmlichen E-Mail, ist jedoch nicht mit dieser kompatibel. So können De-Mails nur an andere De-Mail-Adressen geschickt und von diesen empfangen werden. Eine flächendeckende Nutzung von De-Mail wird darüber hinaus auch durch die für das Versenden jeder De-Mail entstehenden Kosten von 0,33 bis 0,39 Euro (je nach Anbieter) verhindert. Damit lohnt sich De-Mail nur für den Versand von besonders wichtigen Nachrichten, deren Authentizität von Bedeutung ist. Dies stellt ein potentielles Sicherheitsrisiko dar, weil es die wenigen versendeten De-Mails und die separaten Server der De-Mail-Anbieter zu lukrativen Angriffszielen macht.

Die Verwendung von De-Mail mit Ende-zu-Ende-Verschlüsselung ist möglich, liegt jedoch in der Verantwortung des Nutzers und setzt die Installation von spezieller Software zur Verschlüsselung voraus. Zur Schlüsselverteilung kann der vom De-Mail-Anbieter bereit gestellte Verzeichnisdienst genutzt werden. Die dort veröffentlichten Schlüssel sind dann durch die Authentisierung des Nutzers bei der Erstellung eines De-Mail-Accounts ebenfalls authentisiert.

ForceTLS

Mit ForceTLS wird ein Dienst angeboten, der für 100 US Dollar pro Jahr das Versenden aller E-Mails über TLS garantiert.[65] Der Dienst überprüft, ob eine TLS-Verbindung vom Sender einer E-Mail bis zum E-Mail-Server des Empfängers aufgebaut werden kann. Die E-Mails werden dazu nicht über den E-Mail-Provider des Nutzers von ForceTLS, sondern über einen speziellen durch ForceTLS bereitgestellten Server geleitet, der die E-Mail empfängt und zum E-Mail-Provider des Empfängers weiterleitet. Die E-Mail wird erst zugestellt, wenn sich auf beiden Teilstrecken eine TLS-verschlüsselte Verbindung herstellen lässt. Gegebenenfalls wählt der Dienst dazu Alternativrouten, die diese Verbindung ermöglichen. Ist eine TLS-Verbindung nicht möglich, wird die E-Mail nicht versandt und eine Meldung an Sender (und wahlweise Empfänger) generiert. Force-TLS ist dann sinnvoll, wenn der E-Mail-Server eines Nutzers keine TLS-Verbindung von Nutzer zu E-Mail-Server erlaubt, oder die E-Mails zum E-Mail-Server des Empfängers nicht über TLS überträgt. Force-TLS kann die verschlüsselte Übertragung auf beiden Transportwegen sicherstellen, ersetzt jedoch keine Ende-zu-Ende-Verschlüsselung: Zum einen liegt eine E-Mail an jeder Zwischenstation (Server von ForceTLS sowie beim E-Mail-Server des Empfängers) unverschlüsselt vor, zum anderen wird die E-Mail unverschlüsselt zwischen E-Mail-Server des Empfängers und Empfänger übertragen, sofern der Empfänger beim Abrufen der E-Mail keine TLS-Verbindung verwendet.

[65] Vgl. http://www.checktls.com/forcetls.html.

Ende-zu-Ende-Verschlüsselung mit S/MIME

Die verschlüsselte Übermittlung einer E-Mail zwischen Absender bzw. Empfänger und Mail-Provider ist von geringem Nutzen, wenn E-Mails zwischen den E-Mail-Providern unverschlüsselt übertragen werden. Um die Kommunikationsinhalte auch dann zu schützen, wenn E-Mail-Service-Provider nur unzureichende Verschlüsselung anbieten können, ist Ende-zu-Ende-Verschlüsselung notwendig. Secure/Multipurpose Internet Mail Extensions (S/MIME) ist ein Standard der E-Mail-Verschlüsselung, der auch vom BSI empfohlen wird.[66] Für die Verschlüsselung des E-Mail-Verkehrs von Privatpersonen können Zertifikate zur S/MIME Verschlüsselung kostenlos bei einem Trustcenter heruntergeladen werden.[67] Für einen privaten Personenkreis können Zertifikate auch selbst mit Hilfe der Linux-Freeware XCA produziert werden.

Alternativ können Zertifikate auch bei Sparkassen für 10-20 Euro pro Jahr bestellt werden.[68] Die Zertifikate können entweder heruntergeladen oder in Form von Hardware-Tokens (Chipkarten mit Kartenleser) verwendet werden. Kartenleser sind ebenfalls bei der Sparkasse für 50-100 Euro zu erwerben.

S/MIME lässt sich unter Microsoft Outlook, Mozilla Thunderbird und Apple Mail verwenden. Die Verschlüsselung ist neben der Verwendung auf PCs auch auf Smartphones (iOS, Android) möglich. Für GMail existiert ein Firefox-Plugin für den Webmail-Dienst.

Um E-Mail-Kommunikation verschlüsselt durchführen zu können, müssen beide Teilnehmer ein S/MIME-Zertifikat besitzen. Die öffentlichen Schlüssel können an eine signierte (und ggf. verschlüsselte) Mail angehängt werden, so dass kein zusätzlicher Aufwand zum Schlüsseltausch notwendig ist. Allerdings werden die erhaltenen öffentlichen Schlüssel pro Endgerät gespeichert. Der Benutzer muss also die Schlüsselverteilung für alle Geräte selbst verwalten.

Bisher sind keine Sicherheitslücken der Verschlüsselungsfunktion in S/MIME bekannt, die Verschlüsselung kann daher als sicher gelten. Im Zuge des NSA-Skandals ist das hierarchische Vertrauensmodell jedoch als potentielle Schwachstelle gewertet worden, weil von politischer Seite Einfluss auf Zertifizierungsbehörden oder die kommerziellen Implementierungen von S/MIME genommen werden kann.

Ende-zu-Ende-Verschlüsselung mit PGP

Pretty Good Privacy (PGP)[69] wird einerseits kommerziell vertrieben, ist als OpenPGP aber auch öffentlich zugänglich und verwendbar. PGP ist für Mozilla Thunderbird, Microsoft Outlook, AppleMail sowie für Android und iPhone verwendbar. Mit Gpg4win[70] steht ein einfaches Verschlüsselungs-Paket für Mail- und Daten-Verschlüsselung für Windows be-

[66] Siehe für die Spezifizierung Ramsdell 1999.
[67] Z. B. unter www.startssl.com, www.instantssl.com oder www.comodo.com.
[68] Siehe www.s-trust.de.
[69] Siehe für die Spezifizierung Callas et.al. 1998.
[70] Siehe http://www.gpg4win.de.

reit. Es wird sowohl PGP als auch S/MIME unterstützt. Auch unerfahrene Benutzer können mit einem einzigen Installer verschiedene Module (für Dateiverschlüsselung, Mailverschlüsselung, Zertifikatsmanager, entsprechende Plugins für Thunderbird und Outlook) installieren. Eine gute Dokumentation erleichtert den Einstieg. Als kryptographisches Modul liegt die GnuPG Distribution für Windows zu Grunde, deren Sicherheitsparameter sich nach den Empfehlungen des BSI richten.[71]

Mailvelope[72] ist ein Browser-Addon, mit dem PGP-verschlüsselte E-Mails direkt über das Web-Interface beliebiger Webmail-Dienste verschickt werden können. Das Addon ist für Firefox und Chrome verfügbar, und ist für den Einsatz mit GMail, Yahoo Mail, outlook.com und GMX bereits vorkonfiguriert.

PGP unterstützt eine Vielzahl von sicheren kryptographischen Verfahren und Algorithmen. Die tatsächliche Sicherheit hängt jedoch von der verwendeten Implementierung und Software sowie von der Sicherheit des Systems ab, auf dem PGP zum Einsatz kommt. So können Geheimdienste etwa durch Analyse-Software den Speicher von Computern analysieren und PGP-Passwörter auslesen und damit die Verschlüsselung unterwandern.[73]

2.2.4. E-Mail-Anbieter mit Verschlüsselung

Im Folgenden werden E-Mail-Anbieter vorgestellt, die neben der klassischen Funktion eines E-Mail-Providers auch eine Form der Verschlüsselung anbieten. Es handelt sich dabei entweder um Ende-zu-Ende-Verschlüsselung, konsequente Transportverschlüsselung oder eine Mischform aus beidem.

CryptoHeaven

CryptoHeaven[74] ist ein Server-basierter Dienst für Privatpersonen und Unternehmen, der E-Mail-Konten und Web-Speicher bereitstellt. Zur Nutzung muss sich der Nutzer eine Open-Source Client-Software herunterladen, mit der sich die Registrierung sowie die weitere Nutzung des Dienstes durchführen lässt. Bei der Registrierung wird aus einem Nutzerpasswort ein geheimer und ein öffentlicher Schlüssel berechnet, der für die Ende-zu-Ende-Verschlüsselung von E-Mails verwendet wird. Der öffentliche Schlüssel wird automatisch in einem Verzeichnis für andere Nutzer von Cryptoheaven bereitgestellt, während der geheime Schlüssel im Client gespeichert wird. Alternativ kann der geheime Schlüssel auch Passwort-geschützt auf einen USB-Stick oder auf den Server von Cryptoheaven exportiert werden. Sind sowohl Absender als auch Empfänger einer E-Mail Nutzer von Cryptoheaven, wird die E-Mail nur innerhalb des Servers zugestellt, ohne durch

---

[71] Siehe hier BSI 2013a; BSI 2014a; vgl. auch die Empfehlung des BSI unter https://www.bsi-fuer-buerger.de/BSIFB/DE/SicherheitImNetz/Verschluesseltkommunizieren/Einsatzbereiche/einsatzbereiche_node.html.

[72] Mailvelope, https://www.mailvelope.com/.

[73] Vgl. hierzu die Aussage der Bundesregierung http://www.golem.de/news/bundesregierung-deutsche-geheimdienste-koennen-pgp-entschluesseln-1205-92031.html und http://www.com-magazin.de/news/sicherheit/tool-entschluesselt-truecrypt-bitlocker-und-pgp-65810.html; http://blog.crack-password.com/2012/12/elcomsoft-decrypts-bitlocker-pgp-and-truecrypt-containers.

[74] Siehe www.cryptoheaven.com.

das Internet geroutet zu werden. Alle Daten des Nutzers liegen auf dem Server nur verschlüsselt mit dem geheimen Nutzerschlüssel vor. Da die Client-Software Open-Source ist, kann sie auf korrekte Funktionalität überprüft werden.

Der Dienst kostet (je nach Web-Speicher) zwischen 8 und 40 US Dollar monatlich und bietet sich vor allem dann an, wenn E-Mails mit Ende-zu-Ende-Verschlüsselung unter verschiedenen Nutzern von Cryptoheaven ausgetauscht werden sollen. Die Verschlüsselung erfolgt dann automatisch, und die Schlüsselverwaltung wird weitestgehend durch Cryptoheaven übernommen. Damit wird Verschlüsselung besonders sicher und nutzerfreundlich. Nachteilig wirkt sich jedoch aus, dass die von Cryptoheaven verwendete Verschlüsselung nicht mit PGP oder S/MIME kompatibel ist. Eine Ende-zu-Ende-verschlüsselte Kommunikation mit Nutzern anderer Providern ist damit nicht möglich.

Hushmail

Hushmail[75] ist ein kanadischer E-Mail-Anbieter, der die verschlüsselte Übertragung von E-Mails erlaubt. Dabei wird keine Client-Software installiert. Die E-Mails werden im Browser abgeschickt und empfangen und SSL-verschlüsselt zu den Servern von Hushmail übertragen, wo sie mit einem Passwort des Nutzers verschlüsselt werden. Die Schlüsselverwaltung und Verschlüsselung wird damit von Hushmail übernommen. Da die Kommunikationsinhalte jedoch nicht Nutzer-seitig verschlüsselt werden, hat Hushmail auch die Möglichkeit, Nachrichten im Klartext zu speichern, bevor sie verschlüsselt werden. Es handelt sich bei der verwendeten Verschlüsselung damit nicht um echte Ende-zu-Ende-Verschlüsselung. Der Nutzer muss darauf vertrauen, dass die Verschlüsselung ordnungsgemäß vorgenommen wird. Ferner werden E-Mails von Hushmail gescannt, und können bis zu 18 Monate gespeichert werden.[76] Hushmail behält sich außerdem vor, das Passwort des Nutzers im Klartext zu speichern und an kanadische Ermittlungsbehörden zu übergeben.

Safe-Mail

Safe-Mail[77] ist ein israelischer E-Mail-Anbieter, der eine eigene PKI unter Verwendung von S/MIME für seine Nutzer bereitstellt. Nutzer bekommen auf diese Weise ein Schlüsselpaar und ein entsprechendes Zertifikat für Verschlüsselung mit S/MIME. Der geheime Schlüssel und das Zertifikat werden verschlüsselt mit einem Nutzerpasswort auf den Servern von Safe-Mail gespeichert. Die E-Mails liegen ebenfalls verschlüsselt mit dem Nutzerpasswort auf dem Server. Der Zugang zum Account erfolgt entweder über eine Web-Schnittstelle oder über einen beliebigen E-Mail-Client. Da Safe-Mail keinen eigenen Client zur Verfügung stellt, muss der Nutzer darauf vertrauen, dass das Nutzerpasswort von Safe-Mail nicht ausgelesen wird. Ferner müssen Nutzer bezüglich ihrer Zertifikate auf Safe-Mail als PKI vertrauen. Da auch der geheime Schlüssel nicht unter der Kontrolle des Nutzers liegt und E-Mails serverseitig und nicht auf dem Gerät des Nutzers ver- und entschlüsselt werden, handelt es sich trotz der Verwendung von S/MIME bei der von Safe-

[75] Siehe https://www.hushmail.com.
[76] Siehe https://anonymous-proxy-servers.net/blog/index.php?/archives/362-JonDos-empfiehlt-Hushmail.com-nicht.html.
[77] Siehe www.safe-mail.net.

Mail verwendeten Umsetzung nicht um echte Ende-zu-Ende-Verschlüsselung. Die öffentlichen Schlüssel werden ebenfalls auf dem Safe-Mail-Server gespeichert und können dort von jedem anderen Kommunikationspartner unter Angabe der gewünschten E-Mail-Adresse heruntergeladen werden. Die Schlüsselspeicherung wird damit von Safe-Mail übernommen, doch der Schlüsselaustausch muss vom Nutzer selbst initiiert werden. Dabei wird auch jeder öffentliche Schlüssel von Kommunikationspartnern, die nicht bei Safe-Mail registriert sind, auf dem Schlüsselserver von Safe-Mail gespeichert und allen Safe-Mail-Nutzern zur Verfügung gestellt. Der Austausch von E-Mails durch Nutzer untereinander wird nicht automatisch verschlüsselt, sondern nur SSL-verschlüsselt übermittelt. Mit Safebox gibt es eine Möglichkeit, verschlüsselte Nachrichten mit Kommunikationspartnern auszutauschen, die kein S/MIME verwenden. Dabei wird dem Empfänger in einer E-Mail ein Link zugesandt, über den er die eigentliche Nachricht über eine Webseite von Safe-Mail unter Eingabe eines Passwortes abrufen kann. Das Passwort wird entweder vom Absender selbst gewählt und dem Empfänger auf sicherem Weg mitgeteilt, oder von Safe-Mail auf zufällige Weise erzeugt und zusammen mit dem Link zur Safebox im Klartext übermittelt. In beiden Fällen ist Safe-Mail das Passwort bekannt, im letzteren Fall kann das Passwort sogar von jedem gelesen werden, der die E-Mail mit dem Link zur Safebox lesen kann. Da Safe-Mail keinen Client verwendet, können Nutzerpasswörter ausgelesen und damit auch E-Mail-Nachrichten an Ermittlungsbehörden übermittelt werden. Safe-Mail gesteht zu, bereits Ersuche ausländischer Behörden über den israelischen Gerichtshof erhalten zu haben.[78]

Posteo

Posteo[79] ist ein deutscher E-Mail-Anbieter, der auf Datensparsamkeit setzt. Der Zugriff auf die E-Mail-Server kann nur verschlüsselt über TLS mit Perfect Forward Secrecy erfolgen (sowohl über einen Mailclient als auch über den Web-Mailer). Posteo informiert die Nutzer zudem darüber, zu welchen E-Mail-Anbietern durchgehend Transportverschlüsselung verwendet wird. Dies ist neben größeren Anbietern wie Gmail, Web.de, GMX und T-Online auch für Anbieter mit kleinerem Marktanteil in Deutschland wie Vodafone, Yahoo, Freenet, AOL und Arcor der Fall. Mit diesen E-Mail-Anbietern werden die Kommunikationsinhalte damit auf die gleiche Weise gesichert wie bei *E-Mail made in Germany*. Posteo bietet ferner eine Möglichkeit an, das gesamte Postfach mit einem vom Nutzer eingegebenen Passwort zu verschlüsseln, um die auf dem Server gespeicherten E-Mails zusätzlich zu schützen. Der Nutzer muss jedoch darauf vertrauen, dass sein Passwort nicht von Posteo ausgelesen oder im Klartext gespeichert wird.

Startmail

Startmail[80] ist ein niederländischer E-Mail-Anbieter, der mit einer nutzerfreundlichen Möglichkeit der Verschlüsselung wirbt. Dabei kommt ein Web-Mailer zum Einsatz, über den sich E-Mails verschlüsselt versenden lassen. Die Schlüsselverwaltung wird von Start-

[78] Siehe http://bgr.com/2014/02/03/nsa-proof-email-safe-mail.
[79] Siehe www.posteo.de.
[80] Siehe www.startmail.com.

mail übernommen und ist damit sehr benutzerfreundlich. Dabei wird jedoch der öffentliche wie auch der private Schlüssel auf den Servern von Startmail gespeichert, was ein potentielles Sicherheitsrisiko für die Kommunikationsinhalte darstellt. Ferner findet die Ver- und Entschlüsselung auf dem Server statt, was Startmail den Zugriff auf die Nachrichten im Klartext ermöglicht. Es handelt sich damit bei der von Startmail verwendeten Verschlüsselung nicht um echte Ende-zu-Ende-Verschlüsselung. Kommunizieren zwei Nutzer von Startmail über den Web-Mailer miteinander, wird die Verschlüsselung mit PGP automatisch im Hintergrund vorgenommen. Verschlüsselte Kommunikation mit PGP mit Nutzern anderer E-Mail-Anbieter ist nur möglich, sofern der Schlüsselaustausch vom Nutzer selbst übernommen wird. Der Dienst bietet auch eine Möglichkeit der verschlüsselten Kommunikation, falls der Kommunikationspartner keinen PGP-Schlüssel besitzt: In diesem Fall bekommt er per E-Mail einen Weblink, über den sich, nach korrekter Beantwortung einer Sicherheitsfrage, die verwendete Nachricht lesen und verschlüsselt beantworten lässt. Die Sicherheitsfrage kann vom Absender der Mail so festgelegt werden, dass nur der Empfänger die Antwort kennt. Wird anstelle des Web-Mailers ein E-Mail-Client verwendet, muss der Benutzer die Verwaltung der Schlüssel selbst übernehmen. Der Gewinn an Nutzbarkeit wird bei Startmail damit bezahlt, dass der Nutzer dem Dienst in Bezug auf die korrekte Durchführung der Verschlüsselung und sorgsame Verwaltung der geheimen Schlüssel vertrauen muss.

ProtonMail

ProtonMail[81] ist ein E-Mail-Anbieter mit Sitz in der Schweiz, der im Zuge des NSA-Skandals entstanden ist, mit dem Ziel, die Privatsphäre von Nutzern bei der E-Mail-Kommunikation zu sichern. Der Anbieter orientiert sich an den Sicherheitszielen des ehemaligen amerikanischen E-Mail-Providers Lavabit, der im Zuge des NSA-Skandals seinen Betrieb einstellte. ProtonMail versucht einige Schwächen von Lavabit, die zur Schließung führten, zu vermeiden. Zu den Sicherheitszielen von ProtonMail gehört in erster Linie der Schutz gegen Massenüberwachung. Der Zugang zu den E-Mails erfolgt über einen Webclient unter Verwendung von SSL-Verschlüsselung. Zusätzlich werden alle E-Mails verschlüsselt zwischen Browser und Server übertragen. Das Passwort zu dieser Verschlüsselung kennt nur der Nutzer (Details zur Verschlüsselung sind nicht bekannt). Alle E-Mails liegen damit nur verschlüsselt auf den Servern und können selbst von ProtonMail nicht eingesehen werden. Im Gegensatz zu anderen E-Mail-Anbietern versucht ProtonMail den Nutzer durch zwei Maßnahmen davor zu schützen, dass er von ProtonMail einen manipulierten Browser-Code bekommt, durch den ProtonMail das Passwort des Nutzers auslesen und somit alle auf den Servern liegenden E-Mails entschlüsseln kann (wie im Fall von Lavabit geschehen): Zum einen wird der Code nicht in gepackter Form an den Browser des Nutzers geliefert, so dass der Nutzer über eine Funktion seines Browsers den Code direkt überprüfen kann. Der Code soll in Zukunft (zu Teilen) Open-Source werden. Zum anderen soll der Standort in der Schweiz davor schützen, dass Behörden einen E-Mail-Anbieter überhaupt zur Manipulation des Codes zwingen können.

[81] Siehe https://protonmail.ch.

Tutanota

Tutanota[82] ist ein deutscher E-Mail-Anbieter und bietet Ende-zu-Ende-verschlüsselte E-Mail-Kommunikation sowohl für Privat- wie auch für Businessanwender an. Privatanwender können sich kostenlos registrieren und über einen Webclient auf das Tutanota-E-Mail-Postfach zugreifen. Bei der Registrierung wird ein asymmetrisches Schlüsselpaar automatisch erzeugt. Der private Schlüssel des Nutzers wird durch ein Passwort des Nutzers gesichert auf den Servern von Tutanota gespeichert. Es handelt sich damit nicht um echte Ende-zu-Ende-Verschlüsselung. Der Nutzer muss daher darauf vertrauen, dass Tutanota nicht durch eine Hintertür an das Nutzerpasswort kommt und damit an den geheimen Schlüssel.

Die Schlüsselverwaltung wird vollständig von Tutanota übernommen. Mails zwischen Nutzern von Tutanota werden ferner automatisch ver- und entschlüsselt. Verschlüsselte Kommunikation mit Kommunikationspartnern außerhalb von Tutanota ist über ein Webformular möglich, zu dem ein Link mit zugehörigem Passwort mitgeteilt werden kann. E-Mails unter Nutzern von Tutanota (Privat- oder Businessanwender) werden automatisch verschlüsselt übertragen. Ein kostenpflichtiger Dienst ermöglicht für 14,99 Euro monatlich die Nutzung eines Outlook-Addins und die Nutzung der eigenen E-Mail-Adresse (nicht notwendigerweise von Tutanota). Die Funktionsweise der von Tutanota verwendeten Verschlüsselung ist in ihren Details nicht bekannt und nicht mit PGP kompatibel. Das ist nicht nur ein wesentlicher praktischer Nachteil bezüglich der Kompatibilität zu anderen Verschlüsselungen, sondern auch ein potentielles Sicherheitsrisiko.

mailbox.org

Mailbox[83] ist ein 2014 anlässlich des NSA-Skandals gegründeter E-Mail-Provider, der großen Wert auf Datensparsamkeit und Privatsphäre setzt. Dieser hat seinen Sitz in Berlin und wird betrieben von der Heinlein Support GmbH, die bereits seit 1989 den E-Mail-Provider Mailbox JPBerlin betreibt. Die E-Mail-Server sind Teil der eigenen Infrastruktur des Anbieters und mit biometrischer Zugangskontrolle und Wachdienst geschützt. Daneben liegen die E-Mails auf verschlüsselten Servern und lassen sich auf Wunsch des Nutzers mit dessen eigenem PGP-Schlüssel zusätzlich verschlüsseln. Dies gilt ebenso für unverschlüsselte E-Mails, die im Posteingang ankommen. Der geheime Schlüssel selbst wird dabei nicht auf den Servern gespeichert, sondern muss vom Nutzer auf dem eigenen Computer gespeichert werden.[84] Dies führt dazu, dass die E-Mails nicht von einem Web-Mailer aus entschlüsselt werden können, schützt andererseits aber auch den Nutzer davor, dass der E-Mail-Anbieter den geheimen Schlüssel des Nutzers ausliest und so Zugang zu den verschlüsselten E-Mails erhält. Senden und Empfangen von E-Mails erfolgt ausschließlich durch TLS-Verschlüsselung mit Perfect Forward Secrecy. Der Anbieter verfügt über eine Funktion, durch die der Nutzer vor dem Versenden einer E-Mail darüber informiert wird,

[82] Siehe https://tutanota.de.
[83] Siehe www.posteo.de.
[84] Alternativ kann der geheime Schlüssel auch passwortgeschützt auf die Server von Mailbox hochgeladen werden, was jedoch einen geringeren Schutz bietet.

ob ein durchgängig transportverschlüsselter Versandt mit dem E-Mail-Provider des Empfängers möglich ist. Ähnlich hat der Nutzer neben seiner normalen E-Mail-Adresse zusätzlich noch eine spezielle E-Mail-Adresse, über die E-Mails nur versandt und zugestellt werden, sofern eine durchgehende Transportverschlüsselung zum Server des anderen Mail-Providers möglich ist.

Countermail

Countermail[85] ist ein schwedischer E-Mail-Anbieter, der ein E-Mail-Postfach und einen Web-Mailer mit PGP-Funktionalität bereitstellt. Für das Erstellen und Importieren der Schlüssel ist der Nutzer selbst verantwortlich. Die E-Mails im Postfach sowie Kalender und Kontakte können mit dem öffentlichen PGP-Schlüssel verschlüsselt werden und sind über einen Web-Mailer zugänglich. Ebenso können eingehende E-Mails standardmäßig mit dem öffentlichen PGP-Schlüssel verschlüsselt werden. Der private PGP-Schlüssel kann entweder geschützt durch ein Passwort auf dem Server von Countermail oder auf dem eigenen Rechner gespeichert werden. Insbesondere dann, wenn ein Web-Mailer verwendet wird, muss der Nutzer darauf vertrauen, dass Countermail den geheimen Schlüssel nicht im Klartext ausliest. Der Nutzer kann dies nicht überprüfen, weil das zur Entschlüsselung verwendete Java-Applet nicht Open-Source ist. Wird der geheime Schlüssel auf dem Rechner des Nutzers gespeichert, muss der Nutzer darauf vertrauen, dass der geheime Schlüssel vom Server gelöscht wird. Die PGP-Schlüssel von Kontakten, die nicht bei Countermail registriert sind, müssen einzeln in das Schlüsselregister von Countermail eingetragen werden.

Scramble

Scramble[86] ist ein nicht kommerzieller E-Mail-Anbieter, der verschlüsselte und anonyme E-Mail anbietet. Das Projekt befindet sich noch in der Entwicklung. Bei der Anmeldung wird ein asymmetrisches Schlüsselpaar erzeugt und die E-Mail-Adresse als Hashwert aus dem öffentlichen Schlüssel generiert. Auf diese Weise kann von keiner E-Mail-Adresse auf den Namen des Inhabers geschlossen werden. Die Nutzer müssen daher ein Adressbuch führen, durch das sie den kryptischen E-Mail-Adressen Namen zuordnen können und umgekehrt. Durch die Verbindung von E-Mail-Adresse mit öffentlichem Schlüssel ist zugleich gesichert, dass beide wirklich zueinander gehören. Der Zugang zu den E-Mails wird durch eine Web-Mailer realisiert, der sowohl E-Mails, als auch das Adressbuch verschlüsselt. Da kein Vertrauen in den E-Mail-Server vorausgesetzt wird, ist eine Browser-Erweiterung geplant, durch die das Krypto-Applet dauerhaft auf dem Computer des Nutzers gespeichert werden kann. Auf diese Weise wird verhindert, dass der geheime Schlüssel des Nutzers durch manipulierten Code vom Server extrahiert werden kann. Diese Lösung stellt einen bisher einzigartigen Kompromiss zwischen der Funktionalität von Webclients und der Sicherheit von dedizierter Client-Software dar. Nutzer von Scramble können anonym und verschlüsselt untereinander kommunizieren. Findet darüber hinaus Kommunikation zu Nutzern anderer E-Mail-Provider statt, so werden ausgehende und eingehende E-Mails

[85] Siehe https://countermail.com/?p=privacy.
[86] Siehe http://dcposch.github.io/scramble/; siehe auch https://scramble.io/doc und https://scramble.io/doc/faq.html.

stets mit dem öffentlichen Schlüssel des Nutzers auf den Servern von Scramble verschlüsselt. Die Verschlüsselung umfasst sowohl den Textkörper als auch den Betreff der Nachricht. Da den Servern nicht vertraut werden muss und E-Mails nur verschlüsselt dort abgelegt werden, kann jeder freiwillig einen eigenen Scramble-Server betreiben. Es ist geplant, die Anzahl der Server auf diese Weise von den USA als erstem Standort eines Scramble-Servers auf unterschiedliche Länder zu erweitern und so die Anzahl der Server auszubauen. Das stellt jedoch zugleich ein potentielles Sicherheitsrisiko dar, weil damit jeder einen Mirror- oder Backupserver betreiben und auf diese Weise alle E-Mails eines ganzen Landes speichern kann. Die verschlüsselten E-Mails können möglicherweise zu einem späteren Zeitpunkt mit fortschrittlichen Entschlüsselungsmethoden entschlüsselt werden. Ein weiterer praktischer Nachteil ist zudem, dass durch die Verteilung der Server nur ein kleiner Speicherplatz für jedes Postfach bereit steht und daher auf E-Mail-Anhänge verzichtet wird.

Weitere E-Mail-Anbieter

Neben den oben genannten E-Mail-Anbietern gibt es noch weitere, die ähnliche aber weniger weitgehende Sicherheitsfunktionen bieten. Dazu gehören:

- Neomailbox[87] ist ein schweizer Anbieter mit Unterstützung für PGP. Weitere Sicherheitsfeatures sind geplant.
- RiseUP[88] stellt ein Webmail-Programm für PGP-Verschlüsselung bereit. Der private Schlüssel liegt dabei jedoch (passwortgeschützt) auf dem Server.
- Unseen[89] ist ein isländischer E-Mail-Anbieter mit PGP-Verschlüsselung über Roundcube. Der Dienst ist noch in Entwicklung befindlich, so dass nur wenige Details zur Verschlüsselung bekannt sind.
- VMail[90] ist ein seit 2001 bestehender E-Mail-Anbieter mit Schwerpunkt auf Anti-Virus-Filtern. Die Verwendung von PGP ist über einen Webmailclient möglich. Ferner bietet der Dienst eine spezielle Funktion zur Minimierung von Kommunikationsmetadaten (Metadata Mitigator).

2.2.5. Software zur Ende-zu-Ende-Verschlüsselung

Neben E-Mail-Anbietern, die bereits eine Möglichkeit der Verschlüsselung anbieten oder unterstützen, gibt es unterschiedliche Softwarelösungen, die unabhängig vom E-Mail-Provider zur Verschlüsselung verwendet werden können.

Leap

LEAP[91] ist ein nicht-kommerzieller Dienst, der den E-Mail Client Bitmask bereitstellt. Der Client ist Open-Source und schaltet sich wie ein Proxy zwischen einen herkömmlichen E-

[87] Siehe https://www.neomailbox.com.
[88] Siehe https://help.riseup.net/de/email.
[89] Siehe https://www.unseen.is/faq.html.
[90] Siehe https://www.vfemail.net.
[91] Vgl. LEAP Encryption Project, www.leap.se.

Mail Client (z. B. Outlook, Thunderbird) und den E-Mail-Server des E-Mail-Anbieters. Bitmask ermöglicht den Nutzern damit, ihren gewohnten E-Mail-Client zu verwenden und gleichzeitig die zusätzlichen Funktionen für sichere E-Mail Kommunikation zu nutzen. Diese bestehen in der automatischen Verschlüsselung ankommender E-Mails mit PGP, so dass diese verschlüsselt auf dem eigenen Computer abgelegt werden können. Ausgehende E-Mails werden automatisch verschlüsselt, sofern der Empfänger über einen PGP-Schlüssel verfügt. Die Schlüssel von Kontakten sollen automatisch aus dem Internet heruntergeladen werden. Die Funktionalität ist noch beschränkt und hinsichtlich der Details noch unklar, da sich die Software noch im Entwicklungsstatus befindet.

Mailpile

Mailpile[92] ist ein kostenloser Open-Source E-Mail-Client, der sich noch in der Entwicklung befindet. Das Programm wird über den Browser bedient und bietet neben der Funktionalität anderer E-Mail-Clients besonders einfache Möglichkeiten der Ende-zu-Ende-Verschlüsselung. PGP-Schlüssel können über den Client erzeugt werden, und der öffentliche Schlüssel des Nutzers wird standardmäßig in jeder E-Mail verschickt. Ferner kann eingestellt werden, dass sich der Client für alle Empfänger im Hintergrund die zugehörigen Schlüssel aus dem eigenen Schlüsselverzeichnis oder öffentlich zugänglichen Schlüsselservern besorgt und ausgehende E-Mails automatisch verschlüsselt. Für Nutzer von Mailpile ist damit der verschlüsselte Versand von E-Mails besonders einfach. Da Mailpile ein E-Mail-Client ist, ist er mit jedem E-Mail-Provider kombinierbar.

Whiteout

Whiteout[93] bietet einen Open-Source E-Mail-Client in Form einer App für Chrome OS, Android und iOS an (Clients für Windows und Firefox OS sind in Planung). Ferner wird ein Browser-Plugin für Mozilla Firefox zur Verfügung gestellt. Der Client erzeugt lokal ein PGP-Schlüsselpaar, dessen privater Schlüssel auch nur lokal gespeichert wird. Der öffentliche Schlüssel wird automatisch auf einen Schlüsselserver hochgeladen. Beim Verfassen von E-Mails wird für die Empfänger ebenfalls automatisch geprüft, ob ein öffentlicher Schlüssel auf Schlüsselservern vorhanden ist. Sofern kein öffentlicher Schlüssel für die Empfänger vorhanden ist, wird deren Adresse im Client rot hinterlegt. Der Client zeichnet sich damit durch seine Benutzerfreundlichkeit aus, ist durch die fehlende Unterstützung von Windows und Linux jedoch noch von begrenztem Nutzen.

Virtru

Virtru[94] ist ein in der Entwicklung befindliches Konzept zur verschlüsselten Übertragung von E-Mails mit Ende-zu-Ende-Verschlüsselung. Das patentierte Konzept wird von einem amerikanischen Unternehmen (Virtru Corporation) mit Sitz in Washington entwickelt und unterscheidet sich stark von PGP oder S/MIME. Das Konzept setzt einen Virtru-Schlüsselserver und, auf Nutzerseite, Addins für Browser oder Mailclient voraus. E-Mails werden mit Hilfe der Addins im Browser oder im Mailclient verschlüsselt. Dabei wird im Gegensatz zu PGP und S/MIME keine asymmetrische Verschlüsselung verwendet, die E-

[92] Siehe www.mailpile.is.
[93] Siehe https://whiteout.io.
[94] Siehe https://www.virtru.com.

Mails werden vielmehr symmetrisch unter Verwendung von AES verschlüsselt. Jede Nachricht wird mit einem anderen symmetrischen Schlüssel verschlüsselt. Diese werden auf dem Virtru-Schlüsselserver gespeichert. Das Versenden einer verschlüsselten E-Mail kann von einer beliebigen E-Mail-Adresse erfolgen und setzt nur ein Browser- oder Mailclient-Addin voraus. Der Empfänger erhält eine E-Mail mit dem Hinweis, dass eine mit Virtru verschlüsselte Nachricht eingegangen ist. Die Nachricht kann dann entweder durch Installation des entsprechenden Addins oder über einen Virtru-Webreader im Browser gelesen werden. Dabei wird vom Browser oder Addin direkt auf den Virtru-Schlüsselserver zugegriffen und die Nachricht mit dem dort gespeicherten symmetrischen Schlüssel entschlüsselt. Der Vorteil des Konzeptes liegt in seiner intuitiven Bedienbarkeit und Nutzerfreundlichkeit. Die Konzeption erlaubt ferner das Hinzufügen eines Ablaufdatums oder das Widerrufen von Leseberechtigungen. Die Sicherheit beruht darauf, dass ein Angreifer entweder die verschlüsselte Nachricht oder (bei Angriff auf den Schlüsselserver) einen zu einer Nachricht korrespondierenden Schlüssel hat, nicht aber beides. Der Zugang zu einem geheimen Schlüssel erlaubt einem Angreifer selbst mit Zugang zu allen Nachrichten nur das Entschlüsseln einer einzigen bereits gesendeten Nachricht, nicht aber den Einblick in andere oder zukünftige Nachrichten. Schutz vor Geheimdiensten oder Behörden, die sich über Gerichtsbeschlüssen dauerhaften Zugang zum Schlüsselserver und auch den Mailservern einzelner Nutzer verschaffen können, bietet das Konzept dennoch nicht. Für die Zukunft ist eine Funktion geplant, die es den Nutzern erlaubt, die Schlüssel lokal zu speichern und nicht auf den Schlüsselserver zu übertragen. Ebenso ist geplant, den Code der Addins als Open-Source zur Verfügung zu stellen, um das Risiko von manipuliertem Code zu minimieren. Das Konzept ist aufgrund fehlender Details zur Funktionsweise derzeit schwer zu beurteilen. Ebenso schwer zu beurteilen ist der Umstand, dass die meisten Mitarbeit von Virtru NSA-Hintergrund haben - was entweder als Vorteil oder Nachteil gewertet werden kann.

Weitere Software

Neben den oben genannten Programmen gibt es weitere Software-Lösungen, die eine Verschlüsselung der E-Mail-Kommunikation ermöglicht:

- Roundcube[95] ist ein Webmail-Client, für den PGP-Unterstützung geplant und bereits prototypisch implementiert ist.[96]
- Mit dem Browser-Plugin Mailvelope[97] lässt sich PGP-Verschlüsselung im Web-Browser integrieren.
- Enigmail[98] und ist dagegen ein Plugin für E-Mail-Clients (Thunderbird, Seamonkey und Postbox), das PGP-Verschlüsselung ermöglicht. Das Plugin weist viele Konfigurationsmöglichkeiten auf, erfordert jedoch ein grundlegendes Verständnis der Funktionsweise von PGP.

[95] Siehe http://roundcube.net.
[96] Siehe http://trac.roundcube.net/wiki/PluginRepository/Encryption.
[97] Siehe https://www.mailvelope.com.
[98] Siehe https://www.enigmail.net.

- PGP4Win[99] ist ein Softwarepaket, das Möglichkeiten zur Schlüsselerzeugung und Verschlüsselung mit PGP und S/MIME in Microsoft Outlook ermöglicht, jedoch ebenfalls Grundkenntnisse in Funktionsweise und Schlüsselverwaltung der Verfahren voraussetzt.

2.2.6. Alternativen zu E-Mail

Die verschlüsselte E-Mail-Kommunikation lässt sich nicht nur durch Wahl des Providers oder eines geeigneten Clients erreichen, sondern kann auch durch die Wahl eines anderen Kommunikationsverfahrens anstelle der E-Mail ersetzt werden. Solche Verfahren versuchen den Schwächen der herkömmlichen E-Mail durch Entwicklung neuer Protokolle und Kommunikationsformen zu begegnen.

E-Postbrief

Der E-Postbrief ist eine von der Deutschen Post angebotene Möglichkeit, elektronische Nachrichten mit einem besseren Schutz als die der herkömmlichen E-Mail über das Internet zu verschicken. Dazu können sich Nutzer für den Dienst registrieren und erhalten so einen elektronischen Briefkasten, auf den über eine SSL-verschlüsselte Verbindung zugegriffen werden kann. Auf diese Weise können Sender und Empfänger über einen zentralen Server kommunizieren. Die Kommunikationsinhalte werden auf den Teilstrecken zum zentralen Post-Server SSL-verschlüsselt übertragen, liegen auf dem Server jedoch im Klartext vor. Das Verfahren sieht vor, dass neben dem Sender auch der Empfänger einen elektronischen Briefkasten hat - andernfalls wird die elektronische Nachricht von der Post ausgedruckt und dem Empfänger per Brief übermittelt.

Darkmail

Nach der Schließung der Dienste von Lavabit im Zusammenhang mit der NSA-Affäre ist für 2014 eine Neukonzeption des E-Mail-Konzeptes in Form der "Lavabit's Dark Mail Initiative"[100] geplant. Gegenüber der herkömmlichen E-Mail soll dabei nicht nur eine Ende-zu-Ende-Verschlüsselung erreicht werden, sondern auch die Kommunikationsmetadaten verschlüsselt werden.[101] Das Konzept befindet sich jedoch noch in der Entwicklung und ist noch nicht in allen Details bekannt.

Bitmessage

Bitmessage ist ein 2012 entwickeltes Kommunikationsprotokoll, bei dem Nachrichten verschlüsselt in einem Peer-to-Peer-Netzwerk übertragen werden.[102] Dabei wird ein dezentrales Netzwerk aus allen Teilnehmern des Protokolls gebildet, über das Nachrichten verschickt werden. Jeder Teilnehmer verfügt über ein asymmetrisches Schlüsselpaar und eine Bitmessage-Adresse, die aus dem Hashwert des öffentlichen Schlüssels gebildet wird. Jeder Teilnehmer wird einer Gruppe des Netzwerkes, die als "Stream" bezeichnet wird,

[99] Siehe http://www.gpg4win.de.
[100] Siehe https://darkmail.info/.
[101] Die Dark Mail Spezifikation ist verfügbar unter https://darkmail.info/.
[102] Warren 2012; Warren 2013.

zugeordnet. Aus der Bitmessage-Adresse lässt sich auf einfache Weise der Stream berechnen, zu dem der Inhaber gehört. Eine Nachricht an ein Mitglied eines Streams wird mit dessen öffentlichem Schlüssel verschlüsselt, aber gleichzeitig an alle Mitglieder des Streams gesandt. Sie kann jedoch nur vom Empfänger entschlüsselt und gelesen werden, während sie für die anderen Mitglieder des Streams unlesbar bleibt und keinerlei Relevanz besitzt. Eine kostenlose Client-Software[103] ermöglicht den Einstieg in das Netzwerk. Dazu wird ein Schlüsselpaar berechnet, eine oder mehrere zugehörige Bitmessage-Adressen erzeugt und jede Adresse einem Stream zugeordnet. Über den Client können Nachrichten verschickt und empfangen werden. Da jede Nachricht gleichzeitig an alle Teilnehmer des Streams gesendet wird, prüft der Client automatisch, welche Nachrichten für ihn bestimmt sind. Nur diese Nachrichten werden im Client als eingegangene Nachrichten angezeigt.

Bei Kommunikation über Bitmessage werden nicht nur die Kommunikationsinhalte über die standardmäßige Verschlüsselung der Nachrichten geschützt, sondern im Gegensatz zur E-Mail auch Adressat- und Absenderinformationen verborgen. Um das Netzwerk vor Spam zu schützen, muss vom versendenden Gerät für jede Nachricht ein Nachweis erbracht werden, der in der Berechnung von Informationen besteht, für die ein Zeitaufwand von durchschnittlich 4 Minuten entsteht. Dies kann als praktischer Nachteil angesehen werden, weil es die schnelle Kommunikation zwischen Teilnehmern erschwert. Eine potentielle Schwachstelle von Bitmessage könnte auch darin bestehen, dass jedes Mitglied eines Streams die für andere Mitglieder verschlüsselten Nachrichten erhält, und damit viel leichter an Nachrichten gelangt, als es bei E-Mail-Kommunikation der Fall ist. Geheimdienste könnten auf diese Weise sehr einfach verschlüsselte Nachrichten sammeln und möglicherweise zu einem späteren Zeitpunkt mit fortgeschrittenen Methoden der Entschlüsselung mit deutlich geringerem Aufwand entschlüsseln, als dies mit heutigen Methoden möglich ist.

Neben dem derzeit bereits verfügbaren Client wird ein weiterer Client entwickelt, der Bitmessage besonders einfach einem breiten Publikum zur Verfügung stellen will.[104] Ebenfalls in der Entwicklung befindet sich ein Gateway, über den Bitmessage- und E-Mail-Nachrichten gleichzeitig mit dem gewohnten E-Mail-Client abgerufen und verschickt werden können.[105]

Senditonthenet

Senditonthenet[106] ist ein kostenloser Dienst zum verschlüsselten Versenden von Dateien bis zu einer Größe von 80 MB. Das Übermitteln und Empfangen von Dateien funktioniert durch einen Webclient, dessen Javascript-Code so aufbereitet ist, dass er leicht geprüft werden kann. Die zu übermittelnde Datei wird asymmetrisch mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. Als Verschlüsselung wird RSA verwendet. Der

[103] Der Client ist verfügbar für Windows, OS X und Linux unter: https://bitmessage.org/wiki/Main_Page.
[104] Siehe https://bitcoinstarter.com/projects/98.
[105] Siehe https://bitmessage.org/forum/index.php?topic=1587.0.
[106] Siehe https://www.senditonthenet.com.

Empfänger muss registriert sein, um einen öffentlichen Schlüssel zu besitzen. Der Absender kann entweder ebenfalls registriert sein, oder die Datei unter einem Link des Empfängers in einem Webformular hochladen und so verschlüsselt übertragen. Zusätzlich kann zu jeder Datei eine Nachricht übermittelt werden, die jedoch nicht asymmetrisch verschlüsselt wird, sondern bei der nur die Übertragung über SSL geschützt ist.

I2P

I2P steht für *Invisible Internet Project* und ist ein Peer-to-Peer-Netzwerk zur anonymen und verschlüsselten Kommunikation. Dieses kann auf unterschiedliche Arten zur Nachrichtenübermittlung verwendet werden: Durch Installation des Plugins I2P[107] wird durch eine entsprechende Routerkonfiguration die Verbindung zum I2P-Netzwerk hergestellt. Über das Webinterface des Routers kann dann eine I2P-Bote-Adresse erstellt werden. Nachrichten werden ebenfalls über das Webinterface versendet und empfangen. Dabei kommt eine Mehrfachverschlüsselung zur Anwendung, wie sie sich in ähnlicher Form beim Tor-Netzwerk findet. Die I2P-Bote-Adresse ist zugleich der öffentliche Schlüssel, so dass standardmäßig Ende-zu-Ende verschlüsselt werden kann. Die Mailheader werden auf das Notwendigste beschränkt und erhalten nur den Empfänger, sowie wahlweise auch den Absender. Die versendeten Nachrichten sind durch die dezentrale Struktur des Netzwerks nur schwer zu beobachten und sicher gegen Massenüberwachung, Geheimdienste oder behördliche Beobachtung. Die fehlende Kompatibilität mit der herkömmlichen E-Mail sowie die notwendige Konfiguration des Routers sind praktische Hindernisse, die die meisten Nutzer von einer Verwendung des I2P-Dienstes abhalten. Alternativ zum I2P-Bote existiert mit Susimail ein Browser-Applet, um über den E-Mail-Dienst postman[108] ein Postfach zu betreiben, von dem aus E-Mails mit anderen E-Mail-Anbietern ausgetauscht werden können. Diese können wahlweise durch PGP oder S/MIME verschlüsselt werden.

Retroshare

Retroshare[109] ist eine Open-Source Software, durch die zwischen den Nutzern ein dezentrales Netzwerk als Kommunikationsplattform erstellt wird. Die Software ist für alle bekannten Betriebssysteme verfügbar und kann verwendet werden, um Kontakte zu verwalten, Foren zu erstellen und Dateien austauschen. Daneben fungiert sie wie ein E-Mail-Client und ermöglicht so den Austausch von Nachrichten unter den Nutzern. Jeder Nutzer erhält bei der Installation ein asymmetrisches Schlüsselpaar, durch das Nachrichten standardmäßig verschlüsselt werden.

Weitere Alternativen

Neben den oben genannten Lösungen gibt es weitere Alternativen zur E-Mail:

[107] Siehe http://i2pbote.i2p.us.
[108] Siehe hq.postman.i2p.us.
[109] Siehe http://secushare.org.

- Opentrashbox [110] ist ein 24-Stunden Wegwerf-Postfach. Pond[111] ist ein Projekt im Entwicklungsstatus zur sicheren Nachrichtenübermittlung über das Tor-Netzwerk.
- Briar[112] ist eine App für Smartphones, die sichere Kommunikation über ein Peer-to-Peer-Netzwerk ermöglicht.
- SecuShare[113] soll, ähnlich wie Retroshare, sichere Kommunikation über ein soziales Netzwerk als Peer-to-Peer-Netzwerk gewährleisten.
- Martus[114] ist eine Software, mit der Gruppen sicher untereinander kommunizieren können.

Die meisten dieser Lösungen befinden sich allerdings aktuell noch in einem verhältnismäßig frühen Entwicklungsstatus und sind hinsichtlich der von ihnen gebotenen Sicherheit noch nicht ausreichend evaluiert.

2.2.7. Bewertung und Verbreitung bestehender Techniken

Die oben genannten Schutzmechanismen lassen sich in unterschiedliche Grade für den Schutz der Kommunikationsinhalte vor den in Abschnitt 2.2.2 genannten Angriffsmöglichkeiten kategorisieren. Im Folgenden werden dabei drei unterschiedliche Sicherheitsebenen betrachtet, die jeweils ein unterschiedliches Maß an Schutz bieten:

1. **Geringe Sicherheit**

   Ein geringer Grad an Sicherheit wird erreicht, wenn E-Mails durchgehend durch Transportverschlüsselung geschützt werden und die Transportverschlüsselung keine gravierenden Schwachstellen enthält sowie Perfect Forward Secrecy umsetzt. Damit sind die Kommunikationsinhalte durch einen grundlegenden Schutz vor großflächigem Abfangen oder Abhören der Kommunikation bei Sender, Empfänger oder einem der beteiligten Mailserver geschützt. Der Server des eigenen E-Mail-Anbieters weist Schutzmaßnahmen für netzwerkbasierte oder physische Zugriffe von Unbefugten auf. Insbesondere sind die Inhalte auf den Servern verschlüsselt. Keinen Schutz bietet dies vor behördlichen Zugriffen sowie vor Geheimdiensten, die in der Lage sind, SSL-Verschlüsselung zu brechen.

2. **Mittlere Sicherheit**

   Ein weitergehender Schutz wird dadurch erreicht, wenn zusätzlich zur Transportverschlüsselung die E-Mail-Kommunikation Ende-zu-Ende verschlüsselt wird. Alle auf dem Server abgelegten E-Mails werden mit dem eigenen öffentlichen Schlüssel verschlüsselt. Dem Server des eigenen E-Mail-Anbieters wird weitgehend vertraut,

[110] Siehe www.opentrashbox.org.
[111] Siehe https://pond.imperialviolet.org.
[112] Siehe https://briarproject.org.
[113] Siehe http://secushare.org.
[114] Siehe https://www.martus.org.

dennoch wird sein Verhalten überprüft. Private Schlüssel liegen nur Passwort-geschützt auf den Servern des eigenen E-Mail-Anbieters. Schutz wird auch gegenüber Angriffen auf den Server des E-Mail-Anbieters, oder gegenüber Angriffen von Administratoren mit Zugriff auf das eigene Postfach erreicht. Ferner wird Schutz der meisten Kommunikationsinhalte auch dann erreicht, wenn ein Angreifer SSL-Verschlüsselung brechen kann. Kein Schutz wird vor gezielten Angriffen erreicht, bei denen der eigene E-Mail-Anbieter selbst beteiligt ist. Dies umfasst das gezielte Auslesen von Passwörtern durch manipulierten Code an Webclients. Ferner ist ein Teil der Kommunikationsinhalte (unverschlüsselt eingehende und ausgehende E-Mails) auf den Transportstrecken nur durch Transportverschlüsselung geschützt und liegt bei den Kommunikationspartner und deren Servern im schlechtesten Fall im Klartext vor.

3. **Hohe Sicherheit**

   Ein sehr weitgehender Schutz der Kommunikationsinhalte wird erreicht, wenn E-Mails nur Ende-zu-Ende-verschlüsselt gesendet und empfangen werden. Dabei liegt der private Schlüssel ausschließlich Passwort-geschützt auf den eigenen Endgeräten, wie Desktop-PC, Laptop oder Smartphone. Der Zugriff auf E-Mails erfolgt über einen Open-Source E-Mail-Client, dessen Quelltext auf Fehler oder Hintertüren geprüft wurde. Sicherheit wird in diesem Fall gegenüber allen oben genannten Angriffsvektoren erreicht, sofern das eigene Endgerät vor Angreifern geschützt ist.

2.2.8. Gründe für mangelnde Nutzung

Bestehende Schutzmaßnahmen sind insgesamt sehr wenig genutzt. Selbst im beruflichen Umfeld verschlüsselt nur jeder Siebte hin und wieder E-Mails.[115] Die mangelnde Nutzung von Sicherheitslösungen ist auf unterschiedliche Gründe zurückzuführen.[116] Ein erster Hinderungsgrund ist ein fehlendes Bewusstsein für die Gefährdung, denen per E-Mail ausgetauschte Kommunikationsinhalte ausgesetzt sind. Dennoch kann darin nicht der Haupthinderungsgrund gesehen werden, wie die Ereignisse um den NSA-Skandal zeigen. Nutzer sind sich der Risiken der durch E-Mail verschickten Kommunikationsinhalte mindestens teilweise bewusst. Besonders vertrauliche Dokumente werden daher nur per Post und nicht per E-Mail verschickt.[117] Mangelnde Awareness kann daher nur als eine Ursache für mangelnde Nutzung bestehender Verschlüsselungssoftware angesehen werden. Weitere Ursachen liegen im Privatheitsverständnis oder mangelndem technischen Know-How.[118] So gibt in Umfragen nur ca. ein Viertel der Bevölkerung an, ihr Verhalten in Bezug auf E-

[115] BITKOM 2014.
[116] Vgl. hier Renaud et.al. 2014.
[117] BITKOM 2012.
[118] Renau et.al. 2014; Schröder 2013.

Mail-Kommunikation seit dem NSA-Skandal geändert zu haben und vorsichtiger geworden zu sein.[119] Zum Teil sind Nutzer unsicher und ratlos, wie genau sie sich besser schützen können.[120] Eine mangelnde Kenntnis über bestehende Lösungen führt also zu deren geringer Verbreitung. Noch maßgeblicher für die mangelnde Verwendung ist jedoch die fehlende Nutzerfreundlichkeit verfügbarer Programme zur Verschlüsselung. Sie sind in ihrer Handhabung zu kompliziert, fordern eine stetige Beschäftigung mit Sicherheitsabfragen und Schlüsselverwaltung oder überfordern das technische Know-How der meisten Nutzer. Bisherige Lösungen sind nach den obigen Untersuchungen nicht nutzerfreundlich genug.[121] Dies hat sich in den letzten 25 Jahren nicht maßgeblich geändert.[122] Ein wesentlicher praktischer Hinderungsgrund besteht auch darin, dass viele unterschiedliche Lösungen verfügbar sind, die teilweise nicht untereinander kompatibel sind. Ein einzelner Nutzer kann somit nicht wirksam verschlüsseln, wenn seine gängigen Kommunikationspartner nicht gleichziehen. Neue Techniken und bestehende Lösungen werden daher nur zögernd aufgenommen.

2.2.9. Konzepte für neue Technologien

Konzepte für neue Technologien können an bestehende Lösungen ansetzen, müssen diese jedoch optimieren und insbesondere im Hinblick auf die Nutzerfreundlichkeit verbessern. Im Sinne der oben genannten Unterscheidung zwischen drei Graden von Sicherheit (geringe Sicherheit, mittlere Sicherheit, hohe Sicherheit) sind neue Technologien insbesondre im Bereich einer nutzerfreundlichen Ende-zu-Ende-Verschlüsselung zu entwickeln. An bestehende Technologien kann in unterschiedlicher Weise angeknüpft werden, indem eine nutzerfreundliche Software zur Ende-zu-Ende-Verschlüsselung flächendeckend bereitgestellt wird. Eine solche Software muss sowohl Funktionen zur Schlüsselerzeugung als auch zur Schlüsselauthentisierung (siehe auch unten „Identitätsbindung der Schlüssel“), also zur Überprüfung der mit dem Schlüssel verbundenen Identität, beinhalten. Daneben sind Funktionen eines Verschlüsselungs-Addins zu einem E-Mail-Client erforderlich, die die einfache Ver- und Entschlüsselung von E-Mails sowie die Verwaltung von Schlüsseln (Import, Export) ermöglicht. Eine Kernkomponente bildet dabei die Kompatibilität mit gängigen E-Mail-Clients in Form eines Addins. Nutzerfreundlichkeit kann nur dann gewährleistet werden, wenn Nutzer ihren gewohnten E-Mail-Client weiter verwenden können. Gegenüber bereits verfügbaren E-Mail-Clients und bereits vorhandenen Addins zur Ende-zu-Ende-Verschlüsselung sind Addins notwendig, die mit den am häufigsten verwendeten Desktop E-Mail-Clients (Outlook, Thunderbird, Apple Mail) kompatibel sind und auch für neue Versionen ständig und zeitnah aktualisiert werden. Durch den steigenden Gebrauch von mobilen E-Mail-Clients ist eine ähnliche Funktionalität auch für gängige mobile E-Mail-Clients zur Verfügung zu stellen. Eine Erweiterung gängiger E-

[119] DIVSI 2014a; DIVSI 2014b.
[120] Ghiglieri, Simo & Waidner 2012.
[121] Siehe ebenso Sasse & Flechais 2005, 20f; Sheng et.al. 2006; Sousedek 2008.
[122] Whitten & Tygar 1999.

Mail-Clients durch ein derartiges Addin hat das Ziel, Nutzer nach einer einfachen Installation in die Lage zu versetzen, E-Mails auf sehr einfache Weise zu verschlüsseln. Dies setzt unterschiedliche Anforderungen an das Addin voraus, die im Folgenden genannt werden:

Vertrauen in die Software

Nutzern kann auf unterschiedliche Weise das Vertrauen gegeben werden, dass die Software keine Hintertüren enthält und ordnungsgemäß funktioniert. Idealerweise ist der Quellcode der Software einsehbar und durch Experten geprüft. Zusätzlich oder alternativ kann die Software von einem aus Nutzersicht vertrauenswürdigen Herausgeber erstellt werden. Schließlich kann Vertrauen auch dadurch erreich werden, dass die Software von einer unabhängigen und aus Nutzersicht vertrauenswürdigen Instanz geprüft und zertifiziert ist.

Installation und Schlüsselerzeugung

Um Laientauglichkeit zu gewährleisten, ist ein sehr einfacher und weitestgehend automatisierter Installationsprozess erforderlich. Ideal wäre sowohl die Möglichkeit der kombinierten Installation mit gängigen Mailclients in einem einzigen Schritt, als auch die Möglichkeit einer nachgelagerten separaten Installation der Software. Bei der Installation sollten bereits installierte Mail-Clients und auf dem System verwendete E-Mail-Adressen erkannt werden. Beim ersten Start kann Nutzerfreundlichkeit dadurch gewährleistet werden, dass der Nutzer in wenigen Schritte durch einen Prozess geführt wird, bei dem Schlüssel für die auf dem System vorhandenen oder für vom Nutzer eingegebene E-Mail-Adressen generiert werden. Dabei ist eine Interaktion der Software mit Browsern oder auf dem System bereits installierten E-Mail-Clients notwendig, um die erzeugten Schlüssel für diese verfügbar zu machen. Die Nutzung der Schlüssel kann dann ohne weiteren Zwischenschritt von diesen Programmen aus erfolgen.

Identitätsbindung der Schlüssel

Eine weitere Anforderung besteht darin, die generierten Schlüssel an eine Nutzeridentität zu binden.[123] Dabei sind unterschiedliche Wege denkbar. Schlüssel können an eine E-Mail-Adresse gebunden werden, die keinen eindeutigen Zusammenhang mit einem Namen erkennen lässt. In diesem Fall kann die Bindung an die E-Mail-Adresse erfolgen, indem der Nutzer den Zugang zu dieser nachweist (z. B. durch einen Prüfcode). Die Bindung an einen Namen ist ferner über andere Verfahren wie Post-Ident, Micro-Payments oder den Neuen Personalausweis denkbar. Die Identitätsbindung der Schlüssel an den Nutzer muss über eine Registrierungsinstanz erfolgen, die die Gültigkeit der Nutzerauthentisierung überprüft und bestätigt.

Ver- und Entschlüsselung von E-Mails

Die Kernfunktionalität des Addins besteht in der Möglichkeit, E-Mails auf einfache Weise ver- und entschlüsseln zu können. Dazu kann die Basisfunktionalität des E-Mail-Clients verwendet werden. Da derzeitige E-Mail-Clients jedoch nur über begrenzt nutzerfreundliche Funktionen zur Schlüsselverwaltung, -verteilung und -nutzung verfügen, ist eine größere Nutzerfreundlichkeit dadurch zu gewährleisten, dass eine entsprechende Funktionalität durch ein Addin bereitgestellt wird. Ausgehende E-Mails sollten automatisch

[123] Vgl. hier auch die von Schmidt 2015b und Schmidt 2015a dargestellte Problematik.

verschlüsselt werden, sofern ein entsprechender Schlüssel des Empfängers vorhanden ist. Ebenso sollten verschlüsselt eingehende E-Mails automatisch entschlüsselt werden.

Schlüsselverwaltung

Die Schlüsselverteilung und Verwaltung gehört zu den Teilen, die in bisherigen Konzepten die größte Nutzerinteraktion erfordern und damit eine Laientauglichkeit verhindern. Dies gilt insbesondere für PGP-Schlüssel, bei denen aufgrund der Vertrauensstruktur in Form eines „Web of Trust" für jeden Schlüssel eine Überprüfung der Echtheit ratsam ist. Eine wichtige Anforderung ist daher, dass die Schlüsselverwaltung fremder Schlüssel wahlweise automatisch erfolgt oder (für technische versiertere Nutzer) selbst gesteuert werden kann. Daher sollte neben einem laienfreundlichen „Standardmodus" auch eine weitergehender „Expertenmodus" mit größeren Auswahl- und Konfigurationsmöglichkeiten vorhanden sein. Im Standardmodus sollten ausgehenden E-Mails automatisch der öffentliche Schlüssel des Nutzers beigefügt werden, bei eingehenden E-Mails könnten beigefügte Schlüssel automatisch importiert werden. Dadurch wird eine weitgehend automatische Schlüsselverwaltung erreicht. Zusätzlich sollten ausgehende E-Mails immer dann automatisch verschlüsselt werden, wenn ein öffentlicher Schlüssel für den Empfänger vorliegt. Sofern dies nicht der Fall ist, kann das Addin auf Schlüsselservern selbstständig nach einem öffentlichen Schlüssel des Empfängers suchen. Daneben sollten erfahrenere Nutzer durch einen Expertenmodus die Möglichkeit haben, zwischen unterschiedlichen Schlüsselservern und ggf. mehreren dort hinterlegten Schlüsseln selbst zu wählen und Schlüssel nur bei Bestätigung durch den Nutzer zu importieren.

Schlüsselverteilung

Die Schlüssel für E-Mail-Verschlüsselung sind derzeit auf einer Vielzahl von öffentlich zugänglichen oder in Unternehmen eingebundenen Schlüsselservern verteilt und somit nicht immer auf einfache Weise zugänglich. Ferner sind die Schlüssel häufig nicht an die Identität eines Nutzers gebunden und somit die Echtheit des Schlüssels nicht gewährleistet. Notwendig ist damit ein Verfahren, durch das ein E-Mail-Addin automatisch nach dem öffentlichen Schlüssel eines E-Mail Empfängers sucht und die Nachricht mit diesem verschlüsselt. Dies kann insoweit umgesetzt werden, als ein E-Mail-Addin standardmäßig auf den bekanntesten Schlüsselservern nach einem Schlüssel des Empfängers sucht. Die Überprüfung der Echtheit dieses Schlüssels ist mit der bestehenden Infrastruktur jedoch nicht benutzerfreundlich umsetzbar und erfordert eine gesonderte Betrachtung auf der Suche nach Lösungsmöglichkeiten. Dies gilt umso mehr, als PGP-Schlüssel auch für fremde Schlüssel einfach erstellt und im Internet verbreitet werden können. Damit steigt die Gefahr, gefälschte Schlüssel zu importieren.[124] Mit solchen Schlüsseln verschlüsselte E-Mails bleiben damit für die intendierten Empfänger unlesbar. Im Falle von S/MIME ist die Authentizität letztlich immer durch Certificate Authorities begründet, worin ebenfalls eine potentielle Schwachstelle liegt.[125] Dem Importieren gefälschter Schlüssel dadurch zu entgehen, dass der Nutzer selbst für jeden Schlüssel die Echtheit überprüft, widerspricht

[124] Schmidt 2015a; Schmidt 2015b.

[125] Siehe hier Brauckmann 2014; vgl. auch den Fall um den niederländischen Zertifikatsanbieter Diginotar: http://www.heise.de/security/meldung/Der-Diginotar-SSL-Gau-und-seine-Folgen-1423893.html.

aber dem Prinzip einer einfachen Nutzbarkeit. Denkbar wäre es, eine Vernetzung verschiedener Schlüsselverzeichnisse zu erreichen oder Schlüssel über DNSSEC („Domain Name System Security Extension“) und DANE („DNS-based Authentication of Named entities“) in DNS-Server zu integrieren.[126] Neben einer notwendigen Ausdetaillierung zahlreicher damit verbundener Fragestellungen setzt eine solche Lösung eine stärkere Verbreitung der Protokolle DANE und DNSSEC voraus. Wäre diese gegeben, könnten E-Mail-Anbieter zur Überprüfung und Bestätigung eines mit einer E-Mail-Adresse verbundenen öffentlichen Schlüssels beitragen und die Schlüssel auf DNS-Servern hinterlegen. Addins zu E-Mail-Clients könnten damit über DANE und DNSSEC zu jeder E-Mail-Adresse automatisch eine authentische Kopie des öffentlichen Schlüssels beziehen, ohne dass dabei jedes Mal eine Nutzerinteraktion notwendig ist.

Verwendung von Verschlüsselungsstandards

Um der Zersplitterung unterschiedlicher Ansätze zur E-Mail-Verschlüsselung entgegenzuwirken, sollte sich die Verschlüsselung mittelfristig auf gängige Verfahren wie PGP und S/MIME konzentrieren. Diese werden von den meisten bisher verfügbaren Anbietern von Verschlüsselungssoftware unterstützt, weisen bezüglich der Schlüsselauthentizität jedoch potentielle Schwachstellen auf. So erfordert die Authentisierung von PGP-Schlüsseln durch ein „Web of Trust“ häufige Nutzerentscheidungen, um der Gefahr von gefälschten Nutzerschlüsseln zu entgehen.[127] Langfristig sind daher auch Alternativen zu untersuchen.

Privacy by Design

Eine flächendeckende Nutzung von Ende-zu-Ende-Verschlüsselung ist nur dann zu erreichen, wenn die Funktionalität durch ein Addin vom Nutzer nicht zusätzlich installiert werden muss, sondern bereits standartmäßig in gängigen E-Mail-Clients integriert ist.

2.3. Fazit

Kommunikationsinhalte werden im digitalen Zeitalter zunehmend elektronisch übermittelt. Die Vielzahl der dabei verwendeten Kanäle reicht von Messaging-Dienste, Chat und Voice-chat, über Kommunikation in sozialen Netzwerken oder E-Mail-Kommunikation. Auch klassische Kommunikationskanäle wie Telefon-Kommunikation oder Briefe werden zunehmend durch digitale Varianten wie Voice-over-IP-Telefonie oder E-Mail über das Internet übermittelt.[128] Ein wirksamer Schutz der Kommunikationsinhalte ist nur über den Einsatz von Verschlüsselung möglich. Gegenüber einem großflächigen Abschöpfen der Kommunikationsinhalte bieten Lösungen zur Transportverschlüsselung wirksame Gegenmaßnahmen.[129] Gegen weitergehende Angriffe durch Hacker, Administratoren oder Angreifer, die mit den Kommunikationsdienstleistern selbst kooperieren, bietet nur eine Ende-zu-Ende-Verschlüsselung wirksamen Schutz. In Folge des NSA-Skandals ist eine Zunahme an verfügbaren Lösungen der Verschlüsselung zu beobachten. Dies betrifft Verschlüsselungs-Apps für Messaging-Dienste oder Chat und zeigt sich am deutlichsten

[126] Vgl. hier Strotman 2015 und http://heise.de/-2571867.
[127] Schmidt 2015b.
[128] Radicati 2015.
[129] Waidner 2014.

im Bereich der E-Mail-Kommunikation. So garantieren zahlreiche E-Mail-Provider mittlerweile eine konsequente Transportverschlüsselung zu anderen Providern und den Endgeräten des Kunden. Die dabei verwendeten Verschlüsselungsmechanismen entsprechen jedoch nicht immer dem aktuellen Stand der Forschung. Obwohl Lösungen zur Ende-zu-Ende-Verschlüsselung einen über Transportverschlüsselung hinausgehenden Schutz bieten, werden diese kaum genutzt. Dies liegt vor allem daran, dass die vorhandenen Lösungen wenig nutzerfreundlich sind und technisch nicht versierte Benutzer schnell überfordern. Notwendig ist daher die Entwicklung von Lösungen, die auf Standards wie PGP und S/MIME aufsetzen und sich in häufig genutzte Programme (Browser und E-Mail-Clients) integrieren lassen. Lösungen dieser Art, etwa durch die Entwicklung von Open-Source-Addins für E-Mail-Clients, sollten sich ferner durch große Nutzerfreundlichkeit auszeichnen[130] und in Bezug auf Schlüsselerstellung, -verwaltung sowie Schlüsselaustausch und -verteilung weitestgehend im Hintergrund arbeiten. Konzepte solcher Lösungen sind bereits vorhanden und in einzelnen Aspekten bereits verfügbar (mindestens prototypisch). Dennoch ist noch keine massentaugliche Lösung verfügbar, die allen genannten Kriterien genügt. Weitere Forschungsarbeit ist ferner im Bereich der Schlüsselverteilung notwendig. Es sind Lösungen zu entwickeln, wie Schlüssel an eine Identität gebunden und vertrauenswürdig verteilt werden können. Aussichtsreiche Ansätze wie die Integration von Schlüsseln in DNS-Einträge müssen weiter verfolgt und praxistauglich gemacht werden.

[130] Cranor 2005.

3. Verbindungsdaten

Zusätzlich zu den in Kapitel 2 beschriebenen Kommunikationsinhalten müssen die Kommunikations-Metadaten bei einer umfassenden Bedrohungs-Analyse der Privatsphäre der Nutzer miteinbezogen werden. Mit Metadaten werden Daten bezeichnet, die Informationen über andere Daten enthalten. Beispiele sind die Angabe von Autor und Titel bei Büchern, oder auch von Künstler und Titel bei Musikstücken. Im Bereich des Privatsphärenschutzes sind hierbei vor allem die Verbindungsdaten interessant, da diese Daten unter anderem beinhalten können, wer wann mit wem kommuniziert hat. Indem diese Daten in großem Umfang gesammelt und analysiert werden, z. B. im Rahmen der VDS oder durch die NSA, lassen sich Profile der einzelnen Nutzer erstellen, und Beziehungen zwischen den Nutzern erkennen. Die Analyse von Metadaten ist besonders interessant, da die anfallenden Daten durch den Wegfall der Kommunikationsinhalte deutlich geringer sind. Die Relevanz der Metadaten wurde in der Vergangenheit auch durch die Geheimdienste öffentlich bestätigt:

> ...metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content… [It's] sort of embarrassing how predictable we are as human beings.[131]

Der ehemalige Chef der NSA und des CIA, Michael Hayden, äußerte sich hierzu auf einer Podiumsdiskussion im April 2014 besonders deutlich[132]:

> Wir töten auf der Basis von Metadaten.

Das US-Militär sieht die auf der Basis der Analyse von Verbindungsdaten gewonnenen Informationen als aussagekräftig genug an, um Verdächtige zu orten und umzubringen.

Im Folgenden werden verschiedene Bedrohungs-Szenarien vorgestellt. Sind Gegen- oder Schutzmaßnahmen verfügbar, werden diese ebenfalls vorgestellt und hinsichtlich des damit erreichbaren Schutzniveaus und der Benutzbarkeit durch den Nutzer evaluiert.

3.1. Überblick über Techniken mit anfallenden Verbindungsdaten

Bei fast allen modernen Kommunikationstechniken fallen Verbindungsdaten in verschiedenen Formen an. Im Folgenden werden zuerst E-Mail, Messaging-Dienste, und Telefonkommunikation betrachtet. Der Schwerpunkt des Kapitels liegt auf den bei der Internetnutzung anfallenden Verbindungsdaten.

3.1.1. E-Mail-Kommunikation

Bereits in den 60er Jahren war es möglich, Nachrichten zwischen Nutzern des gleichen Großrechners zu übertragen. Anfang der 70er Jahre war es möglich, auch Nachrichten über ein Netzwerk zu versenden, indem man dem Benutzernamen des Adressaten ein „@“

[131] Zitat von Stewart Baker, http://www.nybooks.com/articles/archives/2013/nov/21/snowden-leaks-and-public/
[132] Briegleb & Holland 2014.

und den Hostnamen des Zielcomputers hinzufügte. Heute ist E-Mail eine der am häufigsten genutzten Kommunikationsarten im Internet.

Der Austausch von Nachrichten erfolgt asynchron, d.h. Sender und Empfänger müssen nicht gleichzeitig online sein und eine E-Mail kann gleichzeitig an mehrere Empfänger versendet werden. Die E-Mail wird vom Computer des Senders mittels SMTP[133] zum Mailserver seines Providers übertragen. Von dort wird die E-Mail zum Mailserver des Providers des Empfängers übertragen, und schließlich vom Empfänger über ein spezielles Protokoll (POP3 oder IMAP) abgerufen, siehe auch Abbildung 3 in Kapitel 2.

Der Aufbau einer E-Mail besteht aus zwei Teilen: Dem Header, der unter anderem Informationen über Sender und Empfänger enthält und für die Zustellung benötigt wird, und dem eigentlichen Inhalt der Nachricht. Die im Header enthaltenen und damit bei der E-Mail-Kommunikation auftretenden Metadaten sind unter anderem:

- Name, E-Mail und IP-Adresse des Senders
- Name und E-Mail-Adresse des Empfängers
- Betreff
- Datum, Uhrzeit und Zeitzone
- Eindeutige ID der Nachricht

Durch die Analyse von Sendern und Empfängern lassen sich Beziehungsgraphen erstellen, deren Genauigkeit mit der Menge an zur Verfügung stehenden Daten steigt. Mit „Immersion", einem am MIT entwickelten Online-Tool[134], lässt dich die Effizienz dieser Analysen sehr gut verdeutlichen.

Als individueller Nutzer kann man mit Hilfe von Immersion nur seine eigenen sozialen Verbindungen analysieren. Besteht allerdings Zugriff auf die E-Mail-Metadaten von mehreren Personen, lassen sich die einzelnen Graphen miteinander verbinden, und ermöglichen damit, die Genauigkeit und die Abdeckung des Beziehungsgraphen deutlich zu steigern. Die NSA hat in der Vergangenheit über mehrere Jahre hinweg in großem Umfang E-Mail-Metadaten gesammelt,[135] und die daraus erstellten Netzwerke verwendet, um die Kontakte von verdächtigen Personen zu identifizieren und zu überprüfen. Zur Speicherung der gesammelten Metadaten wird eine spezielle Datenbank verwendet („Marina"). Darin abgelegte Informationen werden bis zu einem Jahr aufbewahrt, auch für Personen, bei denen keine Überwachung angeordnet wurde.[136]

[133] Siehe zu SMTP (Simple Mail Transport Protocol) https://tools.ietf.org/html/rfc5321.
[134] Immersion, siehe https://immersion.media.mit.edu/.
[135] Siehe http://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama.
[136] Siehe http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents.

Abbildung 4 zeigt das Ergebnis einer auf einem Google-Mail Account durchgeführten Analyse. Die farblich unterschiedlich markierten Gruppen von Knoten spiegeln sehr genau die in der Realität tatsächlich vorhandenen Gruppen von Personen wider. Die durch die Analyse identifizierten Gruppen sind unter anderem:

- Kommilitonen aus dem Studium (Orange)
- Kollegen, wobei zwischen verschiedenen Jobs unterschieden wird (Lila, Rot)
- Mitbewohner (Rosa)
- Privater Freundeskreis, unterschieden nach Orten bzw. Lebensabschnitten (Blau, Grün)

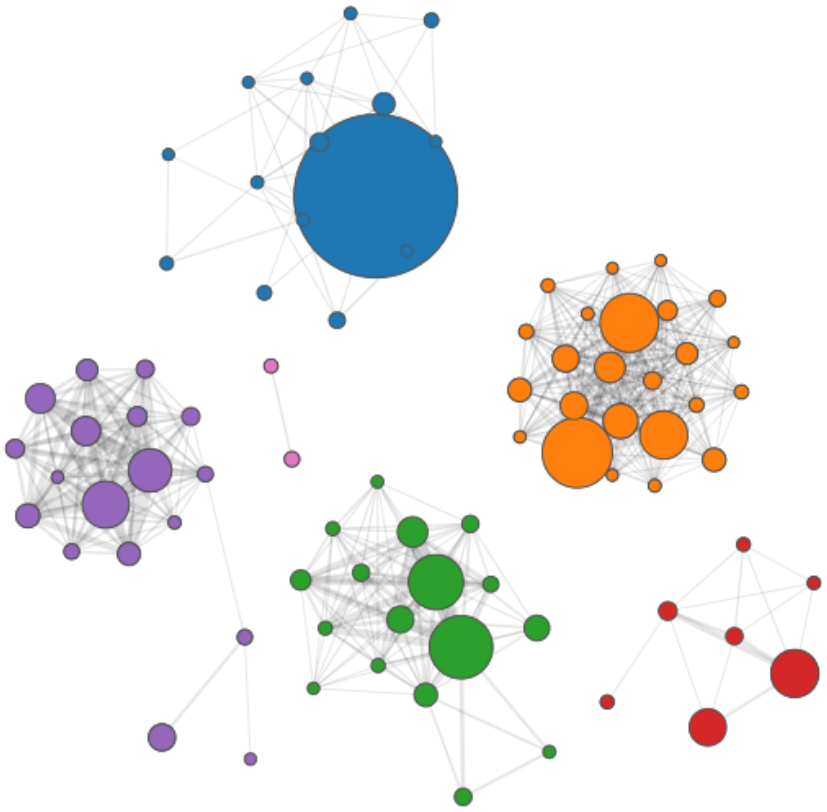

Abb. 4: Von Immersion ermittelter Graph

Das hier vorgestellte Ergebnis spiegelt eine Analyse des kompletten E-Mail-Verkehrs einer Person über mehrere Jahre wider. Neben dem Erkennen von sozialen Beziehungen lassen sich über zeitlich begrenzte Analysen, die mit Immersion auch möglich sind, auch Änderungen im Leben der Nutzer erkennen, wie z. B. Umzüge, neue Jobs oder Abschluss des Studiums. Auch die Intensität der Beziehung zu einzelnen Kontakten kann anhand der Häufigkeit der Kommunikation abgeschätzt werden. Bei der Analyse wurden ausschließlich die Header und damit die Metadaten der E-Mails analysiert, die erreichte Einteilung in die verschiedenen Gruppen war ohne jeglichen Zugriff auf die Inhalte der E-Mails möglich.

Die Ergebnisse der Analysen werden teilweise auch von den Providern in ihre Dienste eingebaut mit dem Ziel, die Attraktivität des eigenen Dienstes zu steigern. Bei Google-Mail

wird eine auf der Erkennung von Beziehungen aufbauende Funktionalität angeboten: Wird bei einer E-Mail ein Kontakt als Empfänger eingegeben, werden dem Nutzer vom System als bekannt identifizierte Kontakte vorgeschlagen, die er dann bequem per Mausklick hinzufügen kann.

Vermeidung von Metadaten

Um die bei der E-Mail-Kommunikation anfallenden Metadaten zu verringern, gibt es verschiedene Möglichkeiten. Bei der Verwendung von Klartext-Protokollen werden diese Daten unverschlüsselt übertragen und sind daher für Angreifer mit Zugriff auf das Netzwerk einsehbar.

Durch die Verwendung von Transport-Verschlüsselung kann verhindert werden, dass Angreifer auf Netzwerk-Ebene Zugriff auf die übertragenen Metadaten erhalten. Allerdings ist damit erstmal nur die Verbindung bis zum eigenen Mail-Server abgesichert, der Nutzer hat keine Kontrolle darüber, wie die Nachrichten zwischen den Mail-Servern übertragen oder schließlich vom Empfänger abgerufen werden. So wurden z. B. in Deutschland bis Mitte August 2014 die E-Mails zwischen den Mail-Servern der großen Provider unverschlüsselt übertragen. Erst mit der Einführung von „E-Mail made in Germany“ sollen E-Mails durchgängig vom Sender bis zum Empfänger verschlüsselt werden, was bisher allerdings nur zwischen wenigen deutschen Providern möglich ist.[137] Mit DANE existiert ein offener Standard, mit dem verschlüsselte Verbindungen zwischen Mail-Servern erzwungen werden können. DANE wird unter anderem vom deutschen E-Mail Provider Posteo[138] und von mailbox.org[139] unterstützt. Selbst bei der Verwendung von durchgängiger Verschlüsselung auf der Transport-Schicht liegen die Metadaten auf allen an der Verbindung beteiligten Servern in Klartext vor.

Durch die Verwendung von Ende-zu-Ende Verschlüsselung mittels der gängigen E-Mail-Verschlüsselungsverfahren (wie z. B. PGP und S/MIME) lässt sich die Menge an auswertbaren Metadaten weiter verringern. Eine komplette Vermeidung von Metadaten ist bei E-Mails allerdings nicht ohne weiteres möglich, hierzu müssen andere Dienste verwendet werden. Verfügbare Alternativen sind in Kapitel 2.2.6 beschrieben.

3.1.2. Messaging-Dienste

Auch bei den in Kapitel 2.1.4 bereits beschriebenen Messaging-Diensten[140] werden neben den eigentlichen Inhalten noch zusätzliche Informationen zwischen den Nutzern übertragen. Die anfallenden Metadaten sind vom verwendeten Protokoll abhängig, beinhalten aber bei den nicht auf sichere Kommunikation spezialisierten Diensten normalerweise mindestens Sender, Empfänger und Datum sowie die Uhrzeit der Nachricht. Damit sind die gleichen Analysen möglich wie bei den E-Mail-Verbindungsdaten.

---

[137] Siehe auch Kapitel 2.2.3

[138] Posteo unterstützt DANE/TLS, vgl. https://posteo.de/blog/posteo-unterstützt-danetlsa.

[139] DANE und DNSSEC bei mailbox.org, siehe https://mailbox.org/dane-und-dnssec-fuer-sicheren-e-mail-versand-bei-mailbox-org/

[140] Beispiele sind ICQ, WhatsApp, Facebook Messenger, XMPP.

Beim weit verbreiteten XMPP Protokoll[141] können unter anderem die folgenden, zusätzlichen Daten anfallen:

- Adressen von Sender und Empfänger in der Form user-id@server
- Name des verwendeten Konferenzraums
- Eindeutige ID der Unterhaltung
- Datum und Uhrzeit der Nachrichten

Vermeidung von Metadaten

Um die anfallenden Metadaten zu minimieren, können die Nutzer auf spezielle Chat-Programme zurückgreifen, deren Verfügbarkeit seit der NSA-Affäre stark zugenommen hat. Ein Nachteil bei diesen Diensten ist die systembedingte Inkompatibilität mit anderen Messenger-Diensten.

- Bleep[142] wird von der amerikanischen Firma BitTorrent Inc.[143] entwickelt und unterstützt sowohl Textnachrichten als auch verschlüsselte Telefonate über VoIP. Bei der Installation des Clients wird ein Schlüsselpaar erzeugt, dessen öffentlicher Teil als Identifikation des Nutzers dient. Es gibt keine Nutzernamen wie bei anderen Diensten. Um die öffentlichen Schlüssel auszutauschen, können von Bleep erzeugte QR-Codes verwendet werden. Die zwischen den Nutzern stattfindende Kommunikation erfolgt verschlüsselt. Dabei werden Algorithmen verwendet, die Perfect Forward Secrecy bieten. Um auf zentrale Server verzichten zu können, werden verteilte Hashtabellen verwendet, anhand derer die IP-Adressen der Nutzer ausgehend vom öffentlichen Schlüssel aufgelöst werden.
  Die Software befindet sich aktuell noch in einem frühen Entwicklungsstadium (Alpha-Version) und ist für Windows, Mac OS X und Android verfügbar. Der Quellcode der Software ist nicht öffentlich (Closed Source), eine unabhängige Überprüfung ist daher nicht ohne Weiteres möglich.
- Tox[144] wird von einem anonymen Team entwickelt, bietet Unterstützung für Textnachrichten, Dateiübertragungen, Telefonate und Video-Anrufe, und verfolgt einen ähnlichen Ansatz wie Bleep: Auch bei Tox wird ein öffentlicher Schlüssel als Identität verwendet. Zur Verschlüsselung der Kommunikation wird die NaCl-Bibliothek[145] eingesetzt.
  Die Software ist für Linux, Windows und Mac OS X verfügbar, zusätzlich gibt es Clients für Android und iOS. Der Quellcode ist offen.[146]
- Ricochet[147] ist eine Weiterentwicklung von TorChat und wird vom Messenger-Projekt invisible.im unterstützt. In diesem Projekt arbeiten Sicherheitsexperten, Programmierer und Journalisten an der Entwicklung eines sicheren Messengers, bei dessen Verwendung keine auswertbaren Metadaten anfallen. Jeder Ricochet-

[141] XMPP, siehe https://tools.ietf.org/html/rfc6120.
[142] Siehe http://labs.bittorrent.com/bleep/.
[143] Siehe http://www.bittorrent.com/company/about.
[144] Siehe https://tox.im/.
[145] Verwendete Algorithmen bei Tox:
curve25519 für Schlüsselaustausch, xsalsa20 für Verschlüsselung, poly1305 für MAC.
[146] Siehe für den Quellcode von Tox: https://github.com/irungentoo/toxcore.
[147] Ricochet Instant Messenger, siehe https://ricochet.im/.

Client erzeugt einen sogenannten „Hidden Service“ im Tor-Netzwerk, der als Identität des Nutzers dient. Diese Hidden Services sind nur über das Tor-Netzwerk erreichbar, und es sind keine praktischen Möglichkeiten bekannt, die Anonymität des Hidden Service aufzuheben, also auf die tatsächliche IP-Adresse des Nutzers zu schließen. Die Kommunikation zwischen den Nutzern erfolgt innerhalb des Tor-Netzwerks, und ist daher verschlüsselt.
Die Software befindet sich noch in einem sehr frühen Entwicklungsstadium (Alpha-Version) und ist für Windows, Mac OS X und Linux verfügbar. In der aktuellen Version können lediglich Text-Nachrichten zwischen den Nutzern ausgetauscht werden. Der Quellcode ist offen und auf GitHub verfügbar.[148]

3.1.3. Telefon-Kommunikation

Bei der klassischen Festnetz-Telefonie sind die anfallenden Metadaten die Telefonnummern der beiden Kommunikationspartner, der Zeitpunkt, die Dauer und die Häufigkeit der Kommunikation. Auch hier lassen sich Beziehungsgraphen erstellen.

Bei der Mobil-Telefonie kommen noch eine Reihe weiterer Metadaten hinzu. Hierzu gehören unter anderem die eindeutige Kennung des Telefons (IMEI), die eindeutige Kennung der Sim (IMSI) und die Kennung der Funkzelle, in der sich der Nutzer aktuell aufhält. Bewegt sich der Nutzer während er telefoniert, lässt sich anhand der vom ihm durchquerten Funkzellen ein Bewegungsprofil erstellen. Die Funkzellen sind besonders in Städten aufgrund der hohen Bevölkerungsdichte relativ klein und erlauben damit eine Positionsbestimmung des Nutzers bis auf wenige 100m. Durch die Auswertung der Metadaten kann sowohl die Bewegung als auch die Aktivitäten der betroffenen Person überwacht werden. Die folgende Abbildung ist ein Ausschnitt aus einer Visualisierung eines Beispiel-Szenarios, bei der der Tagesablauf einer fiktiven Person in Berlin nur anhand von Metadaten rekonstruiert wird.[149]

Abb. 5: Bewegung einer fiktiven Person durch Berlin

[148] Siehe für den Quellcode von Ricochet: https://github.com/ricochet-im/ricochet.
[149] Rieger 2010, jeder grau umrandete Bereich entspricht einer Funkzelle.

Eine andere Verdeutlichung der durch die Analyse von Metadaten erreichbaren Informationen wurde 2011 auf Zeit Online veröffentlicht.[150] Die Basis waren die vom Grünenpolitiker Malte Spitz bei der Telekom eingeklagten Vorratsdaten seines Mobiltelefons. Die Positionsdaten wurden mit frei im Netz verfügbaren Informationen verknüpft und ermöglichen so eine interaktive Reise durch das Leben des Politikers.

Eine weitere Möglichkeit, über die Analyse der Metadaten an vorher unbekannte Informationen zu kommen, wurde von der NSA im Rahmen des CO-TRAVELER Programms verwendet. Dabei wurde erfolgreich versucht, Beziehungen zwischen Benutzern anhand der Bewegungsmuster zu erkennen. Hierzu wurden zuerst über die zeitlich genau feststellbare Zugehörigkeit zu verschiedenen Funkzellen die Bewegungsmuster der zu analysierenden Nutzer erstellt. Diese Muster wurden dann für alle Nutzer auf Überlappungen durchsucht.[151] Wenn sich Nutzer immer wieder zu gleichen Zeiten auf den gleichen Wegen befinden, kann davon ausgegangen werden, dass zwischen diesen Nutzer eine Verbindung besteht, z. B. weil sie in der gleichen Firma arbeiten oder gemeinsam an Treffen teilnehmen.

Die bei Voice-over-IP anfallenden Metadaten hängen vom verwendeten Protokoll ab. Bei dem häufig verwendeten „Session Initiation Protokoll“ (SIP[152]) können unter anderem die folgenden Daten anfallen:

- Betreff
- Name und SIP-Adresse oder Telefonnummer von Sender und Empfänger
- Eindeutige ID der Unterhaltung (Call-ID)

Diese Daten können verschlüsselt übertragen werden, zum Beispiel mit Hilfe des Secure Real-Time Transport Protocol (SRTP). Zum Schlüsselaustausch kann das Protokoll „ZRTP“ verwendet werden, bei dem sich die Gesprächspartner mittels des Diffie-Hellman-Schlüsselaustauschs auf ein gemeinsames Geheimnis einigen können.

Vermeidung von Meta-Daten

Bei der Verwendung des Fest- oder Mobilfunk-Netzes gibt es keine Möglichkeit die zusätzlich zur Sprachübertragung anfallenden Daten zu vermeiden oder zu verringern. Es gibt eine Reihe von speziellen Programmen zur Sprachkommunikation, bei denen weniger oder keine zusätzlichen Daten anfallen. Diese Programme nutzen meist das Internet zur Übertragung der Daten.[153] TorFone[154] ist eine Erweiterung für TorChat, baut auf dem von Phil Zimmermann entwickelten PGPFone auf und überträgt die Gespräche über das Tor-Netzwerk.

---

[150] Biermann 2011.
[151] Saeltzer 2014.
[152] Session Initiation Protocol, vgl. https://tools.ietf.org/html/rfc3261.
[153] Beispiele sind die bereits in Kapitel 2.1.2 genannten SilentPhone und RedPhone.
[154] TorFone, siehe http://torfone.org/.

3.1.4. Fallbeispiel: Telekomgate 2008

Ein Beispiel aus der realen Welt lieferte die Telekom im Jahr 2008. Der Vorfall wurde nach der Aufdeckung als „Telekomgate“ bezeichnet, und der Telekom wurde der Big Brother Award 2008 in der Kategorie "Arbeitswelt und Kommunikation" verliehen[155].

Nachdem interne, eigentlich nur dem Vorstand bzw. Aufsichtsrat zugängliche Informationen an die Öffentlichkeit gelangten, begann die Telekom systematisch mit der Suche nach der undichten Stelle. Hierzu wurden neben legalen Methoden auch illegal beschaffte Verbindungsdaten der verdächtigen Personen analysiert, mit dem Ziel, herauszufinden, welche Telekom-Mitarbeiter mit welchen Journalisten gesprochen hatten. Durch "die Auswertung mehrerer hunderttausend Festnetz- und Mobil-Verbindungsdatensätze" sollen zusätzlich noch Bewegungsprofile erstellt worden sein, um feststellen zu können, ob sich verdächtige Personen miteinander getroffen haben.[156] Es ist unklar, zu welchen Schlüssen die Untersuchungen geführt haben.

3.2. Schwerpunkt: Schutz von bei Internet-Kommunikation anfallenden Verbindungsdaten

In diesem Abschnitt werden die bei der Internetkommunikation anfallenden Verbindungsdaten werden betrachtet. Nach einer Analyse des aktuellen Zustands und einer Verdeutlichung der daraus resultierenden Bedrohungen für die Privatsphäre, werden verfügbare Schutzmechanismen hinsichtlich ihres Schutzniveaus und ihrer Benutzbarkeit evaluiert.

3.2.1. Zustandsanalyse

Internetkommunikation bezeichnet das Aufrufen von Webseiten mittels eines Browsers, wie z. B. Firefox, Internet Explorer oder Safari. Dabei werden die auf Servern im Internet abgelegten Informationen über HTTP (unverschlüsselt) oder HTTPS (verschlüsselt) vom Nutzer abgerufen und im Browser des Nutzers dargestellt. Neben dem Inhalt der Seite werden auch hier zusätzliche Informationen übertragen:

- Die Adresse des Servers und der abgerufenen Webseite
- Datum und Uhrzeit des Webseitenaufrufs
- Vom Benutzer eingegeben Daten wie Login und Passwörter
- Die IP-Adresse des Nutzer, und damit indirekt auch die Position des Nutzers
- Angaben über die verwendete Software (Browser, Betriebssystem) und über die Hardware (Bildschirmauflösung)
- Cookies und zwischengespeicherte Daten

Wird HTTP verwendet, bei dem alle Daten im Klartext übertragen werden, sind all diese Informationen für Angreifer mit Zugriff auf die Verbindung sichtbar. Bei der Verwendung

[155] Bundestag und Telekom erhalten Big Brother Awards 2008, siehe http://heise.de/-213321.
[156] Schäfer 2010.

von HTTPS werden einige dieser Daten verschlüsselt übertragen, und sind daher für Außenstehende nicht ohne Weiteres zugreifbar, wichtige Felder wie Quell- und Zieladresse bleiben allerdings auslesbar. Eine komplette Verschleierung aller übertragenen Metadaten lässt sich nur durch die Verwendung zusätzlicher Software erreichen, die im Folgenden ausführlich beschrieben wird.

3.2.2. Angriffsmöglichkeiten

Anhand der gesammelten Daten lassen sich die Interessen und das Verhalten der Nutzer analysieren, und es können Profile erstellt werden, deren Detailgrad mit der Menge an gesammelten Informationen ansteigt. Diese Techniken werden allerdings nicht nur von Geheimdiensten oder anderen Angreifern verwendet, sondern auch von normalen Webseiten-Betreibern. Deren Ziel ist es, Nutzer wieder zu erkennen, und ihnen, z. B. in einem Online-Shop, passende Kaufempfehlungen anzuzeigen. Diese Identifizierung der Nutzer kann auf verschiedene Arten erfolgen, z. B. durch beim Besuch der Webseite im Browsern abgelegten Identifikations-Informationen, sogenannten „Cookies". Die einmal beim Nutzer abgespeicherten Cookies werden bei einem späteren Aufruf der Seite erneut mitgesendet und ermöglichen es dem Anbieter, den Nutzer wiederzuerkennen. Neben normalen Cookies gibt es noch weitere Möglichkeiten zur Identifikation der Nutzer. Anhand von Projekten wie „Panopticlick" von der Electronic Frontier Foundation (EFF)[157] oder dem „IP Check" von Jondonym[158] kann sich jeder Nutzer verdeutlichen, welche Informationen er beim Besuch von Webseiten preisgibt. Die individuellen Merkmale von Browser, Soft- und Hardware können auf verschiedenste Arten kombiniert und verwendet werden, um Nutzer zu verfolgen und zu profilieren.[159] So bietet z. B. die amerikanische Firma „spring Metrics" unter dem Schlagwort „Behavioral Targeting" eine Technik an, bei der das Verhalten der Webseiten-Besucher überwacht und analysiert wird.[160]

3.2.3. Gegenmaßnahmen

Es gibt verschiedene Möglichkeiten, um den Zugriff auf die anfallenden Verbindungsdaten zu erschweren bzw. die Menge an anfallenden Daten zu verringern. Die Verwendung von HTTPS bietet keinen effektiven Schutz, da die Adresse der aufgerufenen Seiten im Klartext übertragen wird.

Browser im privaten Modus

Alle gängigen Browser[161] bieten zusätzlich zum normalen Betrieb eine Möglichkeit, in einem „privaten Modus" auf das Internet zuzugreifen. Dabei werden die folgenden Daten nicht dauerhaft auf dem Computer des Nutzers gespeichert:

- Besuchte Seiten
- Formular- und Suchfeldeinträge

---

[157] Panopticlick, siehe https://panopticlick.eff.org/.
[158] IP-Check von JonDonym, siehe https://ip-check.info.
[159] Nikiforakis et.al. 2013.
[160] Spring Metrics: Behavioral Targeting, http://www.springmetrics.com/behavioral-targeting/.
[161] Privater Modus verfügbar bei: Internet Explorer, Safari, Firefox, Opera, Chrome.

- Passwörter
- Downloadliste
- Cookies

Als Anwendungsszenario wird im Allgemeinen das Einkaufen von Geschenken auf gemeinsam genutzten Computern oder die Nutzung fremder Computer (z. B. in einem Internet-Cafe) beschrieben. Der private Modus bietet allerdings keinen ausreichenden Schutz vor Tracking durch Seitenanbieter oder vor der Überwachung der Kommunikationsdaten durch Angreifer. Das Löschen von Cookies erschwert es, Nutzer wiederzuerkennen, macht es aber nicht unmöglich.

Web-Proxies

Bei der Verwendung eines Proxies werden die zu übertragenden Daten über einen zusätzlichen Rechner (den Proxy) umgeleitet, sie nehmen also nicht den direkten Weg vom Client zum Server. Es gibt eine Reihe von Web-Proxies,[162] die sich als Anonymisierungsdienste ausgeben, und bei denen die folgenden beiden Schritte bei einem Seitenaufruf durch den Nutzer durchgeführt werden:

- Der Nutzer ruft die Seite des Web-Proxies auf und gibt die Adresse der Seite ein, die er besuchen will
- Der Web-Proxy lädt die Inhalte der Seite herunter und stellt sie auf seiner eigenen Seite dar

Die Identifizierung des Nutzers ist dabei z. B. durch JavaScript möglich, außerdem werden sämtliche Daten über den Server des Proxy-Betreibers übertragen. Die Proxies könnten auch dazu verwendet werden, den Nutzer anzugreifen: Auf der Black Hat Konferenz 2012 wurde eine Technik vorgestellt, mit der Angreifer über speziell eingerichtete Proxies Schadcode auf den Rechner des Nutzer übertragen können.[163]

Virtual Private Networks

Bei der Verwendung eines Virtual Private Networks (VPN) wird eine direkte, verschlüsselte Netzwerkverbindung zu einem anderen Rechner aufgebaut, und sämtlicher Traffic wird über das VPN geleitet. Es gibt verschiedene Anbieter, die damit werben, die übertragenen Daten des Nutzers, und damit auch seine Identität, zu schützen.[164] Die Daten werden zuerst zum VPN-Server, und dann zum eigentlichen Server übertragen. Dabei können Angreifer im Netzwerk nicht direkt nachvollziehen, welche Seiten vom Nutzer aufgerufen werden, oder die tatsächliche IP-Adresse des Nutzers herausfinden. Der Betreiber des VPN-Servers kann die Verbindungsdaten der Nutzer sehen, daher sollten nur vertrauenswürdige Anbieter in Betracht gezogen werden, deren Serverstandort in einem Datenschutz-freundlichen Land liegt.

---

[162] Siehe unter anderem https://hide.me/, https://zend2.com/, http://anonymouse.org/.
[163] Einschleusen von Schadcode über Proxy, siehe https://media.blackhat.com/bh-us-12/Briefings/Alonso/BH_US_12_Alonso_Owning_Bad_Guys_WP.pdf.
[164] Vgl. die Übersicht verschiedener VPN Anbieter unter http://www.bestvpnservice.com/.

Die Verwendung eines VPNs schützt nicht vor der Identifikation bzw. dem Tracking durch die Betreiber der besuchten Seiten, da auf dem Rechner des Nutzers abgelegte Cookies ausgelesen werden können.

Trotz der Verwendung verschlüsselter Verbindungen kann es trotzdem möglich sein, die vom Nutzer aufgerufenen Webseiten zu erkennen. In einem Paper von 2009 wurde eine Technik vorgestellt, mit der ca. 95% der über ein VPN besuchten Webseiten von einem Angreifer erkannt werden konnten.[165]

Mix-Netzwerke

Die Möglichkeit, Verbindungsdaten zu analysieren und daraus zu erkennen, wer wann mit wem kommuniziert, ist schon lange bekannt. David Chaum veröffentlichte 1981 ein Paper,[166] in dem er eine Technik vorstellt, mit der sich die Sender und Empfänger von Nachrichten verbergen lassen: Er führt eine zusätzliche Komponente ein, den sogenannten „Mix“, der zwischen Sender und Empfänger sitzt, und alle Nachrichten übermittelt. Die Anonymität der Kommunikationsteilnehmer wird durch die Verwendung von asymmetrischer Kryptographie erreicht. Eine Nachricht wird wie folgt verschlüsselt:[167]

- Alice besorgt sich die öffentlichen Schlüssel von Bob und vom Mix
- Alice verschlüsselt die Nachricht an Bob mit dessen Schlüssel, verschlüsselt die bereits verschlüsselte Nachricht mit dem Schlüssel des Mix, und schickt die doppelt verschlüsselte Nachricht an den Mix
- Der Mix entschlüsselt eine der beiden Verschlüsselungen der Nachricht und leitet die (immer noch verschlüsselte) Nachricht an Bob weiter

Angreifer mit Zugriff auf das Netzwerk können an die folgenden Informationen gelangen:

- Alice schickt eine Nachricht an den Mix
- Der Mix schickt eine Nachricht an Bob

Damit ist es nicht mehr direkt möglich, zu erkennen, dass Alice mit Bob kommuniziert hat. Werden die Nachrichten allerdings immer direkt vom Mix weitergeleitet, könnte ein Angreifer versuchen, zwischen dem ein- und ausgehenden Verkehr beim Mix Korrelationen zu erkennen, was ihm erlauben würde, den vom Mix gebotenen Schutz wieder aufzuheben. Das von Chaum vorgeschlagene Verfahren leitet die Nachrichten nicht direkt weiter und verwendet noch weitere Schutzmechanismen, um einen solchen Angriff zu erschweren.

Bei der Verwendung eines einzelnen Mix weiß dieser wer wann mit wem kommuniziert. Ein Zugriff auf diesen Mix würde einem Angreifer daher ermöglichen, die Kommunikationsmuster aufzudecken. Chaum schlägt daher die Verwendung von Mix-Kaskaden vor, bei denen mehrere Mixe hintereinander geschaltet werden. Für jeden Mix wird eine zusätzliche Verschlüsselung der Nachricht mit asymmetrischer Kryptographie durchgeführt, was dazu führt dass jeder Teilnehmer der Kommunikation nur die ihm direkt benachbarten

[165] Herrmann, Wendolsky & Federrath 2009.
[166] Chaum 1981.
[167] In diesem Fall ist “Alice” der Sender und “Bob” der Empfänger der Nachricht.

Teilnehmer kennt. Da weder Sender noch Empfänger noch einer der Mixe die komplette Kommunikation sehen kann, sind die Verbindungsdaten geschützt.

Onion Routing

Aufbauend auf den Entwürfen von Chaum wurde 1996 das sogenannte „Onion Routing“[168] vorgestellt, dessen Ziel es ist, die Analyse von Verbindungsdaten in einem öffentlichen Netzwerk zu erschweren. Ein Proxy auf dem Rechner des Senders wählt zuerst eine Verbindung über mehrere Knoten zum eigentlichen Empfänger, der Aufbau der Verbindung wird über ein spezielles Protokoll gesteuert. Ist die Verbindung aufgebaut, können Daten übertragen werden. Die Daten werden mehrfach verschlüsselt, und bei jedem Knoten wird eine der Verschlüsselungs-Schichten wieder entfernt.[169] Im Gegensatz zu der von Chaum vorgeschlagenen Technik werden die beim Onion Routing übertragenen Daten nicht zwischengespeichert, sondern direkt weitergeleitet. Dies ermöglicht die Verwendung bei Protokollen die eine Echtzeit Übertragung der Daten erwarten, wie z. B. HTTP. Die Autoren gehen kurz auf den evtl. auftretenden Konflikt zwischen Anonymität und Strafverfolgung ein, und schlagen ein Verfahren zur Schlüsselhinterlegung („key escrow“) vor, mit dem, entsprechende Berechtigungen vorausgesetzt, Verbindungen deanonymisiert werden könnten.

Software zum Schutz der Metadaten

Von dem bereits in Kapitel 2.2.6 vorgestellte Technologien kann das Invisible Internet Project (i2p) auch zum Zugriff auf das Internet verwendet werden. Die Daten werden mehrfach verschlüsselt und über verschiedene Knoten des i2p-Netzwerks zum eigentlichen Ziel geleitet. Mehrere einzelne Nachrichten werden zusammengefasst und erneut verschlüsselt, was einen erhöhten Schutz vor Analyse der Verbindungsdaten bieten soll.[170] Über Proxy-Dienste wird eine Schnittstelle zwischen dem in sich geschlossenen i2p-Netzwerk und dem offenen Internet eingerichtet.[171]

Tor – The Onion Router

Tor ist eine Weiterentwicklung des bereits vorgestellten Onion Routings und wurde 2004 in dem Paper „Tor: The Second-Generation Onion Router“ vorgestellt. Die Autoren greifen verschiedene Punkte des von Chaum vorgeschlagenen Verfahrens auf und bieten mit Tor einen „vernünftigen Tradeoff zwischen Anonymität, Benutzbarkeit und Effizienz“.[172] Zu den im Vergleich zum Entwurf von Chaum hinzugefügten Funktionalitäten gehören unter anderem:

- Perfect Forward Secrecy:

  Werden die vom Client verwendeten Schlüssel aufgedeckt, können die in der Vergangenheit übertragenen Daten nicht im Nachhinein aufgedeckt werden. Dies wird durch die Verwendung des Diffie-Hellman Schlüsselaustauschs im „Ephemeral“-

[168] Goldschlag, Reed & Syverson 1996.
[169] Daher auch der Name: Die vielen umeinander aufgebauten Schichten erinnern an eine Zwiebel (Onion).
[170] Diese Technik wird von den i2p-Entwicklern “Garlic Routing” genannt und als Erweiterung des Onion Routings bezeichnet.
[171] Detaillierte Beschreibung von i2p: http://wiki.kairaven.de/open/anon/netzwerk/p/anet08.
[172] Dingledine, Mathewson & Syverson 2004.

Modus erreicht, bei dem die Sitzungsschlüssel nie direkt übertragen und auch nicht dauerhaft gespeichert werden.

- Konfigurierbare Exit Policies

  Jede Exit Node kann über eine Konfigurationsdatei festlegen, welche Arten von Daten oder Protokollen über sie übertragen werden dürfen.

- Integritäts-Sicherung

  Die Integrität der über das Tor-Netzwerk übertragenen Daten wird durch die Verwendung kryptographischer Hashes abgesichert. So können Modifikationen der Daten erkannt werden.

- Unterstützung von „Hidden Services"

  Im Tor-Netzwerk ist es auch möglich, Informationen anonym zur Verfügung zu stellen. Ein „Hidden Service" ist ein speziell konfigurierter Web-Server, der nur über das Tor-Netzwerk erreicht werden kann. Zum Zugriff auf Hidden Services wird ein spezielles „Rendezvous"-Protokoll verwendet, durch das sichergestellt wird, dass die IP-Adresse des Web-Servers nicht aufgedeckt werden kann. Bekannte Beispiele für Hidden Services sind der inzwischen nicht mehr existierende Drogenhandel Silk Road und deren verschiedene Nachfolger.

- Verzeichnis-Server
  Es werden spezielle Server verwendet, die eine signierte Liste der aktuell verfügbaren Knoten des Tor-Netzwerk und deren aktuellen Status zur Verfügung stellen.

Die verschlüsselten Verbindungen laufen über von der Quelle (dem Nutzer) über drei Knoten des Tor-Netzwerks zum eigentlichen Ziel. Jeder Knoten kennt nur seine direkten Nachbarn, die verwendete Route wird vom Client berechnet. Ist eine Route festgelegt, werden die zu übertragenden Daten auf dem Client entsprechend verschlüsselt, und an den ersten Knoten geschickt, von wo aus sie über den zweiten zum dritten Knoten weitergeleitet werden. Der dritte Knoten ist der sogenannte „Exit Node", bei dem Daten das Tor-Netzwerk verlassen und in das Internet übermittelt werden. Die Exit Nodes wurden in der Vergangenheit mehrfach dazu verwendet, die Nutzer des Tor-Netzwerks anzugreifen.[173] Dies ist nur dann möglich, wenn ein Klartext-Protokoll wie HTTP zur Übertragung der Daten verwendet wird. Der Exit Node ist dann in der Lage, alle übertragenen Daten, inkl. Benutzernamen und Passwörtern, zu sehen. Außerdem können die über den Exit Node übertragenen Daten modifiziert werden. Es ist damit möglich, Malware in die heruntergeladenen Daten einzuschleusen. Gegen Angriffe dieser Art kann sich der Nutzer schützen, indem er sicherstellt, dass nur verschlüsselte Verbindungen verwendet werden.

[173] Lindskog & Winter 2014; Pitts 2014.

Die Tor-Software ist in verschiedenen Versionen für viele Betriebssysteme[174] verfügbar, der Quell-Code von Tor ist ebenfalls verfügbar. Tor kann auf verschiedene Arten verwendet werden:

- **Standalone**: Der Tor-Client wird auf dem Rechner installiert. Alle Anwendungen die Tor verwenden sollen, müssen vom Nutzer entsprechend konfiguriert werden.
- **Bundle**: Im Tor-Browser-Bundle sind ein speziell konfigurierter Browser (Firefox) und Tor kombiniert. Nach der Installation kann der Tor-Browser gestartet werden, der automatisch das Tor-Netzwerk verwendet, hier ist keine zusätzliche Konfiguration durch den Nutzer nötig.
- **Verwendung im Router**: Tor kann auch auf dem Router im Netzwerk des Nutzers installiert werden. Damit können die Daten aller Geräte im Heim-Netzwerk des Nutzers über das Tor-Netzwerk übertragen werden. Auf den Endgeräten ist keine spezielle Konfiguration nötig, allerdings erfordert die Einrichtung des Routers relativ viel technisches Detailwissen. Es gibt einzelne Projekte die einen fertig konfigurierten Router anbieten,[175] die Sicherheit solcher Lösungen ist allerdings teilweise umstritten.[176]

Durch die Verwendung von Tor ist Anonymität allerdings noch nicht garantiert. Die Identität der Nutzer kann z. B. auch über Browser Fingerprinting festgestellt werden. Das Tor-Projekt bietet eine Reihe von Hinweisen, wie Tor idealerweise benutzt werden sollte.[177] Die Anonymität kann auch aufgedeckt werden, wenn alle Knoten der ausgehandelten Route miteinander kooperieren, was aber aufgrund der verteilten Architektur von Tor als sehr unwahrscheinlich angesehen werden kann.

Das Tor-Netzwerk besteht aktuell aus ca. 6500 Vermittlungsknoten. Es gibt im Tor-Netzwerk keinen „offiziellen“ Betreiber, jeder kann sich die Software herunter laden, installieren und damit zu einem Teil des Tor-Netzwerks werden. Die Electronic Frontier Foundation hat zuletzt im Juni 2014 eine offizielle Challenge gestartet, mit dem Ziel, dem Netzwerk neue Knoten hinzuzufügen.[178]

JonDo

JonDo ist eine Weiterentwicklung des Java Anon Proxy (JAP), der in einem Projekt an der TU Dresden entwickelt wurde. Die Anonymität wird, wie auch bei Tor, durch mehrfache Verschlüsselung der zu übertragenen Daten und Routing über mehrere Knoten geschützt. Auf JonDo kann über einen kostenlosen Zugang oder einen bezahlten „Premium“ Zugang zugegriffen werden. Die Einschränkungen des kostenlosen Zugangs sind unter anderem:

- Bandbreite maximal 50kb/sec, Dateigröße max. 2 MB
- Nur HTTP/HTTPS verwendbar
- Mixkaskade besteht aus 2 Knoten

[174] Tor ist verfügbar für Windows, Linux, Mac OS X, Android.
[175] Zum Beispiel http://cryptographi.com/products/snoopsafe, oder https://pogoplug.com/safeplug.
[176] Edmundson et.al. 2014; Greenberg 2014.
[177] Siehe https://www.torproject.org/download/download#warning.
[178] Tor Relay Challenge, siehe https://www.eff.org/torchallenge/.

Die Daten werden über eine sogenannte „Mixkaskaden“ übertragen, die aus zwei oder drei Knoten bestehen. Nach der Auswahl einer Kaskade tauscht die JonDo-Software mit den Knoten der Kaskade Schlüssel aus. Die zu übertragenden Daten werden mit den ausgehandelten Schlüsseln mehrfach verschlüsselt, und an den ersten Knoten der Kaskade geschickt. Dort wird ein Teil der Daten entschlüsselt und an den nächsten Knoten bzw. an das eigentliche Ziel weitergeleitet.

Momentan sind 6 kostenlose, und 10 Premium-Kaskaden verfügbar. Die Betreiber der Kaskaden sind bekannt und müssen sich zertifizieren lassen, bevor sie in den JonDo-Dienst mitaufgenommen werden. Die Anonymität kann aufgedeckt werden, wenn alle Knoten einer Kaskade zusammen arbeiten. Um dies zu erschweren, sind die einzelnen Knoten jeder Kaskade in unterschiedlichen Ländern stationiert. Strafrechtlichen Anordnungen zur Aufdeckung der Anonymität müssten daher in jedem betroffenen Land angeordnet werden, was als unwahrscheinlich angesehen werden kann.

Die JonDo-Software ist für verschiedene Betriebssysteme verfügbar, kann allerdings nur genutzt werden wenn Java installiert ist. JonDo kann auf verschiedene Arten genutzt werden:

- **Standalone**: Das JonDo Proxy Programm wird auf dem Rechner installiert. Alle Anwendungen die JonDo verwenden sollen, müssen vom Nutzer entsprechend konfiguriert werden.
- **Mit Browser-Unterstützung**: Mit JonDoFox ist ein Benutzerprofil für Firefox verfügbar, das speziell für sicheres und anonymes Surfen optimiert ist. Neben der Konfiguration von JonDo als Proxy beinhaltet JonDoFox weitere Schutzmechanismen, um möglichst viele der gängigen Tracking-Mechanismen zu blockieren.
- **Als Live-DVD**: Die JonDo Live-DVD verwendet ein speziell angepasstes Linux Betriebssystem und beinhaltet neben JonDo auch Tor und Mixmaster sowie weitere Programme zur sicheren Kommunikation über das Internet. Bei der Verwendung der Live-DVD muss keine Software auf dem Computer des Nutzers installiert werden. Das ISO-Image (1GB) kann von der Webseite heruntergeladen und auf DVD gebrannt werden.

Weitere Lösungen

Tails[179] ist eine speziell für Privatsphärenschutz entwickelte Linux-Distribution, die dazu verwendet werden kann, anonym auf das Internet zuzugreifen und dabei zusätzlich keinerlei Spuren auf dem verwendeten Rechner zu hinterlassen. Neben Tor ist in Tails eine Reihe von weiteren Programmen enthalten, wie z. B. OpenPGP zur Verschlüsselung von Daten, KeePassX zur Verwaltung von Passwörtern und OTR zum sicheren Chatten.

Tails kann als ISO-Image heruntergeladen werden (900MB). Das Image kann auf eine DVD gebrannt oder auf einen USB-Stick kopiert und anschließend von dort gestartet werden. Es sind keine Änderungen am System des Nutzers erforderlich.

[179] The Amnesiac Incognito Live System, https://tails.boum.org/.

Whonix[180] verwendet zwei virtuelle Maschinen: Einen Gateway, der den Zugang ins Internet herstellt, und eine Workstation, auf der die normale Software läuft. Die Workstation ist so konfiguriert, dass nur über den Gateway und damit immer auch über das Tor-Netzwerk auf das Internet zugegriffen werden kann. Neben einem Browser beinhaltet sie außerdem speziell konfigurierte Programme für die Kommunikation per Chat oder E-Mail, und zum Verschlüsseln von beliebigen Daten. Auf der Webseite von Whonix gibt es eine lange Liste mit Warn- und Verwendungshinweisen,[181] sowie viele Hinweise wie Nutzer den Grad ihrer Anonymität erhöhen bzw. verringern können.

Um Whonix verwenden zu können, muss das Programm VirtualBox installiert sein. Die beiden virtuellen Maschinen (Gateway und Workstation, je 1,6 GB) müssen heruntergeladen und in VirtualBox importiert werden.

3.2.4. Bewertung und Verbreitung bestehender Techniken

Die zur Verfügung stehenden Techniken schützen die Anonymität des Nutzers an verschiedenen Stellen. Eine perfekte Anonymität kann keine der zur Verfügung stehenden Techniken bieten. Ein global agierender, passiver Angreifer kann ggf. die Anonymität aufheben, indem er die Daten die in das Anonymitäts-Netzwerk eintreten mit den austretenden Daten vergleicht, und nach auftretenden Korrelationen sucht.[182] Diese Art von Angriff lässt sich aufgrund der Echtzeit-Anforderungen an die Übertragung der Daten nicht komplett ausschließen.

Von den vorgestellten Gegenmaßnahmen bieten der Privacy-Modus der verschiedenen Browser, Web-Proxies und VPNs keinen ausreichenden Schutz der Privatsphäre. Mit der Verwendung von Tor oder JonDo kann ein für den normalen Nutzer ausreichender Schutz der Privatsphäre erreicht werden. Der Schutz lässt sich weiter erhöhen, wenn der Nutzer bereit ist, Einschränkungen beim Zugriff auf das Internet, wie z. B. keine Verwendung von Plugins und damit auch einen Verzicht auf die Darstellung von Videos, einzugehen. Auch ein erhöhter Aufwand bei der Einrichtung, z. B. durch die Nutzung von Spezial-Distributionen, kann zu einem besseren Schutz führen, erfordert aber technisches Detailwissen, das bei einem Großteil der Nutzer nicht vorhanden ist.

Durch die Verwendung verschiedener Anonymisierungsdienste lassen sich unterschiedliche Schutzniveaus realisieren. Ein steigender Grad an Schutz ist dabei meistens gleichbedeutend mit einem höheren Einrichtungsaufwand bzw. dem Verzicht auf bekannte Technologien.

1. **Geringe Sicherheit:** Nutzung von Tor/JonDo zusammen mit normalen Anwendungen (z. B. Browser ohne Einschränkungen)

   Wird der Anonymisierungs-Dienst zusammen mit den normalen Anwendungen des Nutzer verwendet, gibt es verschiedene Möglichkeiten den Nutzer zu identifizieren, z. B. kann die echte, unverschleierte IP-Adresse über Verwendung von Java-

[180] Whonix Anonymous Operating System, https://www.whonix.org/.
[181] https://www.whonix.org/wiki/Warning bzw. https://www.whonix.org/wiki/DoNot.
[182] Johnson et.al. 2013.

Script im Browser erkannt werden. Bei dieser Lösung gibt es die geringsten Einschränkungen bei der Benutzbarkeit, die gebotene Anonymität kann aber relativ einfach aufgehoben werden.

2. **Mittlere Sicherheit:** Nutzung von Bundles (eingeschränkte Browser; TBB/JonDoFox)

   Die aktuell verfügbaren Anonymisierungs-Bundles beinhalten neben dem eigentlichen Dienst einen speziell angepassten Browser, der bewusst auf Features verzichtet um die Anonymität des Nutzers zu schützen. Damit ist eine Aufhebung der Anonymität deutlich schwieriger, die Benutzbarkeit ist allerdings auch eingeschränkt. Die Installation und Einrichtung der Bundles ist verhältnismäßig einfach, kann Nutzer mit wenig technischem Wissen allerdings dennoch überfordern.

3. **Hohe Sicherheit:** Nutzung von Live-Distros (Tails/JonDoLive-DVD) oder VMs (Whonix)

   Mit Tails oder Whonix stehen Lösungen zur Verfügung, bei denen das komplette Betriebssystem darauf abgestimmt ist, die Anonymität des Nutzers zu schützen. Damit soll ausgeschlossen werden, dass durch Fehlkonfigurationen Informationen über die Identität des Nutzers nach außen dringen können. Diese Lösungen sind verhältnismäßig schwierig einzurichten, und unterscheiden sich in ihrer Nutzung stark von dem, was die meisten Nutzer aus ihrem Alltag gewöhnt sind.

Verbreitung bestehender Techniken

Das Tor-Projekt stellt auf seiner Webseite[183] umfassende Statistiken über das Tor-Netzwerk zur Verfügung. Aktuell verbinden sich jeden Tag ca. 200.000 Nutzer aus Deutschland direkt mit dem Tor-Netzwerk, dies sind ca. 9% aller Tor-Nutzer. In Deutschland nutzten 2014 ca. 79% der Bürger das Internet, was einer Zahl von 55,6 Millionen entspricht.[184] Es nutzen also nur ca. 0,036% der deutschen Internetnutzer das Tor-Netzwerk.[185]

[183] Tor Metrics, https://metrics.torproject.org/.
[184] ARD/ZDF Onlinestudie 2014, http://www.ard-zdf-onlinestudie.de/index.php?id=506.
[185] Die Nutzerzahlen sind eine Abschätzung, die auf der Anzahl der an die Verzeichnisserver geschickten Anfragen basiert.

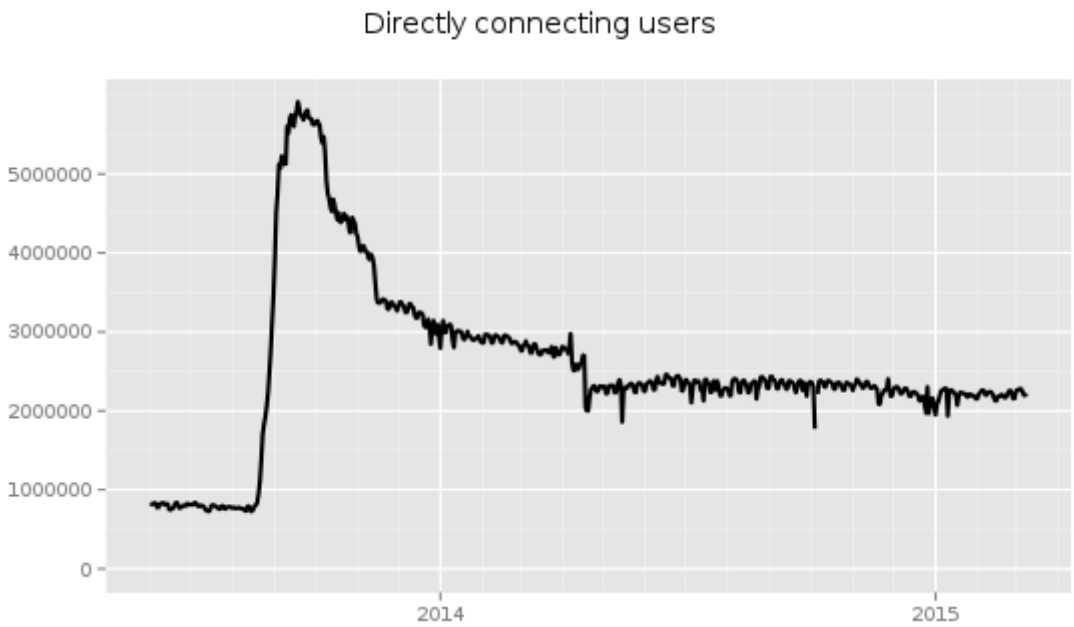

Abb. 6: Entwicklung der Zugriffe auf das Tor-Netzwerk

Abbildung 6 zeigt die Entwicklung der globalen Nutzerzahlen:[186] Bis Mitte 2013 haben täglich ca. 900.000 Nutzer das Tor Netzwerk verwendet. Nach dem Bekanntwerden der NSA-Affäre gab es einen sprunghaften Anstieg, der dann langsam auf den aktuellen Wert gesunken ist.

Auch für JonDo sind die aktuellen Nutzerzahlen online verfügbar.[187] Die kostenfreien Kaskaden können von maximal 2550 Nutzern verwendet werden, die Premium-Kaskaden werden (alle 10 zusammen genommen) meistens von deutlich weniger als 1000 Nutzern verwendet.

3.2.5. Gründe für mangelnde Nutzung

Als Gründe für eine mangelnde Nutzung lassen sich die folgenden Faktoren nennen:[188]

Fehlende Motivation auf Seiten der Nutzer

Den Nutzern ist trotz der umfassenden Berichterstattung unklar, wie intensiv sie überwacht werden, und welche Schlüsse aus der Überwachung gezogen werden können. Die verfügbaren Schutzmechanismen sind größtenteils unbekannt, oder werden als unwirksam angesehen. Allerdings wirkt sich die totale Überwachung auch aktuell nicht wirklich auf den individuellen Nutzer aus. Dies spiegelt sich auch in verschiedenen Umfragen wieder, bei denen teilweise bis zu 75% der Befragten angeben, ihr Verhalten nicht geändert zu haben.[189]

[186] Tor Metrics: Users by Country, Zeitraum 2013-06-01 bis 2015-02-28.
[187] JonDo: Status der Mixkaskaden, https://www.anonym-surfen.de/status/index.php.
[188] Norcie et.al. 2014.
[189] Umfrage des Marktforschungsunternehmens GfK, http://heise.de/-2169169

Fehlende technische Kenntnisse

Für die Einrichtung der hier vorgestellten Techniken sind gewisse technische Vorkenntnisse erforderlich. Selbst die vergleichsweise einfache Installation des Tor Browser Bundles kann Nutzer bereits überfordern. Die korrekte Einrichtung der komplexeren Schutzmechanismen wie Whonix stellt selbst für erfahrene Nutzer eine Herausforderung dar.

Benutzbarkeit der zur Verfügung stehenden Lösungen

Der Zugriff auf das Internet über Tor ist deutlich langsamer als ein direkter Zugang. Wird zusätzlich ein spezieller Browser verwendet, ergeben sich durch den Verzicht auf Techniken wie JavaScript teilweise Darstellungsfehler auf Webseiten, manche Webseiten können ohne JavaScript überhaupt nicht verwendet werden.

3.2.6. Konzepte für neue Technologien

Die folgenden nutzungsfördernden Kriterien lassen sich als Maßgabe für die Entwicklung neuer Technologien ableiten:

Verdeutlichung der Überwachungs-Ergebnisse und der möglichen Konsequenzen

Mit Immersion ist für die E-Mail-Kommunikation ein Tool vorhanden, mit dem die Folgen der Überwachung durch den Nutzer individuell nachvollzogen werden können. Ein vergleichbares Tool für die Analyse der Internetnutzung könnte dem Bürger verdeutlichen, welche Daten über ihn gesammelt werden können, und welche Ergebnisse eine Analyse dieser Daten liefern könnte. Die Lösung könnte als lokaler Proxy realisiert werden, der die aufgerufenen Web-Seiten des Nutzers analysiert. Anhand der aufgerufenen Seiten könnten Profile des Nutzers erstellt werden, die ihm veranschaulichen, welche Folgen die Überwachung haben kann.

Verbesserung der zur Verfügung stehenden Infrastruktur

Um die Geschwindigkeit der über das Tor-Netzwerk übertragenen Daten zu verbessern, könnten verschiedene Institutionen wie Universitäten oder Provider, die über große Bandbreiten verfügen, selbst Knoten im Tor-Netzwerk betreiben. Die Electronic Frontier Foundation hat in den Jahren 2011 und 2014 mit der „Tor Relay Challenge“ eine Initiative gestartet, um möglichst viele neue Knoten für das Tor-Netzwerk zu gewinnen. Beide Challenges waren sehr erfolgreich, 2014 konnten über 1600 neue Knoten für das Tor-Netzwerk gewonnen werden.[190] Das Tor-Projekt unterstützt das „Library Freedom Project“, das unter anderem zum Ziel hat, Tor-Knoten in Bibliotheken zu betreiben.[191]

Stärkung der Medienkompetenz von Bürgern

Vor allem Kinder und Jugendliche, die in den Zeiten von Facebook aufgewachsen sind, haben digitale Medien und soziale Netzwerke ganz selbstverständlich in ihren Alltag in-

[190] Siehe https://www.eff.org/deeplinks/2014/09/tor-challenge-inspires-1635-tor-relays
[191] Für eine Beschreibung des Library Freedom Projects siehe https://libraryfreedomproject.org/ bzw. https://blog.torproject.org/blog/tor-exit-nodes-libraries-pilot-phase-one

tegriert. Es gibt zwar in diesem Bereich bereit Schutz-Programmen wie z. B. spezielle Kinder-Suchmaschinen[192], allerdings noch keine schlüssigen Konzepte, wie Kindern und Jugendlichen die Bedeutung ihrer persönlichen Daten verdeutlicht werden kann. Versuche die Nutzung von sozialen Medien in Schulen zu verbieten hat in der Vergangenheit zu starken Protesten der Schüler geführt.[193] Auch der Thüringer Datenschutzbeauftragte Lutz Hasse sieht Schüler beim Umgang mit persönlichen Daten im Internet schlecht gerüstet. "Sie können sich zwar auf Facebook und anderen sozialen Netzwerken bewegen, sie können auch ihr Handy bedienen, wissen aber nicht, was im Hintergrund passiert", sagte Hasse der Deutschen Presse-Agentur. Das Recht auf informationelle Selbstbestimmung würden die meisten Schüler nicht einmal kennen. [194]

3.3. Fazit

Obwohl bei der Berichterstattung in den Medien meist der Fokus auf der Verschlüsselung der Kommunikationsinhalte liegt, stellt die Analyse von Metadaten eine vergleichbare Gefährdung der Privatsphäre dar. Durch die Auswertung der bei den verschiedenen Kommunikationsarten anfallenden Metadaten lassen sich Profile der Nutzer erstellen, ohne dass ein Zugriff auf die Inhalte nötig ist. Bei der Nutzung von E-Mail und Chat entstehen Metadaten, durch deren Auswertung die sozialen Beziehungen der Nutzer analysiert werden können. Am Beispiel Mobilkommunikation wurde gezeigt, dass über die Auswertung von Mobilfunk-Verbindungsdaten sogar Bewegungsprofile von Nutzern erstellt werden können. Bei den meisten der heutzutage verbreiteten Kommunikationssysteme gibt es kaum Möglichkeiten, die anfallenden Metadaten zu verringern oder zu vermeiden. Die verfügbaren Alternativen, bei deren Entwurf die Vermeidung von Metadaten im Fokus steht, sind meist in der Benutzbarkeit nicht vergleichbar mit den etablierten Systemen. Meist sind die neuen Systeme zusätzlich noch untereinander inkompatibel, was eine weitere Hürde für den Wechsel darstellt.

Im Bereich der Internet-Verbindungsdaten gibt es mit Tor bzw. JonDo Lösungen, die verhältnismäßig einfach zu nutzen sind, aber dennoch Einschränkungen beinhalten. So ist z. B. die Darstellung medialer Inhalte wie Videos nur sehr eingeschränkt möglich, was unter anderem auch an der geringen Geschwindigkeit der Anonymisierungsnetze liegt. Die Nutzerzahlen sind gemessen an der Gesamtbevölkerung extrem niedrig.

Eine Ausweitung der Verbreitung von Techniken, bei denen eine sinnvolle Auswertung der Metadaten nicht mehr möglich ist, kann erreicht werden, indem die identifizierten Gründe für mangelnde Nutzung behoben oder abgemildert werden. Durch die Einbindung großer Netzbetreiber oder Institutionen wie Universitäten und Forschungseinrichtungen, könnte die Geschwindigkeit der Anonymisierungsnetzwerke deutlich erhöht werden. Zusätzlich müssten die Nutzer auf die verfügbaren Lösungen zum Schutz ihrer Privatsphäre

[192] Siehe https://www.fragfinn.de/ und http://blindekuh.de/
[193] Artikel in der c't, http://www.heise.de/-2330731.html
[194] Kossel 2015.

hingewiesen werden. Mit Immersion liegt bereits eine sehr anschauliche Visualisierung für die Auswertung der E-Mail-Metadaten vor. Würde eine vergleichbare Darstellung auf für die anderen Bereiche entwickelt, könnte man die Ergebnisse der verschiedenen Analysen miteinander kombinieren. Diese Gesamt-Analyse würde dem Nutzer sehr detailliert und umfassend aufzeigen, welche Informationen über ihn nur aufgrund der Auswertung von Metadaten in Erfahrung gebracht werden können.

4. Positionsbestimmung

Bei der Positionsbestimmung wird der Aufenthaltsort des Nutzers bestimmt. Die Genauigkeit hängt dabei von der verwendeten Technik ab, Genauigkeiten von wenigen Metern sind heutzutage ohne Probleme erreichbar. Die Positionsbestimmung sollte idealerweise nur mit Zustimmung des Nutzers erfolgen, und die ermittelte Position sollte nicht an Dritte weiter gegeben werden. In der Vergangenheit hat sich allerdings gezeigt, dass die NSA weltweit massenhaft Positionsdaten von Smartphones sammelt und auswertet.[195] Die dabei gesammelten Daten werden in einer speziellen Datenbank (FASCIA) gespeichert und umfassen unter anderem die eindeutige Kennung des Smartphones und die Kennung der Funkzelle.

4.1. Überblick über Techniken der Positionsbestimmung

Im Folgenden werden unterschiedliche Techniken beschrieben, mit denen es möglich ist, die Position des Nutzers zu bestimmen. Nach einem kurzen Überblick wird in Abschnitt 4.2 als Schwerpunkt die Positionsbestimmung von Smartphones behandelt.

4.1.1. Positionsbestimmung über Navigationssatelliten

Bei einem globalen Navigationssatellitensystem[196] werden Satelliten in der Erdumlaufbahn verwendet, die kontinuierlich speziell codierte Signale aussenden. Aufgrund der unterschiedlichen Entfernung des Nutzers zu den einzelnen Satelliten ergeben sich auch unterschiedliche Laufzeiten der Signale. Diese unterschiedlichen Laufzeiten werden verwendet, um die Position des Nutzers zu bestimmen und erlauben, je nach dem verwendeten System, eine Genauigkeit auf wenige Meter. Die Genauigkeit lässt sich durch zusätzliche Verfahren, wie z. B. Differential-GPS, noch deutlich erhöhen (bis auf weniger als 1m). Dabei werden zusätzlich stationäre Empfangsstationen verwendet. Es gibt weltweit verschiedene Systeme, von denen zwei aktuell global verfügbar sind: Das amerikanische GPS (offizielle Bezeichnung NAVSTAR-GPS) und das russische GLONASS. Weitere Systeme sind aktuell in Entwicklung bzw. in Planung.[197]

Da es keinen Rückkanal vom GPS-Empfänger zum Satelliten gibt, kann das GPS-System auch nicht direkt dazu verwendet werden, die Position des Nutzers zu bestimmen. Die GPS-Technik wird unter anderem zur Navigation in Fahrzeugen, zur Wegfindung für Wanderer oder Radfahrer und zum Flottenmanagement verwendet. Hierbei kommen teilweise spezielle Geräte oder Smartphones, die einen GPS-Chip enthalten, zum Einsatz.

[195] Gellman & Soltani 2013.
[196] Zur Einfachheit halber wird im Folgenden die gängige Abkürzung GPS verwendet.
[197] Galileo (Europa), QZSS (Japan), Beidou (China, regional bereits verfügbar).

4.1.2. Positionsbestimmung durch Internetnutzung

Um das Internet nutzen zu können müssen die Nutzer unter einer IP-Adresse erreichbar sein. Diese IP wird Ihnen vom Provider zugewiesen, und bleibt entweder konstant (feste IP) oder ändert sich regelmäßig (dynamische IP, Änderung meist alle 24 Stunden). Ist die IP eines Nutzers bekannt, kann anhand frei verfügbarer Datenbanken[198] die Position des Nutzers bestimmt werden. Die Genauigkeit der Positionsbestimmung beschränkt sich dabei meist auf die Stadt oder Region des Nutzers. Diese Information wird teilweise dazu verwendet, um dem Nutzer ortsbezogene Werbung anzuzeigen oder die auf einer Webseite verwendete Sprache automatisch umzuschalten.

Der Provider kann zusätzlich die exakte Adresse des Anschlussinhabers bestimmen, dem die abgefragte IP-Adresse aktuell zugewiesen ist oder zu einem bestimmten Zeitpunkt zugewiesen war. Diese Informationen dürfen eigentlich nur dann weitergegeben werden, wenn bestimmte rechtliche Voraussetzungen erfüllt sind. Dass diese Voraussetzungen allerdings nicht immer eingehalten werden, zeigte sich Ende 2013: Das Landgericht Köln ordnete die Herausgabe von Namen und Anschriften zu IP-Adressen wegen eines angeblichen Abrufs von Porno-Streams an, ohne dass die hierfür notwendigen Bedingungen gegeben waren.[199] Das Landesgericht revidierte seine eigene Entscheidung im Januar 2014.

4.1.3. Patras

Das Patras-System ist ein vom Deutschen Zoll betriebenes Ortungssystem, mit dem verdächtige Personen, Fahrzeuge und Waren verfolgt werden können. Zur Überwachung werden entweder Mobilfunkgeräte oder spezielle GPS-Tracker verwendet, die z. B. an den zu überwachenden Fahrzeugen befestigt werden. Das System wurde durch einen Hackerangriff im Jahr 2011 auch in der Öffentlichkeit bekannt. Nach Angaben der Hacker waren auf dem Server Bewegungsprofile aus dem ganzen Land zu finden.[200]

4.2. Schwerpunkt: Schutz von Positionsdaten von Smartphones

Die meisten aktuellen Smartphones verfügen sowohl über einen GPS-Empfänger, als auch über eine WLAN-Schnittstelle zur drahtlosen Übertragung von Daten. Außerdem beinhalten die meisten Handy-Tarife einen Datentarif, über den vom Smartphone auf das Internet zugegriffen werden kann, was bereits in Abschnitt 4.1.2 beschrieben wurde. Zusätzlich ergeben sich durch die Architektur des Mobilfunk-Netzwerks weitere Möglichkeiten, die Position des Nutzers zu bestimmen und zu verfolgen.

[198] z. B. http://www.ip-adress.com/ip_lokalisieren/.
[199] Froitzhuber 2014.
[200] Lischka & Rosenbach 2011.

4.2.1. Zustandsanalyse und Angriffsmöglichkeiten

Werden die Positionsdaten über einen längeren Zeitraum gesammelt, lassen sich Bewegungsprofile der Nutzer erstellen.[201] Anhand dieser Profile lassen sich nicht nur die Wohn- und Arbeitsorte bestimmen, sondern es können auch Vorhersagen über die Bewegungen des Nutzers getroffen werden.[202] Auch das bereits in Abschnitt 3.1.3 beschriebene COTRAVELER Programm der NSA nutzt gesammelte Positionsdaten, um Profile zu erstellen und Beziehungen zwischen Personen anhand von Überschneidungen in diesen Profilen zu erkennen. Anhand der Bewegungsprofile können Nutzer auch wiedererkannt bzw. voneinander unterschieden werden: In einer Studie des MIT[203] wurden aus den anonymisierten Daten eines Mobilfunkbetreibers Bewegungsprofile erstellt. Die Daten enthielten 1,5 Millionen unterschiedliche Nutzer, die anhand ihrer Profile eindeutig voneinander unterschieden werden konnten: Bereits mit 4 bekannten Positionen konnten 95% der Nutzer wiedererkannt werden.

Die Positionsbestimmung erfolgt häufig mit Zustimmung des Nutzers, oder wird durch ihn initiiert. Neben klassischen Anwendungen wie Navigations-Systemen, gibt es Dienste wie Facebook Places, Foursquare, und neuerdings auch Dating-Apps wie Tinder.[204] Dabei können die Nutzer selbst in bestimmten Geschäften oder Gaststätten „einchecken", wobei ihre Position dann häufig auch ihren Kontakten mitgeteilt wird. Dienste dieser Art werden häufig genutzt, jeder dritte Smartphone-Nutzer teilt auf diese Weise seinen Standort mit[205].

Foursquare ist einer der bekannten Anbieter in diesem Bereich, und bietet mit Abzeichen einen zusätzlichen Anreiz für das häufige Einchecken an einem bestimmten Ort. Der Nutzer mit den häufigsten CheckIns bekommt zusätzlich den Titel des „Bürgermeisters" verliehen. Auf 45 Millionen aktive Nutzer kommen bei Foursquare jeden Tag 6 Millionen CheckIns.[206] In Deutschland nutzen knapp 500.000 Personen Foursquare.[207] Die Daten werden zur Verarbeitung in die USA übertragen, und Foursquare sichert sich in den AGB ein sehr weitreichendes Nutzungsrecht an allen Nutzereingaben, zu denen auch die CheckIns gehören:

> Indem Sie Nutzereingaben über die Website oder anderweitig durch den Service einsenden, erteilen Sie Foursquare eine weltweite, nicht-exklusive, lizenzgebürenfreie, vollständig beglichene, unterlizenzierbare und übertragbare Lizenz, um **Ihre Nutzereingaben zu benutzen, kopieren, bearbeiten, verändern, vervielfältigen und zu verbreiten, abgeleitete Arbeiten zu erstellen, sie zu zeigen, vorzuführen** und anderweitig im Zusammenhang mit der Website, dem Service und der Geschäftstätigkeit Foursquares (sowie seinen Nachfolgern und Bevollmächtigten) uneingeschränkt zu nutzen, unter anderem etwa dafür, die Website oder den

[201] Choudhury et.al. 2009.
[202] Beal et.al. 2006.
[203] Blondel et.al. 2013.
[204] Tinder, siehe www.gotinder.com.
[205] BITKOM, https://www.bitkom.org/Presse/Presseinformation/Jeder-dritte-Smartphone-Nutzer-teilt-seinen-Standort-mit.html, 2013.
[206] Golbeck 2015.
[207] Foursquare: Nutzerzahlen in Deutschland, Stand 2013, http://allesfoursquare.de/500-000-foursquare-nutzer-in-deutschland-dach-nutzerzahlen-das-grose-geheimnis/.

> Service ganz oder in Teilen zu bewerben und weiterzuverbreiten (ebenso wie davon abgeleitete Arbeiten), in jedem beliebigen Medienformat und über sämtliche Medienkanäle (einschließlich etwa Websites und Feeds Dritter).
>
> Quelle: AGB Foursquare,[208] Hervorhebung hinzugefügt.

Die Dating-App Tinder wird von ca. 2 Millionen Menschen in Deutschland genutzt.[209] Die App bestimmt den Standort des Nutzers, um ihm Singles in seiner Umgebung anzuzeigen. Eine Nutzung der App ist nur möglich, wenn der Nutzer auch einen Facebook-Account besitzt. Tinder hat nach der Autorisierung durch den Nutzer auch Zugriff auf alle Inhalte seines Facebook-Profils. Wie bei Foursquare sind auch bei Tinder die Nutzungsrechte, die sich das Unternehmen an den gesammelten Daten einräumt, sehr weitreichend. Anfang 2015 wurde bekannt, dass Tinder mit Gillette zusammenarbeitet: Gillette stellt die These auf, dass ungepflegte Gesichtsbehaarung unattraktiver ist, und will dies mit den von Tinder bereitgestellten Daten überprüfen.[210] Es gab in der Vergangenheit mehrere Sicherheitslücken bei Tinder, die sehr gut verdeutlichen, welche Folgen der unvorsichtige Umgang mit hochgradig sensiblen Daten haben kann: Im Juli 2013 wurde bekannt, dass bei Anfragen über die API die exakte GPS-Position des gerade vom Nutzer angesehen Profils übertragen wurde.[211] Auch nach der Behebung dieser Schwachstelle war es weiterhin möglich, die Position andere Nutzer zu bestimmen: Statt der exakten GPS-Position wurde die Entfernung zur Position des angefragten Profils übertragen. Der Angreifer erstellte sich drei unterschiedliche Profile, ermittelte jeweils die Entfernung zum Profil des Ziel-Nutzers, und bestimmte dann mittels Triangulation dessen exakte Position.[212]

Positionsbestimmung mit Hilfe des Mobilfunknetzes

Die Position von Mobilfunk-Nutzern lässt sich anhand der eindeutigen Kennung der Funkzelle bzw. des Sendemastes bestimmen. Die Genauigkeit hängt dabei von der Größe der Funkzelle ab, deren Durchmesser zwischen ca. 200 Metern in Innenstädten und mehreren Kilometern in ländlichen Gebieten variiert.[213] Die Bestimmung der Funkzelle ist für das Routing von Gesprächen und Daten nötig, und sollte im Normalfall nur für den Netzwerk-Betreiber möglich sein.

Zur Positionsbestimmung durch Dritte werden meistens sogenannte „Stille SMS“ verwendet, die zwar an das Telefon des Nutzers übertragen, dort aber nicht dargestellt wird. Die deutschen Sicherheitsbehörden haben diese Technik im ersten Halbjahr 2014 knapp 140.000-mal verwendet.[214] Es gibt allerdings auch kommerziell angebotene Produkte,[215]

---

[208] AGB Foursquare, https://de.foursquare.com/legal/terms.
[209] Spiegel Online, 2015, www.spiegel.de/netzwelt/web/a-1015930.html.
[210] Gillette teams up with Tinder, http://www.news4jax.com/news/30809778.
[211] Siehe http://qz.com/106731/tinder-exposed-users-locations/.
[212] Include Security, Februar 2014, „How I was able to track the location of any Tinder user“, http://blog.includesecurity.com/2014/02/how-i-was-able-to-track-location-of-any.html.
[213] Telekom 2013.
[214] Keine Angaben vom Zoll, wahrscheinlich insgesamt noch deutlich mehr; vgl. Spiegel Online: www.spiegel.de/politik/deutschland/a-984665.html.
[215] Skylock von Verint, Infiltrator Real Time Tracking System von Defentek Vital Solutions.

die jedem Kunden eine solche Positionsbestimmung ermöglichen. Um einen Mobilfunknutzer mit einem dieser Produkte zu lokalisieren, ist lediglich dessen Mobilfunknummer nötig. So kann z. B. auf handyorten.org eine „Handyortung in nur 60 Sekunden“ ab 90 Cent gebucht werden.[216] Auf dem Chaos Communication Congress 2014 wurde von Tobias Engel[217] gezeigt, dass prinzipiell jeder, der Zugriff auf das im Kern des Mobilfunknetz verwendete SS7-Protokoll erlangen kann, die Position von Nutzern bestimmen kann.

Durch die Verwendung von IMSI-Catchern, speziellen Geräten zur Ortung von Mobilfunkteilnehmern, lässt sich die Position eines Nutzers noch genauer bestimmen: Der IMSI-Catcher gibt sich als Basisstation des Mobilfunknetzes aus, mit dem Ziel, dass sich das Smartphones des Nutzers in die vorgetäuschte Basisstation einbucht. Bei der Verwendung eines IMSI-Catchers werden neben der eigentlichen Zielperson die Positionen aller Personen in der Nähe bestimmt.

Positionsbestimmung durch WLAN-Technik

Es gibt zwei unterschiedliche Möglichkeiten, um die Position des Nutzers mit Hilfe der WLAN-Technik zu bestimmen:

Auswertung der sichtbaren WLAN-Netzwerke: Je nachdem, wo sich der Nutzer aktuell aufhält, ist eine bestimmte Menge von WLAN-Netzwerken für ihn sichtbar. Sind die Standorte der sichtbaren WLAN-Netzwerke bekannt, kann durch die Auswertung der empfangenen Signalstärken die Position des Smartphones bestimmt werden. Es gibt verschiedene, teilweise öffentlich verfügbare Datenbanken,[218] die eine Liste von SSIDs und deren Position enthalten. Die Bestimmung der Position erfolgt auf dem Gerät des Nutzers.

Verfolgung der MAC-Adresse des Smartphones: Um sich mit einem bekannten WLAN-Netzwerk zu verbinden, senden die meisten Smartphones regelmäßig sogenannte „Probe Requests“ aus, die neben der global eindeutigen MAC-Adresse der WLAN-Schnittstelle im Smartphone teilweise auch den Namen des bekannten Netzwerks enthalten. Diese Probe Requests werden unverschlüsselt übertragen, und können mit relativ geringem Aufwand von Personen in Reichweite des Smartphones mitgehört werden. Es gibt hierfür spezielle Software,[219] die auf normalen Laptops genutzt werden kann. Durch die Verwendung von spezieller Hardware[220] lässt sich der Angriff noch einfacher bzw. effizienter durchführen. Die Position des Nutzers kann damit bis auf einen bestimmten Radius um den Punkt bestimmt werden, von dem aus der Angriff durchgeführt wird. Damit könnte z. B. überwacht werden, wann der Nutzer sein Haus verlässt, ein bestimmtes Café betritt, oder sich an einer bestimmten Haltestelle aufhält. Die Positionsbestimmung erfolgt von außen, erfordert aber, dass der Angreifer an den Orten, an denen er die Nutzer überwachen will, entsprechende Detektoren platziert hat.

---

[216] Siehe https://www.handyorten.org/ortung-starten.php.
[217] Engel 2014.
[218] Siehe z. B. https://location.services.mozilla.com/, https://combain.com/, http://openwlanmap.org.
[219] Kostenlos und frei verfügbar: http://edwardkeeble.com/2014/02/passive-wifi-tracking/ und http://blog.rootshell.be/2012/01/12/show-me-your-ssids-ill-tell-who-you-are/.
[220] WiFi Pineapple, https://www.wifipineapple.com/.

Werden im Probe Request auch die Namen der bekannten WLAN-Netzwerk übertragen, lassen sich zusätzliche Informationen über den Nutzer sammeln, z. B. welche Cafés er häufig besucht oder in welchen Hotels er regelmäßig übernachtet.

Die Verfolgung des Nutzers ist auch möglich, wenn keine regelmäßigen Probe Requests ausgesendet werden. Selbst bei identischen WLAN-Schnittstellen gibt es minimale Unterschiede in den übertragenen Datenpaketen. Durch die Auswertung dieser Unterschiede können passive Angreifer einzelne Geräte mit sehr hoher Wahrscheinlichkeit identifizieren.[221]

Positionsbestimmung mit Hilfe von Bluetooth Low Energy

Mit Bluetooth Low Energy[222] wird eine Weiterentwicklung von Bluetooth bezeichnet, deren Fokus vor allem auf einem deutlich geringeren Energieverbrauch und geringeren Kosten liegt. Mit BLE ist es möglich, kostengünstige kleine Sender (sogenannte Beacons) herzustellen, die kontinuierlich Daten aussenden. Diese Beacons können mit Hilfe spezieller Apps dazu verwendet werden, die Position des Nutzers bis auf weniger als einen Meter zu bestimmen, auch innerhalb von Gebäuden. Anwendungsszenarios sind das Anzeigen von ortsbezogenen Informationen wie z. B. Werbung. Beacons werden allerdings auch in Museen[223] und als Kunstprojekte[224] verwendet.

Anfangs waren für die Auswertung der Daten spezielle Apps nötig, mit iOS 8 wird die Funktionalität jedoch bereits im Betriebssystem integriert. Die Bestimmung der Position erfolgt auf dem Gerät des Nutzers. Es gibt mit Bluetooth Low Energy keine direkte Möglichkeit, die Position des Nutzers von außen zu bestimmen. Allerdings kann es sein, dass die vom Nutzer verwendeten Beacon-Apps die lokal ermittelte Position weiter geben.

Positionsbestimmung durch die Analyse des Stromverbrauchs

Eine weitere Möglichkeit die Position des Nutzers zu bestimmen, wurde Anfang 2015 von Forschern der Universität Stanford vorgestellt.[225] Dabei wird über Zugriff auf den Ladezustand der Batterie der aktuelle Stromverbrauch gemessen, der als Indikator für die Position des SmartPhones verwendet wird, und davon abhängt, wie groß die Entfernung zur Basisstation ist. In den vorgestellten Tests konnte in 93% der Fälle zwischen vier bekannten Routen unterschieden werden. Die Positionsbestimmung kann allerdings nur an bereits bekannten Orten durchgeführt werden, und wird durch das Vorhandsein von anderen Apps, die sich ebenfalls auf den Stromverbrauch auswirken, deutlich erschwert.[226]

---

[221] Banerjee et.al. 2008.
[222] Alternativ auch bezeichnet mit iBeacon, Bluetooth LE oder Bluetooth Smart.
[223] Eggert 2014.
[224] Sweeper App zur Verdeutlichung der Gefahren von Landminen: http://mashable.com/2014/04/04/ibeacons-land-mines-simulation/.
[225] Boneh et.al. 2015.
[226] Scherschel 2015.

Positionsbestimmung durch Kombination der verschiedenen Techniken

Die Genauigkeit der Positionsbestimmung kann verbessert werden, indem die verschiedenen hier vorgestellten Techniken miteinander kombiniert werden. Google Maps verwendet GPS, WLAN und die Kennung des Mobilfunkmastes um die Position des Nutzers zu bestimmen.[227] Unter iOS werden GPS, WLAN, Mobilfunk und Bluetooth zur Positionsbestimmung verwendet.[228]

4.2.2. Verfügbare Schutzmaßnahmen

Auf dem Endgerät lässt sich die Positionsbestimmung mit Hilfe des Mobilfunknetzes nicht verhindern. Es gibt lediglich die Möglichkeit, Angriffe mit Hilfe spezieller Apps zu erkennen, z.B. mit dem Android IMSI-Catcher Detector oder Snoopsnitch.

- Android IMSI-Catcher Detector

  Die „Android IMSI-Catcher Detector"-App (AIMSICD[229]) soll Angriffe mittels IMSI-Catcher und den Empfang von stillen SMS erkennen, und den Nutzer darüber benachrichtigen. Der Quellcode der kostenlosen App ist frei verfügbar.

- Snoopsnitch[230]

  Die App „Snoopsnitch" wird von der Berliner Firma SRLabs entwickelt, ist kostenlos im Google PlayStore erhältlich und ermöglicht das Erkennen von Angriffen mittels IMSI-Catcher und den Empfang von stillen SMS. Die von der App gesammelten Daten werden auf dem SmartPhone gespeichert und können optional an das „GSM Security Map"[231] Projekt übertragen werden.

Der Nutzer kann sich gegen einige der vorgestellten Techniken zur Positionsbestimmung schützen, indem er die entsprechende Hardware (GPS-Empfänger, WLAN-Schnittstelle, Bluetooth) in seinem Smartphone deaktiviert. Mit Hilfe von „Fake Location"-Apps[232] können falsche GPS-Daten eingegeben werden, die echte Position des Nutzers kann dann durch andere Apps mittels GPS nicht mehr bestimmt werden. Die App „Location Privacy" der Firma PlaceMask[233] ermöglicht dem Nutzer, die von ihm verwendeten Apps in verschiedene Klassen einzuteilen, und für jede Klasse individuelle Einstellungen bzgl. der Genauigkeit der Positionsbestimmung vorzunehmen. Zusätzlich bietet die App eine Übersicht über alle Apps, die die Position des Nutzers bestimmen möchten. Da bei den aktuellen Smartphone Betriebssystem allerdings meistens gleichzeitig unterschiedliche Techniken zur Positionsbestimmung verwendet werden, bietet das Deaktivieren einzelner Techniken keinen ausreichenden Schutz.

---

[227] Siehe https://support.google.com/gmm/answer/2839911.
[228] Siehe https://support.apple.com/de-de/HT201357.
[229] AIMSICD-App: https://secupwn.github.io/Android-IMSI-Catcher-Detector/.
[230] SnoopSnitch-App: https://opensource.srlabs.de/projects/snoopsnitch.
[231] GSM Security Map: https://gsmmap.org.
[232] Im Google PlayStore sind sehr viele „Fake Location" Apps verfügbar, auch kostenlos.
[233] PlaceMask: http://www.placemask.com/.

Es gibt spezielle Schutzhüllen wie „Der Stalin“,[234] die durch die Verwendung von Abschirmfolie alle Verbindungen zum Handy blockieren. Die Verwendung solcher Schutzhüllen bietet einen effektiven Schutz vor jeglicher Art von Ortung, zur normalen Nutzung muss das Telefon allerdings aus der Tasche genommen werden, womit der Schutz unwirksam wird. Einen Schutz vor Ortung würde auch das Entfernen des Akkus bieten, dies ist bei aktuellen Geräten allerdings oft nicht mehr möglich.

4.2.3. Konzepte für neue Technologien

Weiterentwicklung und Evaluierung bestehender Schutzmechanismen

Die wenigen existierenden Schutzmechanismen wie Snoopsnitch, AIMSICD oder PlaceMask sind bisher nicht hinsichtlich des tatsächlich gebotenen Schutzes detailliert evaluiert. Eine solche Evaluierung könnte einerseits, bei positiven Ergebnissen, das Vertrauen der Nutzer in die Schutzmechanismen steigern. Werden andererseits bei der Evaluierung Fehler oder ein nicht ausreichendes Schutzniveau entdeckt, könnte dies in die Weiterentwicklung und kontinuierliche Verbesserung der Apps miteinfließen.

Awareness

Auch bezüglich der Bedrohung der Privatsphäre durch die Positionsbestimmung scheinen die Nutzer nicht ausreichend informiert zu sein. Durch die Verwendung von Diensten wie Facebook Places, Foursquare oder Tinder geben die Nutzer freiwillig und kontinuierlich ihre eigene Position preis und erlauben den Dienstanbietern durch Akzeptieren der AGB nahezu komplette Freiheit bei der Verarbeitung der gesammelten Informationen. Hier könnte es hilfreich sein, anhand einer neu entwickelten App alle Positionsdaten des Nutzers auf seinem eigenen Telefon zu überwachen, zu sammeln, und ihm in einer visuell aufbereiteten Form zur Verfügung zu stellen. Dabei sollte der Nutzer auch darüber informiert werden, wie er sich vor den festgestellten Bedrohungen schützen kann.

Mix Zones

Vor allem im Bereich der Car-to-X Kommunikation gibt es aktuell viele Forschungsaktivitäten die sich mit der Steigerung der Privatsphäre durch die Verwendung von sogenannten Mix Zones beschäftigen.

4.3. Fazit

Die Position des Nutzers wird dauerhaft von unterschiedlichen Akteuren bestimmt. Dies erfolgt teilweise ohne Wissen und Zustimmung des Nutzers, wie im Fall der Positionsbestimmungen mittels Mobilfunk durch staatliche Behörden, und teilweise bewusst durch die aktive Nutzung von Diensten und Apps wie Facebook Places, Foursquare oder Tinder. Dabei steht die freizügige Weitergabe der eigenen Position durch die Nutzer bei den verschiedenen Apps im starken Kontrast zur Bedeutung der eigenen Position für die Wahrung der Privatsphäre.

[234] „Der Stalin – die abhörsichere Handytasche“, http://www.derstalin.de/.

Der Nutzer kann sich nur in sehr begrenztem Umfang vor den verschiedenen Möglichkeiten der Positionsbestimmung schützen. Bei der Positionsbestimmung mittels WLAN oder GPS kann der Nutzer eingreifen, indem die Techniken abgeschaltet werden, oder die Ergebnisse der Positionsbestimmung mittels spezieller Apps verfälscht bzw. deren Genauigkeit herabgesetzt wird. Die Ortung über Mobilfunk kann vom Nutzer zwar mit Hilfe von Apps wie Snoopsnitch erkannt, aber nicht verhindert werden.

Es ist für den Nutzer also kaum möglich, sein Mobiltelefon aktiv zu nutzen und gleichzeitig die eigene Position zu Verschleiern oder sogar ganz zu Verbergen. Dies spiegelt sich auch in den Aussagen von verschiedenen Forschern wider, wie z. B. Chris Soghoian von der ACLU (um den eigenen Standort nicht zu verraten, müsste man „alle modernen Kommunikationsgeräte ausschalten und in einer Höhle leben.“[235]) oder Tobias Engel vom Chaos Computer Club („Schutzmöglichkeiten für Mobilfunk-Nutzer: Telefon wegwerfen.“[236])

[235] Gellmann & Soltani 2013
[236] Engel 2014

5. Daten im Bereich Smart Home

Der Begriff „Smart Home“ bezeichnet eine Vielzahl von Geräte am und im Haus, die mit Sensoren und Netzwerkverbindungen ausgestattet sind und durch intelligente Funktionen die Wohnqualität erhöhen.[237] So können Haushaltsgeräte selbstständig über das Internet Haushaltsprodukte oder Lebensmittel bestellen. Multimediageräte können vernetzt werden und damit hinsichtlich Funktionsumfang und Nutzungsqualität verbessert werden. Und schließlich können ältere Menschen durch Technikeinsatz leichter betreut oder bezüglich ihrer Gesundheit durch Sensoren in der Wohnung kontrolliert werden. [238]

Die Vernetzung von Haushaltsgeräten nimmt aufgrund der damit verbundenen Vorteile von Tag zu Tag.[239] So geht die Fokusgruppe Connected Home des Nationalen IT-Gipfels der mit Smart-Home-Technologien ausgestatteten Haushalte bis 2020 von einem Wachstum von 18-24% aus.[240] Neben diesen Vorteilen liegen Risiken für die Privatsphäre der Haus- oder Wohnungsbewohner auf der Hand: Sensoren, die Bewohner oder deren Geräte ständig kontrollieren, können leicht zur Überwachung missbraucht werden. Dementsprechend warnen Datenschützer vor den Risiken der Überwachung oder warnen vor technischen Schwachstellen in der Sicherheitsausstattung von Geräten des intelligenten Hauses.[241] Dieses Kapitel gibt einen Überblick über Techniken im Bereich Smart Home und zeigt die damit verbundenen Risiken für die Privatsphäre auf. In einer Schwerpunktanalyse werden insbesondere Smart-TVs im Hinblick auf Risikopotential gängiger Geräte und mögliche Schutzmaßnahmen hin untersucht.

5.1. Überblick über Techniken im Bereich Smart Home

„Smart Home“ ist ein Sammelbegriff für die Vernetzung verschiedener Geräte, die eine intelligenter Kommunikation der Geräte untereinander sowie eine komplexe (Fern-)Steuerung einzelner Geräte ermöglichen. Die zu Smart Home gehörigen Komponenten lassen sich in verschiedene Kategorien einteilen: Durch den Begriff der Haus- oder *Gebäudeautomation* werden die fest am Haus installierten Einrichtungen wie Außen- und Innensensoren (z. B. Lichtmesser oder Bewegungsmelder), Alarmanlagen, gesteuerte Rollläden, Einfahrt- bzw. Garagentore, Außen- und Innenbeleuchtung und Heizung zusammengefasst. Eine andere Komponente ist *Smart Metering* als Bezeichnung von intelligenten Strom-, Wasser- oder Gaszählern. Schließlich bilden *netzwerkfähige elektronische Geräte* wie Kühlschränke, Spielekonsolen, vernetzte E-Book-Lesegeräte oder Smart-TVs weitere Komponenten des Smart Home. Im Folgenden werden anhand dieser Kategorisierung eine Vielzahl von zu Smart Home gehörenden Geräten kurz vorgestellt und hinsichtlich

[237] OECD 2013.
[238] Klinger 2012; Schulze 2012; Zahneisen 2012; Kuhlen 2012.
[239] Statista 2010 (“Wie wird sich der Markt für Smart Home bis 2020 entwickeln?”); Kuhlmann 2014.
[240] Fokusgruppe Connected Home des Nationalen IT-Gipfels 2014.
[241] Ohland 2014; Jacoby 2014; Wocher 2014; Froböse 2014, Aufsichtsbehörden 2014; Weichert 2014. Siehe ferner http://www.heise.de/newsticker/meldung/Smart-Home-Datenschuetzer-warnt-vor-Big-Brother-im-Haus-2160624.html;
http://www.smarthome-guide.de/smart-home-und-ueberwachung-freiheit-statt-angst/.

des Bedrohungspotentials der damit verbundenen Daten und möglichen Schutzmaßnahmen analysiert.

5.1.1. Gebäudeautomation

Gebäudeautomation umfasst die Steuerung von Haustechnik wie Alarmanlagen, Außen- oder Innenbeleuchtung, Heizkörper, Steckdosen oder Rollläden. Alarmanlagen werden entweder von darauf spezialisierten Firmen angeboten, [242] oder zusammen mit anderen Geräten über ein Smart-Home-Starterset gesteuert.[243] Smart-Home-Sets werden von verschiedenen Anbietern vertrieben und bieten umfassende Sensoren und Steuerelemente der Gebäudeautomation, die unter einer einzigen Plattform miteinander vernetzt sind. Anbieter sind Firmen wie Gigaset, RWE, iConnect, QIVICON, iComfort, tapHOME oder XAVAX MAX. Da durch unterschiedliche Anbieter eine Segmentierung der zur Verfügungen stehenden Technologien entsteht, versucht die Initiative QIVICON der Deutschen Telekom zusammen mit deutschen Industrieunternehmen vernetzbare Geräte unterschiedlicher Hersteller miteinander zu kombinieren und zu einem einheitlichen System zu verschmelzen. [244] Eine weitere Bestrebung zur Vereinheitlichung bildet der Zusammenschluss von ABB, Bosch und Cisco zur Entwicklung einer einheitlichen Software-Plattform für das vernetzte Haus.[245] Der derzeitige Markt bietet damit immer umfassendere und einfachere Möglichkeiten, Steuerungsmöglichkeiten der Gebäudeautomation in einem einzigen, zentral steuerbaren System zu verbinden.

Durch die rasante Marktentwicklung sind die verfügbaren Lösungen hinsichtlich ihrer Sicherheitsarchitektur jedoch nicht immer hinreichend durchdacht und offenbaren zahlreiche Sicherheitslücken. So zeigt eine Untersuchung von Smart-Home-Starter-Kits, dass vier von sieben der marktführenden Anbieter in ihren Lösungen Schwachstellen oder ernstzunehmende Sicherheitslücken aufweisen.[246] Dazu zählen eine mangelnde oder fehlende Verschlüsselung der Netzwerkkommunikation, Manipulationsmöglichkeiten bei der Steuerung, mangelnder Schutz gegen interne Angreifer oder fehlende Authentisierung der Geräte untereinander.[247] Ähnliche Schwachstellen finden sich bei Alarmanlagen. So findet die Übermittlung von Signalen der Sensoren von Alarmanlagen untereinander häufig unverschlüsselt statt, so dass Angreifer die Alarmanlage leicht umgehen können.[248] Dementsprechend erweist sich die Annahme, dass eine Zunahme an Sicherheitssensoren auch zu einer Zunahme an Sicherheit führt, als Trugschluss. Gerade Alarmanlagen sind anfällig für eine Vielzahl von Angriffen, durch die Alarme unterdrückt oder manipuliert werden können.[249]

---

[242] So etwa Lösungen von Mobilcom oder Gigaset.
[243] So beispielsweise ADT, ABUS,
[244] Siehe https://www.qivicon.com/.
[245] Siehe http://www.mobilegeeks.de/news/abb-bosch-und-cisco-gruenden-unternehmen-fuer-smart-home-software-standards/ ;
http://www.abb.de/cawp/seitp202/da5416d57b3cccd4c1257c12003a2c27.aspx.
[246] Lösche et.al. 2014.
[247] Lösche et.al. 2014.
[248] Zetter 2014.
[249] Lamb 2014; Cesare 2014.

Durch diese Sicherheitslücken im Bereich der Gebäudeautomation können nicht nur die Lebensgewohnheiten der Bewohner eines Smart Homes bis ins Einzelne verfolgt werden (Überwachen von unverschlüsselten Sensordaten von Licht-, Temperatur- oder Bewegungssensoren), sondern auch gezielte Einbrüche geplant und durchgeführt werden (Detektieren von Abwesenheitszeiten der Bewohner, Überwinden der Alarmanlage, etc.). Abhilfe schafft nur ein vollständig durchdachtes Sicherheitskonzept, dass in der Praxis allerdings noch Mangelware ist.

5.1.2. Smart Metering

Durch die Zunahme an vielfältigen erneuerbaren Energiequellen ist die Gewährleistung eines Gleichgewichts zwischen Energieeinspeisung und Energiebedarf zu einer komplexen Herausforderung geworden. Dies ist dadurch bedingt, dass eine größere Anzahl von dezentralen Quellen Energie ins Netz einspeisen (dazu können auch private Haushalte zählen), diese aber hinsichtlich der spezifischen Einspeisezeiträume meist nicht mit den Zyklen des Spitzenverbrauches übereinstimmen. Um die Stabilität des Netzes zu gewährleisten, ist ein Smart Grid („intelligentes Netz“) notwendig, das durch Smart Meter („intelligente Zähler“) an den Einspeise- und Verbrauchspunkten in der Lage ist, Energieerzeugung und Energiebedarf zu koordinieren.[250]

Die Verwendung von Smart Metern für Strom, Erdgas, Fernheizung und Warmwasser ist seit 2006 durch eine EU-Richtlinie geregelt[251] und soll in Deutschland für Haushalte mit einem Verbrauch über 6.000 Kilowattstunden pro Jahr verpflichtend sein.[252] Als Smart Meter werden Zähler bezeichnet, die einen Micro-Prozessor enthalten. Der tatsächliche Verbrauch wie auch die tatsächliche Nutzungszeit von Energie kann zu jeder Zeit angezeigt und über ein Kommunikationsnetz an den Energieversorger übermittelt werden. Die Übermittlung der Verbrauchsdaten kann dabei auf unterschiedliche Weise erfolgen, etwa über die Festnetztelefonleitung, Mobilfunk, GPRS, LAN oder über das Stromnetz. Smart-Meter erstellen eine Tageskurve über den Energieverbrauch. Energieanbieter können so zielgerichteter Tarife anbieten, die sich am Verbrauch der Nutzer messen. Zudem können Nutzer durch günstige Tarife dazu bewegt werden, ihren Verbrauch teilweise von Spitzenzeiten in Randzeiten zu verlegen, wodurch ein gleichmäßigerer Energieverbrauch erreicht wird.

---

[250] Vgl. für eine Übersicht der mit Smart Grid verbundenen Teilnehmern und Rollen: Eckert, Krauß 2011; Eckert & Krauß 2012; vgl. ferner Broy 2012 und die im Sommer 2013 vorgestellten Ergebnisse des dreijährigen EU-Forschungsprojekt Web2Energy unter https://www.web2energy.com/de/

[251] EU-Richtlinie 2006/32/EG.

[252] Siehe hier das Papier „7 Eckpunkte für das ‚Verordnungspaket Intelligente Netze‘“, online unter http://www.bmwi.de/BMWi/Redaktion/PDF/E/eckpunkte-fuer-das-verordnungspaket-intelligente-netze Damit wird eine frühere Vorschrift aufgeweicht, nach der seit dem 1.1.2010 in Deutschland durch das Energiewirtschaftsgesetz der Einbau von Smart Metern für Gebäude vorgeschrieben war, die neu an das Energieversorgungsnetz angeschlossen oder größeren Renovierungen unterzogen werden (siehe http://www.gesetze-im-internet.de/bundesrecht/enwg_2005/gesamt.pdf).

Die technischen Möglichkeiten von Smart-Metern umfassen:

- Sekundengenaue Messung des Stromverbrauchs
- Erstellen von Lastprofilen
- Übertragung der Verbrauchsdaten in engen Zeitintervallen (oft 15-minütig)
- Kontaktloses Auslesen über Funkverbindung, Mobilfunk oder Internet
- Zugang zu den Verbrauchsdaten über Internetportale

Mit Smart Metern werden verschiedene Daten ausgetauscht. Darunter fallen Messwerte, Daten zur Abrechnung, aktuelle Verbrauchsdaten, Preisinformationen, Rechnungsdaten, Steuerungsdaten, Wartungsdaten, Statusdaten und weitere.[253]

Die zeitabhängige Messung und große Genauigkeit von Smart-Metern stellen jedoch auch Sicherheitsrisiken dar. Technisch ist es möglich, mehr Daten zu erheben und zu übermitteln, als der Kunde bemerkt und kontrollieren kann. Neben der Anfälligkeit solcher Systeme für Hacker[254] lassen Smart-Meter vor allem Rückschlüsse auf Nutzerdaten und Lebensgewohnheiten zu und bedrohen damit die Privatsphäre. Dabei sind Messdaten, Daten zur Abrechnung, aktuelle Verbrauchsdaten, Statusmeldungen und Rechnungsdaten personenbezogen oder personenbeziehbar und damit aus Sicht des Datenschutzes relevant. Insbesondere durch Messdaten können Lastprofile erstellt und damit detailliert die Lebensgewohnheiten des Verbrauchers erschlossen werden.[255] Die Einführung von Smart-Metern wurde vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein des Öfteren kritisiert.[256] Das BSI hat daher verschiedene Richtlinien für die Sicherheit von Smart-Metern ausgearbeitet, die für die in Deutschland verwendeten Smart-Meter bindend sind und in denen kryptographische Funktionen und Anforderungen für Smart Meter standardisiert werden.[257] Trotz dieser Maßnahmen bieten Smart Meter jedoch nur unzureichenden Schutz vor lokalen Angriffen.[258]

5.1.3. Vernetzte Spielekonsolen

Spielekonsolen wie die Xbox (Microsoft), Wii (Nintendo) oder die PlayStation (Sony) haben für die Wiedergabe von Videospielen ein festes Marktsegment, eignen sich jedoch auch zunehmend als Allround-Multimedia-Geräte. Durch moderne Spielekonsolen wird die Nutzung verschiedener Medien zentralisiert (Fernseher, BluRay-Player, Musikanlage, Internet, Spielekonsole, etc.). Dies ist sowohl auf die stetig steigende technische Leistungsfähigkeit als auch den wachsenden Funktionsumfang zurückzuführen. Die Ausstattung mit zusätzlichen Sensoren wie Kamera, Mikrofon oder Bewegungssensor ermöglicht

[253] Eckert & Krauß 2012.
[254] Knoke 2010; Lemos 2010.
[255] Vgl. Costache 2011.
[256] Siehe https://www.datenschutzzentrum.de/smartmeter/20110615-pm-smartmeterregelung.htm.
[257] Siehe hier BSI 2013b; BSI 2014b.
[258] Stumpf 2012a; Stumpf 2012b. Prototypen von Smart-Meter-Gateways, die die Richtlinien des BSI erfüllen, jedoch darüber hinausgehen, werden in Stumpf 2012b und Urban et.al. 2014 vorgestellt.

ein komplexeres Spieleerlebnis, indem die Konsole auf Sprachbefehle oder Bewegungen des Nutzers reagieren kann. Die Netzwerkanbindung ermöglicht zusätzlich das Herunterladen von Filmen, Spielen, Musik oder Bildern sowie die Synchronisation von Spielständen durch Online-Accounts des Nutzers. Die technischen Möglichkeiten von Spielekonsolen sind durch die ausgeprägte Sensorik jedoch auch ein potentielles Risiko für die Privatsphäre des Nutzers. Der technische Funktionsumfang einer modernen Spielekonsole (insbesondere Xbox ONE) umfasst:[259]

- Erkennung des Nutzers durch HD-3D-Kamera mit Infrarot (hochauflösende 3D-Aufnahme bei Licht und Dunkelheit) und Gesichtserkennung
- Analyse von Gesichtsausdrücken
- Zuordnung von Person und Stimme über Mikrofon und Kamera
- Analyse von Bewegungen des Nutzers durch Kameraauswertung
- Erkennung von Anzahl der Nutzer vor der Konsole
- Aufzeichnung aller Geräusche durch Mikrofon, auch im Standby
- Messung und Speicherung von nutzerspezifischen Reaktionszeiten
- Analyse von Stimmungen des Nutzers
- Nutzerspezifische Aufzeichnung von Art der Nutzung (z. B. Spiel, Internetseite), Zeit und Dauer der Nutzung
- Sammlung von Daten zu allen Bereichen der Nutzung: Filme, Internet, Spiele, Musik, Bilder, etc.
- Übermittlung aller gespeicherten Daten und Informationen über das Internet
- Regelmäßige Übertragung von Daten durch Internetzwang in Intervallen (alle 24h) und Cloud-Speicher
- Steuerung von anderen Wohnzimmergeräten über Infrarot.

Aufgrund dieser technischen Ausstattung und der zunehmenden Verwendung von Spielekonsolen als Multimediageräte im Zentrum der Wohnung ergeben sich zahlreiche Risiken für den Datenschutz des Nutzers. Spielekonsolen wurden daher aus Sicht des Datenschutzes vom Bundesdatenschutzbeauftragte Peter Schaar kritisiert.[260] Aus Sicht des Datenschutzes potenzieren sich durch den großen Funktionsumfang als Multimediagerät die Gefahren: Die unterschiedlichen Medien sind bereits vernetzt und an einer einzigen Stelle zentralisiert. Durch die häufig zentrale Platzierung der Konsole in der Wohnung ist damit gleichzeitig der Zugriff auf den Bereich des privaten Lebens gegeben, an dem sich der größte Teil des häuslichen Lebens abspielt. Ein Missbrauch der technischen Möglichkeiten kann auf verschiedene Weise geschehen:[261]

[259] Vgl. hier vor allem Korte 2013 und http://www.gamestar.de/hardware/konsolen/microsoft-xbox-one/news-artikel/xbox_one,483,3012491,3.html.
[260] Siehe http://www.spiegel.de/netzwelt/games/ueberwachung-datenschuetzer-peter-schaar-kritisiert-microsofts-xbox-one-a-901893.html.
[261] Siehe hier Korte 2013 und Bundesregierung 2013.

1. *Datensammlung (trotz korrekter Funktionalität aller Komponenten) durch den Konsolenbetreiber:* Auch ohne Manipulation der Konsole können durch die Vernetzung der Konsole umfangreiche Daten übermittelt werden, ohne dass dies dem Nutzer bewusst ist. Dazu gehören in erster Linie Nutzungsstatistiken, die Auskunft darüber geben, welcher Nutzer welche Inhalte (Spiele, Musik, Videos, etc.) wann und wie häufig nutzt. Durch die Kamera ist die automatisierte Unterscheidung unterschiedlicher Nutzer möglich. Ferner ist die Konsole technisch in der Lage, aus einer Personengruppe einzelne Benutzer an Stimme oder Gesichtsmerkmalen wiederzuerkennen und damit umfangreiche und detaillierte Benutzerprofile zu generieren. Durch die HD-3D-Kamera mit Infrarot funktioniert dies für den gesamten einsehbaren Raum und auch bei Dunkelheit.
2. *Fehlende Möglichkeit zum Abschalten der Funktionen der Datenaufzeichnung, -sammlung und -übermittlung:* Die vom Betreiber vorgesehenen Funktionen müssen trotz der korrekten Funktionalität für den Nutzer nicht transparent sein. Es sind verschiedene Grade in der Aktivität der Steuerung durch den Nutzer denkbar:
    - Der Nutzer verfügt nicht über das technische Verständnis, das Potential der technischen Möglichkeiten zur Datensammlung zu beurteilen oder macht sich keine Gedanken über die datenschutzrechtlichen Konsequenzen der verbauten Technologien. In diesem Fall werden alle standardmäßig aktivierten Funktionen genutzt und können vom Betreiber zur Datensammlung genutzt werden.
    - Der Nutzer möchte die Datensammlung minimieren, doch die Funktionalität der Konsole lässt dies nur unzureichend zu. In diesem Fall wären die aktivierten technischen Möglichkeiten zur Datensammlung (Kamera, Mikrofon, Nutzungsprotokolle) und Übermittlung (Internetverbindung) nicht durch den Nutzer abstellbar. Ein Eingriff in die Privatsphäre könnte nicht unterbunden werden.
    - Der Nutzer möchte die möchte die Datensammlung minimieren, doch die Funktionalität der Konsole zum Deaktivieren ist nicht transparent, die Einstellung mit großen Hürden oder gar dem Wegfall von wesentlichen Funktionen verbunden.
3. *Fremdzugriff und -steuerung durch Malware:* Der Zugriff durch Malware ist auch bei Spielekonsolen gegeben und kann die Aktivierung von Sensoren (Kamera, Mikrofon) – sogar im Standby – die Aufzeichnung und Übermittlung von Daten an unbefugte Dritte zur Folge haben.

Die mangelnde Transparenz darüber, welche Sensoren zu welcher Zeit Daten aufnehmen und über das Internet übermitteln, macht es für Nutzer schwer, sich vor der Ausspähung der Privatsphäre zu schützen. Ferner sind in der Menüführung der Konsole keine feingranularen Einstellmöglichkeiten für Sensoren oder Datenübermittlung vorhanden, so dass beim Kauf der Konsole das volle Risiko des Datenmissbrauchs in Kauf genommen werden muss.

5.1.4. E-Book-Lesegeräte

Nach einer von BITKOM 2013 durchgeführten Studie[262] steigt die Nutzung von E-Books stark an. Mehr als ein Fünftel (21%) der Deutschen liest E-Books, das entspricht einem Anteil von 29% bei denjenigen, die überhaupt regelmäßig Bücher lesen. Obwohl auch der Absatz von E-Book-Readern in den letzten Jahren stetig gestiegen ist (2013 wurden über 800.000 Geräte in Deutschland verkauft), liest derzeit nicht einmal jeder Fünfte (18%) Leser von E-Books auf einem E-Book-Reader. Die meisten verwenden mehrere Geräte zum Lesen parallel, v.a. den Computer (77%), Smartphones (58%) oder Tablet-Computer (18%). Nach den Prognosen von BITKOM wird der Tablet-Computer das Mediengerät Nr. 1 für E-Books werden.[263]

Unabhängig von der Art des Lesegerätes, bildet das Digitale Lesen für Hersteller von Lesegeräten oder Lese-Apps eine im Vergleich zum herkömmlichen Papierbuch ungeahnte Fülle von Möglichkeiten, spezifische Nutzerdaten zu erheben.[264] Darüber kann ermittelt werden, welche Bücher oder Buchteile bei Lesern gut ankommen, und welche Seiten überblättert werden. Das liefert den Verlagen wertvolle Hinweise, die zur Verbesserung des Angebotes genutzt werden können. Die Erhebung von Daten hat jedoch offensichtlich auch ein großes Potential, die Privatsphäre des Nutzers zu gefährden.

5.2. Schwerpunkt: Daten von Smart-TVs

In diesem Abschnitt[265] wird zunächst eine Analyse des gegenwärtigen technischen Forschungsstands und der Verwendung von Smart-TVs gegeben und die dabei beteiligten Akteure (Nutzer, Gerätehersteller, Fernsehsender, etc.) erläutert. Anschließend folgt eine Beschreibung des mit Smart-TVs verbundenen Bedrohungspotentials und möglicher Schutzmaßnahmen.

5.2.1. Zustandsanalyse

Als *Smart-TV* werden Fernsehgeräte bezeichnet, die über zusätzliche Funktionen und Schnittstellen wie Internetanschluss, USB, Speicherkarten und Netzwerkanschluss verfügen. Neben der einfachen Fernseh-Funktion werden durch die Funktion *Hybrid Broadcast Broadband TV* (HbbTV)[266] Medieninhalte zur laufenden Sendung oder damit verbundene

---

[262] Siehe http://www.bitkom.org/de/markt_statistik/64018_77541.aspx.
[263] Siehe http://www.bitkom.org/files/documents/BITKOM_PK_Charts_E-Books_Studie_01_10_2013_final.pdf. Vgl. dazu den steigenden Absatz von Tablet-Computern: http://www.smart-digits.com/2013/07/ereader-vs-tablet-auf-welche-gerate-sollten-verlage-setzen/.
[264] http://www.welt.de/wirtschaft/webwelt/article114505544/E-Book-Reader-senden-Nutzerdaten-in-die-Zentrale.html
[265] Die Forschungsergebnisse von Pro Privacy zu Smart TVs wurden bereits in einem Buchbeitrag (Ghiglieri, Lange, Simo & Waidner 2015) veröffentlicht. Dieser Abschnitt basiert daher maßgeblich auf den Inhalten des Buchbeitrages.
[266] Siehe hierzu ausführlich unten.

Inhalte aus einer Mediathek zur Verfügung gestellt. Ein Smart-TV ist ein Multimedia-Center, das auch verwendet werden kann, um im Internet zu surfen, Bilder anzuschauen, Musik zu hören oder Video-Telefonie zu betreiben.[267] Durch die Netzwerkanbindung können Smart-TVs häufig über Smartphones oder Tablets gesteuert werden. In Deutschland wird bis 2016 die Anzahl aktiv vernetzter TV-Geräte auf voraussichtlich 20 Millionen Geräte ansteigen,[268] jeder dritte Haushalt wird ein HbbTV-fähiges TV-Gerät besitzen.[269] Ein ähnlich deutlicher Trend ist in den USA zu beobachten.[270] Grund für die starke Verbreitung von Smart-TVs ist der gegenüber herkömmlichen Geräten wesentlich gesteigerte Funktionsumfang sowie die Tatsache, dass im Verkauf herkömmliche Fernseher bereits vollständig durch Smart-TVs ersetzt wurden. Die wesentlichen Ausstattungs- und Funktionsmerkmale werden im Folgenden genannt.

Umfangreiche Sensoren

Ähnlich wie mobile Endgeräte sind Smart-TVs vernetzte Plattformen, die mit leistungsstarken Prozessoren sowie unterschiedlichen und z. T. eingebauten Steuerungs- und Bewegungssensoren bestückt sind. Moderne Smart-TVs werden mit einer Vielzahl von Sensoren ausgestattet. Dazu gehören neben Mikrofon und Kamera zur Stimm- und Gesichtserkennung[271] auch Bewegungs-, Temperatur- und Luftfeuchtigkeitssensoren. Diese stellen Rückkanäle zur Verfügung, die dem Nutzer die Interaktion und Partizipation am TV-Programm bzw. die Nutzung von Web-Anwendungen wie Voice-Chat-Diensten oder soziale Netzwerken ermöglichen. Ähnlich wie bei Spielekonsolen ermöglichen die Sensoren einen erweiterten Funktionsumfang wie Video-Chat, Nutzung von Spielen oder die Verwendung von Sprachsteuerung.[272]

Integration von Web-Technologien

Anders als bei konventionellen TV-Geräten können moderne Fernsehgeräte direkt mit dem Internet über LAN oder WLAN verbunden werden, ohne die Notwendigkeit eines Anschlusses an einen externen Rechner oder einer Set-Top Box. Neben wirtschaftlichen Vorteilen und aufgrund neuer interaktiver TV-Geschäftsmodelle für Gerätehersteller, TV-Sender, Content-Anbieter, Infrastrukturbetreiber und Werbetreibende, zielt eine derartige Konvergenz zwischen Internet und TV auf hohen Nutzerkomfort und einfache Bedienbarkeit.

Die Integration von Web Technologien in das Fernsehen ermöglicht einen Zugriff auf Inhalte des World Wide Web, typischerweise sowohl durch einen (zum Teil rudimentären) Web-Browser als auch durch unterschiedliche Kommunikationsdienste wie etwa Musik-

---

[267] Statista 2010 („Wie wird sich der Markt für Smart Home bis 2020 entwickeln?“).
[268] Statista 2011a; Sattler 2011; Goldmedia 2012; Birkel 2013. Vgl. zum steigenden Umsatz des Smart-TV-Marktes in Deutschland auch Pwc 2013.
[269] Goldhammer, Wiegand & Birkel 2012.
[270] Sattler 2011; Statista 2011b; vgl. auch eMarketer 2014 und https://www.strategyanalytics.com/default.aspx?mod=pressreleaseviewer&a0=5472.
[271] Vgl. Lendino 2014.
[272] http://www.spiegel.de/netzwelt/gadgets/samsung-warnt-vor-eigenen-smart-tv-geraeten-a-1017447.html.

Player, E-Mail, Spiele, Social Media, VoIP und Bezahlungsdienste oder Online-Banking. Web-Browser und Kommunikationsdienste werden dem Nutzer in Form von Apps zur Verfügung gestellt. Die Verbindungen zum Internet werden bei derzeitigen Geräten häufig mittels SSL verschlüsselt, allerdings weisen die dabei verwendeten Verfahren und Zertifikate häufig große Schwächen auf.[273]

Erweiterter Funktionsumfang

Durch die Integration von Sensoren und Web-Technologien vereinen SmartTVs im Gegensatz zu herkömmlichen Fernsehern eine große Anzahl an Funktionen. Dies umfasst:[274]

- Herkömmliches Programmfernsehen
- HbbTV: Darstellung von TV- und Internet-Inhalten
- Video on Demand: Zugriff auf kostenpflichtige Internet-Videotheken (z. B. iTunes, Maxdome)
- Mediathek: Nutzen von durch Sender bereitgestellte Mediatheken (ARD-/ ZDF-Mediathek) oder von Videos im Internet (Youtube)
- Zugriff auf private Daten wie Bilder, Musik, Filme
- Info-Apps, z. B. zu News, Wetter
- Kommunikation über Facebook, Twitter, Skype
- Internetzugriff: Surfen im Netz, E-Mail-Abruf, Shopping
- Spielekonsole: Spielen von Games

Moderne Smart-TVs gelten dementsprechend zunehmend als Multimedia-Center, die externe Kommunikations- und Fernsehdienste mit anderen Multimedia-Anwendungen verbinden können. Durch die Integration von Web-Inhalten und durch die Möglichkeit, verschiedene Apps zu installieren, ist der Funktionsumfang ständig erweiterbar. Ähnlich wie auf Smartphones, bieten Apps die Möglichkeit zur Erweiterung der Funktionalität eines Smart-TV Gerätes. Smart-TV Apps sind überwiegend bereits vorinstalliert, können aber auch von Online-App-Stores heruntergeladen, oder von externen Speichermedien installiert werden. Die meisten Fernsehgerätehersteller betreiben einen eigenen App-Store und bieten i.d.R. Apps für iOS oder Android- Geräte an. Dies ermöglicht u. a. eine Echtzeit Synchronisierung zwischen den Smart-TVs und einer mobilen App auf dem Smartphone oder Tablet des Zuschauers. Das Konzept ist unter dem Begriff „Second-Screen Ansatz“ bekannt und gilt als wichtiges Instrument, um eine erweiterte Nutzung von neuen Diensten und zusätzlichen senderbezogenen Multimedia-Inhalten zu realisieren. [275]

[273] Ghiglieri 2014; Eikenberg 2014; vgl. ferner https://blog.kaspersky.de/shopping-und-online-banking-mit-dem-smart-tv-ist-nicht-sicher/2412/.
[274] PwC 2013.
[275] Kuri 2014.

Unterstützung des HbbTV-Standard

Die Verknüpfung von Rundfunk mit interaktiven Online-Diensten auf Smart-TV-Geräten ist mit gängigen Web-Technologien möglich. Prominentes Beispiel ist der offene internationale Standard HbbTV.[276] HbbTV ist ursprünglich eine pan-europäische Initiative zur Harmonisierung der Rundfunk- und Breitband Bereitstellung von Multimediainhalten durch Internet-fähige Fernseher. Die HbbTV-Spezifikation[277] basiert auf Erweiterung bestehender Web-Technologien und Standards wie JavaScript, HTML und CSS. Mittlerweile wird der HbbTV-Standard über Europa hinaus als ernsthafte Alternative bzw. Ergänzung bestehender Rundfunkstandards betrachtet.[278] Der HbbTV-Standard eröffnet die Möglichkeit, dem Zuschauer neben herkömmlichem Programmfernsehen sowohl Web-basierte Medienangebote (z. B. Werbung, Wetterberichte oder Teletext) zum laufenden und zukünftigen Programm als auch On-Demand Dienste zur Verfügung zu stellen. Damit ergibt sich jedoch auch das Risiko, dass genutzte HbbTV-Inhalte jederzeit vom Inhaltsanbieter nachverfolgt werden können. HbbTV ist wie die Nutzung von Apps oder Multimediainhalten im Second-Screen-Modus oder durch Einblendung von Inhalten in das Fernsehbild möglich.[279] HbbTV-Dienste werden i.d.R. über die Rote Taste auf der Fernbedienung aufgerufen und daher oft als „Red-Button"-Dienste bezeichnet. Anbieter von HbbTV-Diensten bzw. der über HbbTV angebotenen Inhalte sind die jeweiligen Programmveranstalter. Für Werbetreibende und TV-Sender bestehen die Vorteile des „Red-Button" mit HbbTV in erster Linie in der Möglichkeit, neue interaktive TV-Geschäftsmodelle zu etablieren.[280] So haben die Eigenschaften von HbbTV das Potential, eine personalisierter Empfehlungen für Shows und Web-basierte Inhalte sowie die Realisierung des Nachfolgesystems des heutigen Teletexts zu ermöglichen.[281]

5.2.2. Beteiligte Akteure

Der Betrieb von Smart-TVs umfasst eine Vielzahl beteiligter Akteure und Parteien und ist damit aus Sicht des Daten- und Privatsphärenschutzes besonders komplex. Die beteiligten Akteure und Instanzen werden im Folgenden kurz beschrieben.

Smart-TV-Gerät

Smart-TVs stellen die Basis der Architektur dar. Heutige Smart-TVs bestehen aus einer Vielzahl von integrierten Sensoren, die im Zusammenspiel mit einer proprietären Firmware (bzw. einem Betriebssystem) sowohl interaktives Fernsehen als auch verschiedene Funktionalitäten realisiert, u. a. Sprachsteuerung und Gestensteuerung (s.o.). Smart-TVs werden i.d.R. von den Geräteherstellern, wie z. B. Samsung, Sony und LG kontrolliert. Sie

[276] Deutsche TV Plattform 2014. Auf Smart-TV-Geräten können HbbTV-Services von Sendern per Knopfdruck aufgerufen werden.
[277] Deutsche TV Plattform 2014.
[278] Deutsche TV Plattform 2014.
[279] IRT GmbH 2014.
[280] BLM 2012.
[281] Siehe http://www.hbbtv-infos.de.

werden typischerweise in intimen Bereichen des Haushaltes wie etwa im Wohn- oder Schlafzimmer platziert.

TV-Sender

Die TV-Sender bieten Fernsehprogramme in Form von Sendungen sowie zusätzliche Online-Inhalte als Zusatzmaterial für einzelne Sendungen an. Sie sind für das HbbTV-Angebot verantwortlich.

Gerätehersteller/ Servicetechniker

Die Gerätehersteller arbeiten mit führenden Soft- bzw. Hardwareherstellern und Anbietern interaktiver Inhalte zusammen, um Fernsehgeräte anzubieten, die den besonderen Anforderungen der Smart-TV-Angebote genügen. Sie machen sich die Hard- und Firmware-Merkmale der Geräte sowie einen heute bundesweit relativ weit verbreiteten breitbandigen Internetzugang zu Nutze, um eine Fernwartung (incl. Aktualisierung/ Update der Firmware auf dem TV) durchzuführen. Ähnliche Wartungstätigkeiten werden bei Bedarf durch einen (Vertrags-) Servicetechniker erledigt, für den der Hersteller spezielle Schnittstellen und Wartungsoptionen auf dem Smart-TV vorgesehen hat. Die bei der (Fern-) Wartungsarbeit anfallenden Daten werden ggf. (vertraglich festgelegt) mit weiteren Hardwareherstellern und Inhaltsanbietern geteilt.

Inhaltsanbieter

Inhaltsanbieter stellen Apps mit moderierten und sonstigen Inhalten zur Verfügung. Sie tragen jeweils die redaktionelle und rechtliche Verantwortlichkeit für die Inhalte der Applikationen und Programme, die den Nutzer angeboten werden. Inhaltsanbieter können den Zugang zu interaktiven Online-Inhalte entweder durch einen Zugangsanbieter (wie z. B. Kabelnetzbetreiber oder Telekommunikationsunternehmen) ermöglichen, oder selbst die notwendige Zugangsinfrastruktur betreiben. TV-Sender, Gerätehersteller und Werbetreibende werden dementsprechend als Inhaltsanbieter betrachtet.

Kommunikationsnetze und Infrastrukturbetreiber

Kommunikationsnetze beziehen sich auf eine Vielzahl von öffentlichen und privaten Kommunikationsnetzen. Sie sind Voraussetzungen für den Informationsaustausch, sowohl zwischen den Smart-TVs und weiteren intelligenten elektronischen Geräten innerhalb von Heimnetzwerken als auch für die Kommunikation mit externen Parteien (u. a. Gerätehersteller, Infrastrukturbetreiber, Programmveranstaltern/ Fernsehanstalten, Werbetreibende). Infrastrukturbetreiber sind Betreiber von Kabelnetzen und Telekommunikationsunternehmen. Sie stellen oftmals gegen einen pauschalen monatlichen Tarif die technische Infrastruktur zur Verfügung, die notwendig ist, um Kommunikation zwischen sämtlichen Akteuren zu ermöglichen.

Nutzer

Die Gruppe der Nutzer umfasst sowohl Zuschauer als auch weitere Privatpersonen, die ein Smart-TV nutzen, um neben traditionellen Rundfunkdiensten auch zusätzliche über das Internet erreichbare interaktive Medieninhalte zu konsumieren. Einbezogen werden können auch juristische Personen, die ihre Räumlichkeiten mit Smart- TVs ausstatten, z. B. Arbeitgeber oder Gastronomie- und Veranstaltungsbetriebe (Hotels oder Cafés).

Werbetreibende

Smart-TVs und die damit verbundenen Second-Screen-Technologien ermöglichen Werbetreibenden, bestimmte Zuschauergruppen gezielt zu adressieren und mit ihnen über die Dauer des Spots hinaus zu interagieren. Aus Sicht von Werbetreibenden oder direkt angeschlossenen Dienste, wie etwa dem Online-Statistikdienst Google Analytics, birgt dieser Trend das Potenzial, die Interaktion der Zuschauer mit den Werbeinhalten besser zu erfassen und auszuwerten. Die dabei anfallenden Daten werden u. U. mit den Inhaltsanbietern bzw. den TV-Sendern geteilt.

Sonstige Akteure

Weitere Akteure werden einbezogen, um Geschäftsmodelle in HbbTV Anwendungen mit Online-Bezahlverfahren zu unterstützen bzw. kostenpflichtige Smart-TV-Inhalte anzubieten. Beispiele sind online Bezahldienste wie Paypal[282] und Kreditkartenunternehmen wie Visa.[283]

5.2.3. Angriffsmöglichkeiten

Durch die erweiterte Funktionalität von Smart-TVs und den unterschiedlichen bei der Bereitstellung und dem Betrieb von Smart-TV-Angeboten beteiligten Akteuren entstehen Risiken für die Privatsphäre der Nutzer. Insbesondere durch die Integration von Sensoren wie Kamera und Mikrofon sowie durch die Web-Anbindung steigt auch das Risiko für Schwachstellen in den verwendeten Apps und der Software für die Sensorsteuerung. Durch die Vielzahl der beteiligten Akteure multipliziert sich die Anzahl der potentiellen Bedrohung für die Privatsphäre des Nutzers. Bei der Analyse des Bedrohungspotentials des Nutzers lassen sich die folgenden Angriffsmöglichkeiten unterscheiden:

Bedrohung durch Sender

Smart-TV-Geräte verbinden sich zu den Sendern des jeweils auf dem Gerät laufenden Programmes, sofern diese eine HbbTV-Anwendungen bereitstellen. Mindestens beim Einschalten des Senders wird vom Gerät eine Anfrage an einen Server des Senders gestellt, um den sog. „Red Button“, der die Verfügbarkeit von weiteren Onlineinhalten zum gewählten Programm anzeigt, auf dem Bildschirm einzublenden. Viele Sender belassen es jedoch nicht mit einer einmaligen Anfrage, sondern senden periodische Anfragen mit einem Zeitintervall zwischen einer Sekunde und mehreren Minuten.[284] Auf diese Weise ist der Sender in regelmäßigen Abständen (teilweise sekundengenau) darüber informiert, zu welcher Zeit der Nutzer den Sender eingeschaltet hat. Bei einigen Sendern werden über periodische Anfragen auf den Server des Senders zugleich Trackingskripte von Drittanbietern (z. B. Google Analytics, Chartbeat, Webtrekk) geladen (s.u.: Bedrohung durch Dritt-Dienstanbieter) oder Cookies gesetzt. Beides sind Maßnahmen, um das Nutzerverhalten zu tracken.[285] Die Ergebnisse des Trackings mit Google Analytics bekommt der

[282] Siehe www.paypal.com.
[283] Siehe www.visa.de.
[284] Siehe hier ausführlich: Ghiglieri, Oswald & Tews 2013a.
[285] Vgl. auch Ertel 2014; Schleipfer 2014.

Sender selbst nur in anonymisierter Form. So darf etwa die IP-Adresse nur in Teilen an den Sender übermittelt werden. Dagegen ermöglicht die Verwendung von Cookies dem Sender die Erfassung wesentlich detaillierterer Informationen zum Nutzerverhalten. Dem Setzen von Cookies kann in vielen Smart-TV-Geräten nicht widersprochen werden, ferner können sie oft gar nicht oder nur umständlich gelöscht werden.[286] Beides hat zur Folge, dass gesetzt Cookies für immer auf dem Gerät gespeichert bleiben und damit eine dauerhafte, eindeutige Nutzerkennung darstellen. Da Cookies von mehreren Sendern gesetzt werden, wird damit auch ein Sender-übergreifendes Tracking der Nutzer und die Erstellung von detaillierten Nutzerprofilen möglich. Dass die Sender tatsächlich derartige Nutzerprofile erstellen, zeigt die bei manchen Sendern in festen Zeitabständen eingeblendete personalisierte Werbung.[287]

Dieses Tracking des Nutzerverhaltens ist besonders problematisch, weil dies technisch sogar dann möglich ist, wenn der Nutzer keinen Red-Button gedrückt und damit nicht aktiv zusätzliche Funktionen ausgewählt hat. Auch dann wird durch eine Verbindung zum Sender die IP-Adresse des Nutzers übertragen, die eine grobe Lokalisierung des Nutzers erlaubt. Da IP-Adressen bei vielen Internetprovidern für 24 Stunden oder länger gleich bleiben, liefert die IP-Adresse damit zugleich die Möglichkeit, den Nutzer in diesem Zeitraum wiederzuerkennen. Durch das Setzen von dauerhaften Cookies ist dies sogar für einen viel längeren Zeitraum (u. U. über die gesamte Lebensdauer des Gerätes) möglich. Von alledem bekommt der Nutzer nichts mit. Besonders problematisch dabei ist, dass der Nutzer in den allermeisten Fällen auch keinen Grund hat, dagegen vorzugehen, weil er eine Übermittlung von Inhalten gar nicht erwartet. Viele Nutzer von Smart-TV-Geräten sind sich nicht einmal der Tatsache bewusst, dass ihr Gerät über eine Verbindung ins Internet verfügt.[288]

Bedrohung durch Smart-TV-Hersteller

Die Verbindung mit dem Internet bringt die Möglichkeit mit sich, dass Nutzerdaten über das Internet an den Hersteller des Gerätes übermittelt werden. Technisch beinhaltet das die folgenden Möglichkeiten, die teilweise bereits von Herstellern genutzt wurden:[289]

- Vollständige Protokollierung des Fernsehverhaltens inkl. Sender und Zeitstempel
- Vollständige Protokollierung des Surf-Verhaltens inkl. besuchter Seiten und Zeitstempel
- Protokollierung der eingelegten Medien (z. B. USB-Stick) und der wiedergebebenen Multimedia-Inhalte

[286] Ghiglieri, Oswald & Tews 2012.
[287] Ghiglieri, Oswald & Tews 2012.
[288] Nach Pwc 2013 wissen 22% der Smart-TV-Benutzer nicht, ob ihr Smart –TV mit dem Web verbunden ist; 10% der TV-Haushalte wissen nicht, ob ihr TV-Gerät ein Smart-TV ist.
[289] Vgl. zu den Ende 2013 von LG-Fernsehern versendeten Daten: http://www.zeit.de/digital/datenschutz/2013-11/lg-smart-tv-daten-panne. Vgl. ferner Raiko 2014; Bager & Zivadinovic 2014 und http://meedia.de/2015/03/04/smart-tvs-daten-werden-staendig-ungefragt-uebertragen/.

Die Protokollierung des Nutzerverhaltens wird zum Teil zur personalisierten Werbung verwendet. Dass Smart-TVs Daten übermitteln, lässt sich für die Nutzer kaum verhindern, ohne Einschränkungen im Funktionsumfang in Kauf nehmen zu müssen.[290]

Bedrohung durch Dritt-Dienstanbieter

Durch Einbindung eines Dritt-Dienstanbieters, der die Auswertung der Nutzerstatistiken vornimmt, bekommt dieser Zugriff auf die vollen IP-Adressen der Nutzer und kann die Daten für mehrere Sender zusammenführen und damit umfassende Nutzerprofile erstellen (s.u.). Apps haben i.d.R. umfassenden Zugriff auf unterschiedliche Geräte- bzw. nutzerspezifische Daten. Nutzer haben oft nur ein begrenztes Bewusstsein darüber, welche Daten bei der Nutzung einer App anfallen, auf welche Daten verschiedene Apps zugreifen und für welchen Zweck sie benötigt werden. Die Apps werden verwendet, um auf eine Vielzahl von externen (Multimedia-)Inhalten zuzugreifen. Dabei setzen sie das Fernsehgerät zusätzlichen Risiken aus. Forscher der koreanischen Forschungseinrichtung „GrayHash – Offensive Security Research Center" zeigten 2013, wie die fehlende Transparenz über die Erhebung und Verarbeitung sensibler Daten durch Apps vom Angreifer ausgenutzt werden kann, um Schadsoftware in Fernsehgeräte einzuschleusen.[291] Unabsichtlich installierte oder mitgelieferte datenschutzunfreundliche Smart-TV Apps können so vom Angreifer benutzt werden, um auf im Smart-TV anfallende sensible Daten zuzugreifen.

Eine andere Bedrohung durch Drittanbieter entsteht, wenn über den in Smart-TVs integrierten Browser auf das Internet zugegriffen wird. Smart-TVs verwenden einen Internetbrowser, der im Umfang jedoch sparsamer ausgestattet ist, als ein normaler Internetbrowser. Dementsprechend lassen sich für Smart-TVs dieselben Trackingmethoden anwenden, die auch bei Browsern im Internet zum Einsatz kommen. Durch zwei Umstände wird das Bedrohungspotential bei Smart-TVs jedoch erheblich vergrößert: Zum einen verhindert der geringere Funktionsumfang der eingesetzten Browser Gegenmaßnahmen oder eine wirksame Nutzerkontrolle durch fehlende Einstellungen (z. B. über die Speicherung von Cookies). Zum anderen ist sich der Nutzer im Gegensatz zum herkömmlichen Browser nicht bewusst, wann er welche Internetseite besucht, weil die Verbindung vom TV-Gerät im Hintergrund und damit für den Nutzer unzugänglich aufgebaut wird. Der Nutzer surft damit auf einer Reihe von Internetseiten – jedoch ohne davon zu wissen. Problematisch ist, dass die Möglichkeiten zur Abschaltung in der Menüführung häufig schwer zu finden ist.[292]

Bedrohung durch Beobachter

Eine weitere Bedrohung besteht in der Möglichkeit, aus den über drahtlose Netzwerke (WLAN) übermittelten Inhalten von Smart-TVs Rückschlüsse auf das Nutzungsverhalten zu ziehen. Ist ein Smart-TV über WLAN mit dem Internet verbunden und ein Angreifer in der Reichweite des WLANs, ist es möglich, zu jeder Zeit zu verfolgen, welches Programm

[290] Reiko 2014.
[291] Kim & Lee 2013.
[292] Vgl. hier etwa Kaps 2014.

auf dem Gerät läuft. Dies ist sogar dann der Fall, wenn für die Übertragung durch WLAN eine Verschlüsselung mit WPA2 nach aktuellen Sicherheitsanforderungen mit ausreichend langem Passwort verwendet wird.[293] Dies liegt daran, dass Sender unterschiedliche und jeweils charakteristische Paketgrößen für die übertragenen Daten verwenden. Durch einen Abgleich mit einem eigenen Smart-TV kann ein Angreifer auf diese Weise sogar bei verschlüsselten Datenpaketen leicht Übereinstimmungen feststellen.[294]

Gelingt es einem passiven Angreifer, den Verkehr zwischen Smart-TV und externem Webserver (z. B. den des Geräteherstellers oder des Online Bezahldienstes) auszuspähen, kann dieser unbemerkt und unautorisiert Zugriff auf sensible Zuschauer- und Fernseherdaten erlangen. Ghiglieri und andere zeigten 2013, wie Dritte (z. B. ein Nachbar) Schwächen des HbbTV Protokolls ausnutzen können, um das Nutzungsverhalten der Zuschauer eines HbbTV tauglichen Fernsehers mit WLAN Nutzung ohne ihre Wissen oder das der TV-Sender aufzuzeichnen.[295] Zudem dokumentierten die Autoren wie HbbTV Features die Sendeanstalten befähigen, sensible Daten (z. B. das Nutzungsverhalten) über ihre Zuschauer detailliert zu erfassen. Dieselbe Schwachstelle könnte auch von aktiven Angreifern, z. B. (bösartigen) Infrastrukturbetreibern, ausgenutzt werden, um zusätzlich bestimmte Inhalte zu blockieren bzw. zu zensieren oder präparierte Datenpakete in Fernsehgeräte als Vorstufe eines großflächigen „Denial of Service“ Angriffs einzuschleusen.

Ein weiterer Angriff bezieht sich auf das Rundfunksignal, welches die URL für die HbbTV Anwendung beinhaltet. Durch Manipulation der HbbTV-URL im Rundfunksignal kann eine großflächige Manipulation von Inhalten auf HbbTV-fähigen Geräten stattfinden. Die Schutzmaßnahmen im Rundfunksignal sind äußerst niedrig. Eine Studie zeigte 2014 einen Angriff, mit dem bis zu 20.000 Haushalte mit einem niedrigen Kostenaufwand manipuliert werden könnten.[296]

Bedrohung durch Schad- und Spähsoftware

Browser in Smart-TVs und ihre Unterstützung von Web Technologien wie Cookies, Javascript oder HTML eröffnen Angreifern neue Wege, um unbemerkt den ungefähren Standort des Smart-TVs sowie Informationen zum Gerätetyp genauer und kontinuierlich zu erfassen. Ferner dienen sie Angreifern dazu, den Fernseher mit Schadsoftware zu infizieren sowie dazu, den Datenaustausch zwischen Browser und Webserver abzuhören, zu manipulieren oder zu unterbinden. Diese Gefahr wird dadurch verschärft, dass die implementierte Sicherheitsfunktionen häufig unzureichend sind und zusätzliche Sicherheitsmängel im Smart-TV Browser (z. B. durch inkorrekte Überprüfung der digitalen Zertifikate bei der Unterstützung des HTTPS-Standards[297]) Einfalltor für Spähsoftware und andere bösartige Inhalte wie Phishing-Websites sein können.[298] Ein HbbTV-Browser ist gewöhnlich nicht sichtbar und vom Smart-TV Browser auf dem Fernsehgerät getrennt. Es

[293] Ghiglieri, Oswald & Tews 2013a.
[294] Ghiglieri, Oswald & Tews 2013a.
[295] Ghiglieri, Oswald & Tews 2013a; Ghiglieri, Oswald & Tews 2013b.
[296] Oren & Keromytis 2014.
[297] Siehe Ghlieri 2014.
[298] Ghiglieri & Tews 2014.

gelten allerdings die gleichen Gefahren, wie auch für einen Smart-TV Browser. Der Unterschied besteht darin, dass der Nutzer den HbbTV-Browser häufig nicht vom eigentlichen TV-Programm unterscheiden kann, da er bei eingeschalteter HbbTV-Funktionalität transparent auf dem übertragenen TV Programm liegt. Bei vielen Smart-TV-Geräten ist die HbbTV Funktionalität standardmäßig aktiviert. Nutzer wissen so nicht, ob ein bestimmtes Element auf dem angezeigten Bildschirm tatsächlich aus dem Internet oder über das Rundfunksignal kommt.

Spähsoftware und andere Schädlinge können zusätzlich als Multimediainhalte eingeschleust werden und unentdeckt bleiben.[299] Dabei machen sich die Angreifer die Schwächen der auf fast allen Smart- TV Modellen integrierten Media-Player zu Nutze. Der Player und die damit verbundenen Codecs ermöglichen das Öffnen und Ausführen von unterschiedlichen Dateitypen inklusive Videos und Bildern. Diese Dateien werden typischerweise entweder von einem Datenträger (USB-Stick, Speicherkarte) oder von einem externen Server auf den Smart-TV gespielt. Sie sind potentiell Träger von Trojanern und ermöglichen dem Angreifer

i) unbemerkt die Kontrolle über kritische Hardware-Module wie Kameras und Mikrofon zu erlangen,[300]
ii) auf sensitive Daten (z. B. Kontakte, Passwörter, Kreditkartenummern, Standort des Gerätes, etc.) zuzugreifen, oder
iii) das Gerät zum Absturz zu bringen.[301]

Ähnlich können Angreifer (bzw. datenhungrige Geräthersteller, TV-Sender oder Servicetechniker) Schwachstellen im Design der Fernwartungsstrategie für Smart-TVs ausnutzen, um Nutzer dazu zu bewegen, präparierte Firmware-Updates mit integrierter Spähsoftware auf dem Fernseher zur Ausführung zu bringen. Es ist daher wichtig, dass Sicherheitsaktualisierungen in allen Teilsystemen auf dem Smart-TV schnell und zügig auch beim Nutzer ankommen. Veraltete System erhöhen das Risiko signifikant.

Angreifer können Kenntnis über die Architektur der eingebauten Hardware bzw. Sensoren und über das Zusammenspiel zwischen diesen und weiterer Software auf dem Smart-TV erlangen. Sie können dieses Wissen nutzen, um das System zu kompromittieren. Eine vielbeachtete Untersuchung unterschiedlicher Smart-TV-Modelle der Firma Samsung hat 2013 gezeigt, wie vorinstallierte Web-Anwendungen wie Skype oder Facebook von Angreifern manipuliert werden können, um Zuschauer (bzw. deren Wohnzimmer oder Schlafzimmer) aus der Ferne über in Smart-TVs eingebaute Kameras und Mikrofone auszuspionieren.[302] Dabei ist das Fernsehgerät nicht mehr in der Lage, den üblichen Hinweis (je nach Ausstattung rotes bzw. grünes Licht oder keine Information an den Nutzer) über den Status der Kamera bzw. des Mikrofons zu geben. Somit ist der Betrieb von Webcam und Mikrofon durch den Nutzer nicht mehr kontrollierbar.

[299] Michéle & Karpow 2014.
[300] Schmundt 2014.
[301] Siehe http://aluigi.altervista.org/adv/samsux_1-adv.txt.
[302] Grattafiori & Yavor 2013.

5.2.4. Konsequenzen für die Nutzer

Die finanziellen oder politischen Anreize, Smart-TV-Daten systematisch zu erfassen und auszuwerten, beinhalten vor allem in der kommenden „Big Data"-Ära schwerwiegende Folgen für die Privatsphäre des Nutzers. Implikationen für die Privatsphäre ergeben sich in folgender Hinsicht:

Tracking und Profilbildung

Smart-TV-Geräte verbinden sich zu den Servern der Sender des jeweils auf dem Gerät laufenden Programmes, sofern diese eine HbbTV-Anwendung bereitstellen. Mindestens beim Einschalten[303] des Senders, häufig jedoch in regelmäßigen Abständen (teilweise sekundengenau) wird vom Gerät eine Anfrage an einen Server des Sendes gestellt, um den sog. „Red Button", der die Verfügbarkeit von weiteren Onlineinhalten zum gewählten Programm anzeigt, auf dem Bildschirm einzublenden.[304] Auf diese Weise ist der Sender in regelmäßigen Abständen darüber informiert, zu welcher Zeit der Nutzer einen Sender eingeschaltet hat. Auf diese Weise können detaillierte Nutzerprofile erstellt werden, aus denen sehr genau die Vorlieben und Abneigungen eines Nutzers herausgelesen werden können.

Massenüberwachung und gezielte Überwachung der Zuschauer

Aus Daten von kompromittierten Smart-TV-Sensoren (z. B. Video-, Bilder-, und Stimmaufnahmen) lassen sich ohne Wissen und Einverständnis der Nutzer Informationen über Aktivitäten und Verhaltensweisen der Nutzer sowie über die Ausstattung in sensiblen Bereichen des Haushalts ableiten.[305] Dies stellt nicht nur ein Sicherheitsrisiko dar, weil Einbrecher oder aufdringliche Dienstanbieter den Zuschauer On- und Offline (gezielt) überwachen können. Auch Regierungsorgane wie etwa Geheimdienste können die im Smart-TV-Ökosystem anfallenden Daten zweckentfremden, um Massenüberwachungsprogramme durchzuführen.

Intransparenz der Datenverarbeitung

Die von Smart–TVs erhobenen Daten über die Interaktion mit den Nutzern und weitere Komponenten in Privathaushalten sind personenbezogene Daten. Jedoch sind sich die Nutzer nicht immer bewusst, dass ihre Fernsehgeräte solche Daten häufig auch ohne konkreten Bedarf erfassen und weiterleiten. Besonders problematisch dabei ist, dass Nutzer in den allermeisten Fällen auch keinen Grund haben dagegen vorzugehen, weil eine Übermittlung von Inhalten gar nicht erwartet wird. Diese Problematik wird verschärft dadurch, dass viele Nutzer sich nicht über die Verbindung ihres Gerätes zum Internet bewusst sind.[306] Damit ermöglicht die Systemgestaltung heutiger Smart-TVs eine Erhebung

---

[303] Datenschutzfreundlichere Varianten von HbbTV ermöglichen das Laden der Inhalte über das Rundfunksignal. Dies lässt Nutzertracking und Profilbildung nicht zu.

[304] Yeong et.al. 2012.

[305] Siehe http://meedia.de/2015/03/04/smart-tvs-daten-werden-staendig-ungefragt-uebertragen/.

[306] Nach PwC 2013 wissen 22% der Smart-TV-Benutzer nicht, ob ihr Smart –TV mit dem Web verbunden ist; 10% der TV-Haushalte wissen nicht, ob ihr TV-Gerät ein Smart-TV ist.

und Verarbeitung dieser Daten ohne Mitwirkung der Betroffenen.[307] Nicht nur verlieren Nutzer so die Gerätehoheit über ihr TV-Gerät,[308] auch gefährdet die ungefragte Datenübermittlung an externe Akteure das Einhalten des Transparenzprinzips gegenüber den Nutzern.

Einschränkung der Entscheidungsautonomie

Die Nutzung heutiger Smart-TV-Dienste kann schwerwiegende Folgen für die individuelle Entscheidungsautonomie haben. Insbesondere gibt es Bedenken, dass aufgrund der Gestaltung der Plattform und Methoden zur Erhebung und Verarbeitung der Daten im Smart-TV-Ökosystem den Nutzern keine echten Entscheidungsoptionen gegeben werden. Dies lässt die Verbraucher mit einer nicht akzeptablen Wahl zurück, da ein Widerspruch der Datenerhebung meist mit einem völligen Verlust des Dienstes verbunden ist.[309] Alleine die Möglichkeit, Smart-TVs und die dabei anfallenden Daten zur gezielten Überwachung einzusetzen, kann die Entscheidungsautonomie der Endnutzer stark einschränken. Endnutzer können ihr Nutzungsverhalten als Reaktion auf ein Gefühl des Beobachtetwerdens zu ihren Ungunsten einschränken, oder gar auf die Nutzung eines Smart-TVs gänzlich verzichten.

Weitere Konsequenzen

Darunter fällt u. a. das Risiko einer Offenlegung vertraulicher Daten (z. B. Konto- und Registrierungsdaten des Zuschauers) als Folge von technischem oder menschlichem Versagen oder Cyber-Angriffen. Damit eng verbunden ist das Risiko für millionenfachen Identitätsdiebstahl mit potenziell schwerwiegenden Auswirkungen für die Nutzer, etwa in Form von materiellem oder finanziellem Schaden nach Identitätsmissbrauch.

5.2.5. Verfügbare Schutzmaßnahmen

In den vorherigen Abschnitten hat sich gezeigt, dass trotz einer starken Zunahme von internetfähigen modernen Fernsehgeräten nur unzureichende Sicherheitsmaßnahmen existieren, um die Geräte oder sensible Nutzerdaten zu schützen. Smart-TVs verfügen kaum über wirksame Schutzmaßnahmen. Dies ist umso gravierender, als Smart-TVs häufig nicht über Sicherheitsfeatures derselben Güte wie etwa Webbrowser oder Smartphones verfügen, gleichzeitig aber denselben und sogar umfassenderen Angriffsmöglichkeiten ausgesetzt sind. Aufgrund fehlender Schutzmaßnahmen ist die Mehrzahl der HbbTV-fähigen Fernseher der großen Anzahl an Angriffsmöglichkeiten und Bedrohungen für die Privatsphäre der Nutzer schutzlos ausgeliefert.

[307] DoctorBeet's Blog 2013.
[308] Albers 2013.
[309] Ghiglieri 2014.

5.2.6. Konzepte für neue Technologien

Schutzmöglichkeiten sind derzeit nicht ausreichend umgesetzt. Perspektivisch bestehen jedoch unterschiedliche Ansätze, um den Datenschutz und die Sicherheit von Smart-TVs zu erhöhen:[310]

Datensparsamkeit

Die Datensparsamkeit ist ein einfaches Mittel um Gefahren zu minimieren. Dabei beinhaltet Datensparsamkeit nicht nur, anfallende Daten zu minimieren, sondern die Aussagekraft von übermittelten Daten zu minimieren. Im Optimalfall werden nur die Daten übertragen, die für eine korrekte Funktionalität benötigt werden. Bei Smart-TVs trifft man allerdings auf einen Interessenskonflikt. Hersteller wollen möglichst genau erfahren, in welcher Umgebung ein Gerät eingesetzt wird. Diese Daten können unter anderem dafür genutzt werden, um möglichst effiziente und kostenoptimierte Hardware für bestimmte Anwendungsfälle zu produzieren. Durch die Erhöhung der Konnektivität wird es jedoch auch anderen Dienstanbietern möglich, Dienste auf die Smart-TV-Geräte zu bringen. Es werden Verfahren und Methoden benötigt, die die Interessen aller alle Akteure berücksichtigen. Eine solche Methode könnte in der Datenaggregation bestehen (s.u.).

Datenaggregation und Verschlüsselung

Eine einfache Aggregation in Form einer Datenanonymisierung und die anschließende Weiterleitung dieser Daten an Dienste könnte sowohl die Privatsphäre der Nutzer wie auch die Nutzbarkeit dieser Daten durch Werbetreibende und Gerätehersteller gewährleisten. Bei besonders sensiblen Daten könnte man kryptographische Verfahren wie etwa Techniken der homomorphen Verschlüsselung nutzen. Die Aggregation von Daten könnte dann beispielsweise mit der Gewissheit durchgeführt werden, dass die Daten selbst für den verarbeitenden Anbieter nicht sichtbar sind, aber dennoch bestimmte Operationen ausführbar bleiben. Falls Datentransfer unerlässlich ist, sollte eine geeignete Form der Übertragung genutzt werden. Allgemein sollten für den Schutz der Nutzungsdaten Verfahren verwendet werden, die die Vertraulichkeit und Integrität der übertragenen Daten sicherstellen. Im Bereich des Internets haben sich HTTPS Verbindungen etabliert, um Daten auf dem Transportweg zu verschlüsseln und vor Veränderung zu schützen. Diese Techniken sollten auch bei Smart-TVs konsequenter und mit ausreichendem Sicherheitsniveau zum Einsatz kommen.

Nutzersensibilisierung

Die Sensibilisierung der Nutzer ist ein wichtiges Instrument, um Transparenz und Vertrauen in neue Techniken zu schaffen. Dies erscheint auf den ersten Blick einfach, dennoch ergeben sich einige technische Probleme, die gelöst werden müssen. Dies umfasst insbesondere die benutzergerechte Visualisierung und dementsprechende Deutung der Daten. Dabei ist zu beachten, dass die stetige Ersetzung von alten Fernsehgeräten mit neuen Smart-TV-Geräten den Nutzerkreis vergrößert. Es wird zu beobachten sein, dass auch we-

[310] Vgl. für einige der folgenden Vorschläge zu Smart-TV: Ghiglieri, Oswald & Tews 2013a.

niger-technikaffine Personen die Funktionen eines Smart-TVs nutzen, aber einen versteckten Datentransfer nicht erwarten. Solche Nutzer für die übertragenen Daten von Smart-TVs zu sensibilisieren, ist daher ein wichtiger Schritt.

Die Nutzersensibilisierung kann in Form von Visualisierungen der Datenströme erfolgen. Eine solche Visualisierung beginnt bei dem Sichtbarmachen von Datenströmen von Geräten zum Internet bis zur Kommunikation der Geräte untereinander. Häufig sind die Daten ohne Kenntnis über den Inhalt und die Bedeutung der Daten schlecht für Nutzer bewertbar. Die reine Kommunikation mit einer Fremdpartei kann zwar schon Indiz für eine unberechtigte Verbindungsaufnahme sein. In vielen Fällen jedoch ist es wünschenswert, den Grund und den Inhalt für eine Kommunikation mit in die Bewertung einfließen zu lassen.

Datenscanner

Die Deutung der anfallenden Daten stellt eine größere Herausforderung dar. Wie auch bei Virenscannern ist eine große Datenbank von Signaturen und Mustern notwendig, damit die Erkennung und Deutung bestimmter Übertragungsmuster erkennbar ist. Der Unterschied beider Datenbanken ist, dass Viren Schadprogramme sind, die für jeden ähnlich schädlich eingestuft wird. Bei Geräten, die Daten übermitteln, ist es nicht immer für jeden Nutzer klar, was gewünscht und ungewünscht ist. Das Etablieren einer solchen Datenbasis für Smart-TVs ist wünschenswert, aber bedarf weiterer Forschung. Das Erheben einer solchen Datenbasis birgt allerdings auch Gefahren für jeden einzelnen Nutzer oder Haushalt, da unter Umständen private Nutzungsgewohnheiten veröffentlicht werden könnten. Daher müssten Methoden und Verfahren evaluiert werden, wie die Generierung ohne Datenschutzprobleme vollzogen werden kann. Ein bestehendes Forschungsproblem ist das Verallgemeinern solcher Daten, so dass der erzeugende Haushalt keine Informationen zu Nutzungsgewohnheiten preisgibt. Die heutigen Filterungs- und Blockierungsmaßnahmen sind häufig nur technisch auf der Netzwerkebene realisiert. Bei zunehmender Funktionalität von Geräten ist es jedoch erwünscht, inhaltsbasierte Filterung anzuwenden. So könnten zum Beispiel HbbTV Anwendungen von öffentlich rechtlichen Sendern übertragen werden und eine Blockierung von HbbTV auf Privatsendern könnte durchgeführt werden. Der einfachste Fall ist die Blockierung von ganzen Geräten, so dass diese beispielsweise keine Verbindung ins Internet aufbauen dürfen. Denkbar ist auch die Blockierung verschiedener Dienste auf dem Fernsehgerät.

Benutzerfreundlichkeit

Eine aktive Steuermöglichkeit würde nach Deutung der Daten dem Nutzer die Möglichkeit bieten, den unerwünschten Datenstrom zu unterbinden. Im Wesentlichen lassen sich als Maßnahmen die Filterung und Blockierung von Datenverbindungen nennen. Ein entscheidender Punkt für die Realisierung einer solchen Methode spielt die Benutzerfreundlichkeit. Nur wenn eine Sicherheitsmaßnahme ohne Einschränkung der Nutzer möglich ist, wird sie sich dauerhaft durchsetzen können. Als positives Beispiel kann auf HTTPS verwiesen werden: HTTPS ist für jeden Benutzer nutzbar, ohne dass sich etwas an der Benutzbarkeit verändert. Als negatives Beispiel kann man heutige Firewalls anführen: In heutigen Heimroutern sind zwar Firewall-Werkzeuge integriert, dennoch haben Nutzer häufig nicht die richtigen Kenntnisse, um die korrekte Steuerung zu beherrschen. Auch

die Aktualisierungsmöglichkeit der Smart-TV-Geräte muss benutzbar sein. Ein Konsument wird im Regelfall nicht auf die Herstellerwebseite gehen um dort eine Aktualisierung der Software auf einem Fernsehgerät durchzuführen. Hier ist die Beachtung bereits etablierter Methoden notwendig.

Sicherheitsupdates

Regelmäßige Aktualisierung der Software auf den Geräten ist wichtig, da sie ähnlich leistungsfähig sind wie Computersysteme. Durch die Erhöhung der Konnektivität ist die Wahrscheinlichkeit für das Auffinden von Sicherheitslücken in Smart-TVs gegenüber Computern deutlich größer. Aus diesem Grund müssen Aktualisierungen vom Hersteller durchgeführt und auf alle Smart-TV Geräte gebracht werden. Anders als bei Computersystemen ist die übliche Lebenszeit von Smart-TV Geräten noch nicht bekannt. Geht man aber von ähnlichen Lebenszeiten wie von konventionellen Fernsehgeräten bekannt aus, müssen Aktualisierungen über mehrere Jahre bereitgestellt werden. Bei einigen Smartphone Herstellern liegt derzeit die Aktualisierungszeit bei 18 Monaten, was bei Fernsehgeräten deutlich zu niedrig wäre. In mehreren Fällen sind durch veraltete Software oder Fehler in der Software Sicherheits- und Datenschutzprobleme aufgetreten.[311] Diese können nur wirkungsvoll behoben werden, wenn die Aktualisierung der Fernsehgeräte schnell, sicher und ohne schwierige Handlungen der Nutzer durchgeführt werden können. Heutige Smart-TV-Geräte erfordern teilweise die Aktualisierung per USB-Stick mit vorherigem Herunterladen von Software aus dem Internet. Dies ist in vielen Fällen für den Nutzer nicht durchführbar. Es sind daher Methoden der Aktualisierung gefragt, die ohne Nutzerinteraktion im Hintergrund ablaufen und so eine ständige Aktualität des Gerätes garantieren.[312]

Privacy Protector

Auch bei Umsetzung der oben genannten Methoden und Best Practices sind Techniken zu einem vollständiger Schutz vor allen Gefahren derzeit noch nicht möglich. Viele Gefahren und Möglichkeiten der Datennutzung sind derzeit unbekannt. Die Möglichkeit einer noch genaueren Zuschauermessung über HbbTV wurde bereits nachgewiesen[313] und wurde durch einen Privacy Protector[314] prototypisch durch den Nutzer steuerbar gemacht. Mit dem Privacy Protector wurde eine Konzeptimplementierung für einen kleinen Computer (Raspberry Pi) vorgestellt, die es dem Konsumenten ermöglicht, das Laden von HbbTV Inhalten ohne seine Zustimmung zu unterbinden. Der Raspberry Pi wird dabei zwischen dem Smart-TV und dem herkömmlichen Internet-Router angeschlossen. Die Verbindung zwischen Smart-TV und Raspberry Pi ist üblicherweise ein Kabelanschluss und die Verbindung zum Internet kann ebenfalls per Kabel oder Drahtlos-Adapter bewerkstelligt werden. Das Gerät kann hinter ein Smart-TV-Gerät montiert werden und ist damit nicht sichtbar. Nach Inbetriebnahme wird eine HbbTV Anwendung nicht mehr standardmäßig

[311] Ghiglieri 2014; Michéle & Karpow 2014.
[312] Vgl. DoctorBeet's Blog 2014.
[313] Ghiglieri, Oswald & Tews 2013a.
[314] Ghiglieri & Tews 2014.

geladen. Der Benutzer bekommt auf dem Bildschirm mitgeteilt, dass eine Internetaktivität durch HbbTV blockiert wurde, woraufhin der Nutzer diese mit dem Drücken des „Green Button“ zulassen kann. Drückt er auf der Fernbedienung nun die grüne Taste, wird erst dann die ursprünglich vom Sender angeforderte Webseite geladen.[315]

In einer weiteren HbbTV-Analyse wurde nachgewiesen, dass eine Nutzermessung auch auf Radiokanälen, die über Satellit übertragen werden, möglich ist.[316] Dies wurde mit einer Erweiterung des oben genannten Systems ebenfalls unterdrückt. Es wurde bereits demonstriert, wie eine neue Art der Zuschauermessung datenschutzfreundlich durchgeführt werden kann.[317] Die derzeitigen Verfahren setzen voraus, dass eine Telefonleitung eine Verbindung zwischen Erfassungsunternehmen und Haushalt herstellt. Im dort vorgestellten Ansatz können nun auch Internetverbindungen genutzt werden, bei dem eine Zwischeninstanz dafür genutzt wird, um Daten zu aggregieren. Diese Aggregation dient dazu, dass Daten über einen speziellen Haushalt nicht an das Erfassungsunternehmen weitergegeben werden, sondern nur gesammelt weitergegeben werden (in diese Falle beispielsweise die Anzahl der Zuschauer über alle Haushalte). Das dort beschriebene Verfahren hat den Vorteil, dass auch andere Geräte (wie z. B. smarte Stereoanlagen) gemessen werden können. Als zusätzliche Besonderheit bekommt der Nutzer die Möglichkeit, die Daten einzusehen und sogar eine Übertragung vollständig abzulehnen.

5.3. Fazit

Der Bereich des Smart Home ist in rasanter Entwicklung begriffen, die an unterschiedlichen Fronten stattfindet. Dies umfasst intelligente Haushaltsgeräte, vernetzte Hausautomation oder netzwerkfähige Multimediageräte. Durch die schnelle Entwicklung kommt die Entwicklung geeigneter Sicherheitsmaßnahmen kaum hinterher. Neben stetig neu bekannt werdenden Sicherheitslücken in einzelnen Lösungen wie Techniken der Gebäudeautomation oder Multimediageräten liegt das größte Bedrohungspotential in den von vernetzten Geräten gesammelten oder verwendeten Daten. Dies zeigt sich besonders deutlich im Bereich der Smart-TVs, die zunehmend den Stellenwert zentraler Allround-Multimedia-Geräte einnehmen und durch ihre umfangreichen Sensoren und die Platzierung im Mittelpunkt des Wohnung ein besonders sensibler Angriffspunkt auf die Privatsphäre der Nutzer sind. Eine zusätzliche Problematik zeigt sich ferner – und dies gilt analog für andere Geräte im Bereich des Smart-Home – in der großen und teilweise unübersichtlichen Anzahl der involvierten Akteure (Geräteherstelle, Gerätebetreiber, Erst-, Zweit- und Drittdienstleister, etc.). Dementsprechend vielfältig ist auch die Anzahl und Art der Angriffsvektoren, die von neugierigen Dienstleistern oder Geräteherstellern bis hin zu böswilligen und gezielten Angriffen mit dem Ziel der Datenbeschaffung reicht. Während die Daten durch Verschlüsselung häufig vor Ausspähen durch unbeteiligte Dritte geschützt werden

[315] Technische Details werden in diesem Rahmen nicht weiter erläutert. Weitere Details befinden sich in Ghiglieri, Tews 2014. Eine prototypische Implementierung des Systems kann auf den Seiten der TU Darmstadt (http://www.smarthome.sit.tu-darmstadt.de/) heruntergeladen werden.
[316] Ghiglieri, Oswald & Tews 2013a.
[317] DoctorBeet’s Blog 2013.

können, sind Nutzer dem Missbrauch der Daten durch die beteiligten Akteure derzeit schutzlost ausgeliefert. Es existieren keine wirksamen Gegenmaßnahmen, die vor ungewollter Datenübermittlung oder dem Tracking von Nutzerverhalten schützen. Dennoch sind perspektivisch unterschiedliche Ansätze denkbar, um die Privatsphäre bei der Nutzung von Smart-TVs zu erhöhen. So hat die Vergangenheit gezeigt, dass eine Erhöhung des Datenschutzes alleine schon durch die korrekte Anwendung von einfachen Best Practice Regeln erreicht werden kann. Dazu zählt der konsequente Einsatz von verschlüsselten Verbindungen zur Datenübertragung. Eine weitere Schutzmöglichkeit liegt darin, eine Aktualisierungsstrategie für Smart-TV Geräte zu etablieren.

Ein auftretendes Sicherheits- und Datenschutzproblem bei Smart-TVs kann direkt einen Vertrauensverlust bei Nutzern und Reputationsverlust bei Unternehmen führen. Um diesem Effekt frühzeitig entgegenzuwirken, ist es notwendig, eine hohe Transparenz in der Einführungsphase solcher Geräte für alle Prozesse zu schaffen. Die rasante Entwicklung neuer Funktionalität stellt vor zahlreiche Herausforderungen. Diese reichen von der Sensibilisierung und Aufklärung der Bevölkerung bis hin zur Entwicklung von komplexen technischen Schutzmaßnahmen. Auch die Aktualisierungsstrategie von Smart-TV-Geräten muss zugunsten einer regelmäßigen und weitgehend automatisiert im Hintergrund vorgenommenen Aktualisierung optimiert werden. Ferner Eine könnte eine konsequente Umsetzung des Prinzips der Datensparsamkeit und einer transparenten Datenübermittlung Nutzern die derzeit nicht gewährleistete Entscheidungsautonomie über die übermittelten Daten zurückgeben. Dazu wird es notwendig sein, einen etablierten Datenschutzprozess zu definieren. Ein Schutz der Kommunikationskanäle könnte ferner durch eine konsequentere Verwendung kryptographischer Methoden der Verschlüsselung erreicht werden.

Ein umfassender Schutz ist jedoch nur möglich, wenn die Übermittlung von Nutzerdaten durch eine Schutzmaßnahme in Form eines „Privacy Protectors“ geschützt werden. Dieser könnte als Gateway zwischen Smart-TV und Internetanbindung geschaltet werden und so die ein- und ausgehenden Verbindungen und Inhalte überwachen. Eine Implementierung dieser Schutzmöglichkeiten wurde bereits prototypisch umgesetzt.[318] Es wäre allerdings eine Serienfertigung sowie eine flächendeckende Verwendung solcher oder ähnlicher Systeme notwendig, um Nutzer vor unerwünschter Datenübermittlung zu schützen. Eine zentrale Rolle wird dabei die Benutzerfreundlichkeit spielen, die für eine flächendeckende Verwendung entscheidend ist. Eine solche Technik ließe sich nicht nur für Smart-TVs, sondern auch als Gateway für die Gesamtheit aller Geräte eines Smart Homes einsetzen. In Zukunft sind Systeme dieser Art notwendig, die etwa wie handelsübliche Router als Standard in jedem Haushalt eingesetzt werden. Sie könnten den Datenstrom überwachen und nach gewissen Regeln ungewollte Verbindungen ignorieren und den Nutzer dadurch schützen.

[318] Siehe Ghiglieri 2014 & Tews.

6. Literatur

Albers, Erik 2013: „Das Recht auf eigene Gerätehoheit als Bedingung der Privatsphäre“, in: Beckedahl & Meister 2013, 249-259.

Aufsichtsbehörden für Datenschutz 2014: „Smartes Fernsehen nur mit smartem Datenschutz“, Technischer Bericht, Gemeinsame Position der Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich (Düsseldorfer Kreis) u. Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten.

Bager, Jo; Dusan Zivadinovic 2014: „Unter Beobachtung. Unterhaltungselektronik spioniert Benutzer aus“, in: c’t, 5/2014, S. 76–77.

Bager, Jo; Schmidt, Jürgen 2014: „Briefgeheimnis. So sichern E-Mail-Provider ihre Privatsphäre“, in: c’t, 4/2014, S. 86–95.

Ball, James 2014: „NSA collects millions of text messages daily in 'untargeted' global sweep“, The Guardian vom 16.01.2014. Online verfügbar unter: http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep; zuletzt abgerufen am 09.09.2015.

Banerjee, Suman; Brik, Vladimir; Gruteser, Marco; Oh, Sangho 2008: „Wireless Device Identification with Radiometric Signatures”, in: Proceedings of the 14th ACM international conference on Mobile computing and networking, ACM.

Beal, Matthew; Ghosh, Joy; Ngo, Hung; Qiao, Chunming 2006: „On Profiling Mobility and Predicting Locations of Wireless Users“, in: Proceedings of the 2nd international workshop on Multi-hop ad hoc networks: from theory to reality, ACM.

Beckedahl, Markus; Meister, Andre (Hrsg.) 2013: „Überwachtes Netz. Edward Snowden und der größte Überwachungsskandal der Geschichte“, Newthinking communications, Berlin.

Biermann, Kai 2011: „Was Vorratsdaten über uns verraten“, Februar 2011. Online verfügbar unter: http://www.zeit.de/digital/datenschutz/2011-02/vorratsdaten-malte-spitz; zuletzt abgerufen am 09.09.2015.

Birkel, Mathias 2013: „Smart TV schafft neue Nutzungstrends“, in: New Business 9/2013, S. 24-26

BITKOM 2012: „Vertrauen und Sicherheit im Netz“, Technischer Bericht, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V., 2012.

BITKOM 2014: „Sicherer E-Mail-Versand ist die große Ausnahme“, BITKOM Presseinformation vom 30. Juni 2014.

Bleich, Holger 2014: „Vertrauenssache. Die Schwächen der E-Mail und was dagegen hilft“, in: c’t 4/2014, S. 82–85.

BLM 2012: „HbbTV beinhaltet Chancen für Lokalfernsehen - Smart-TV-Anwendungen können Reichweiten und Umsätze lokaler TV-Anbieter erhöhen“, BLM Meldung vom 25. 04 2012. Online verfügbar unter: http://www.blm.de/de/infothek/pressemitteilungen/2012.cfm?object_ID=436; zuletzt abgerufen am 09.09.2015.

Boneh, Dan; Michalevsky, Yan; Nakibly, Gabi; Schulman, Aaron 2015: „PowerSpy: Location Tracking using Mobile Device Power Analysis“, arXiv preprint arXiv:1502.03182.

Brauckmann, Jürgen 2014: „Zukunft der Web-PKI? Wege aus der Vertrauenskrise“, in: DuD 7/2014, S. 452–457.

Braun, Herbert 2014a: „Feuer und Flamme. Gründe und Folgen der WhatsApp Übernahme durch Facebook“, in: c’t 7/2014, S. 136–138.

Braun, Herbert 2014b: „Was los ist. Wie WhatsApp zu einem der größten Social Networks wurde“, in: c’t 5/2014, S. 74–774.

Briegleb, Volker; Holland, Martin 2014: „Ex-NSA-Chef: Wir töten auf Basis von Metadaten", Heise Meldung vom Mai 2014. Online verfügbar: http://heise.de/-2187510; zuletzt abgerufen am 09.09.2015.

Broy, Mandred 2012: „Smart Grid: IKT-Architektur für das intelligente Stromnetz“, in: Smart Letter 2012 – Sondernewsletter des Fraunhofer AISEC zu Smart Grid und Smart Meter, S. 2.

BSI 2013a: „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“, BSI – Technische Richtlinie TR-02102-2. Technischer Bericht, Bundesamt für Sicherheit in der Informationstechnik. Online verfügbar unter: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html; zuletzt abgerufen am 09.09.2015.

BSI 2013b: „Technische Vorgaben für intelligente Messsysteme und deren sicherer Betrieb“. BSI-Technische Richtlinie TR-03109, Bundesamt für Sicherheit in der Informationstechnik. Online verfügbar unter: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03109/index_htm.html; zuletzt abgerufen am 09.09.2015.

BSI 2014a: „E-Mail-Sicherheit. Handlungsempfehlungen für Internet-Service-Provider“, Technischer Bericht, Bundesamt für Sicherheit in der Informationstechnik.

BSI 2014b: „Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP)“, Schutzprofil BSI-CC-PP-0073, Version 1.3, Bundesamt für Sicherheit in der Informationstechnik. Online verfügbar unter: https://www.bsi.bund.de/DE/Themen/SmartMeter/Schutzprofil_Gateway/schutzprofil_smart_meter_gateway_node.html; zuletzt abgerufen am 09.09.2015.

Bundesregierung 2013: „Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan Korte, Ulla Jelpke, Jens Petermann, weiterer Abgeordneter und der Fraktion DIE LINKE: Datenschutzprobleme bei Spielekonsolen“, Drucksache 17/14116 vom 12.07. 2013. Online verfügbar unter: dip21.bundestag.de/dip21/btd/17/143/1714373.pdf; zuletzt abgerufen am 09.09.2015.

Callas, Jon; Donnerhacke, Lutz; Finney, Harold; Thayer, Rodney 1998: „OpenPGP Message Format“, RFC 2440, November 1998. Online verfügbar unter: https://www.ietf.org/rfc/rfc2440.txt; zuletzt abgerufen am 09.09.2015.

Cesare, Silvio 2014: „Breaking the Security of Physical Devices“, Blackhat 2014. Online verfügbar unter: regmedia.co.uk/2014/08/06/dfgvhbhjkui867ujk5ytghj.pdf; zuletzt abgerufen am 09.09.2015.

Chaum, David 1981: „Untraceable electronic mail, return addresses, and digital pseudonyms”, in: Communications of the ACM, 24(2)/1981, S. 84-90.

Choudhury, Romit Roy; Cox, Landon; Constandache, Ionut; Gaonkar, Shravan; Sayler, Matt 2009: „Energy-efficient Localization via Personal Mobility Profiling”, in: Mobile Computing, Applications, and Services, S. 203-222, Springer Berlin.

Costache, Mihai, Tudor, Valentin; Almegren, Magnus; Papatriantafilou, Marina; Saunders, Christopher 2011: „Remote control of smart meters: friend or foe”, in: Proceedings of the 7th European Conference on Computer Network Defense, S. 49-56.

Cranor, Lorrie F.; Garfinkel, Simson 2005: „Security and Usability: Designing secure systems that people can use“, O’Reilly, Sebastopol.

Deutsche TV Plattform 2014: „Deutsche TV Plattform“, Meldung der Deutschen TV Plattform vom Mai 2014. Online verfügbar unter: http://www.tv-plattform.de/images/stories/pdf/marktanalyse_smart-tv_2014_de.pdf; zuletzt abgerufen am 09.09.2015.

Dingledine, Roger; Mathewson, Nick; Syverson, Paul 2004: „Tor: The second-generation onion router“, Naval Research Lab Washington DC.

DIVSI 2014a: „Jeder zehnte ist vorsichtiger geworden, die Mehrheit reagiert eher gleichgültig: Abhören? Egal, ich habe nichts zu verbergen!“, DIVSI Presseinformation 23. Mai 2014. Online verfügbar unter: https://www.divsi.de/ wp-content/ uploads/ 2014/ 05/ DIVSI-PM-SNOWDEN_2014-05-23.pdf; zuletzt abgerufen am 09.09.2015.

DIVSI 2014b: „Untersuchung zur Wahrnehmung des Snowden/NSA-Skandals in Deutschland“, Technischer Bericht, DIVSI. Online verfügbar unter: https://www.divsi.de/wp-content/uploads/2014/05/dimap-Bericht-DIVSI.pdf; zuletzt abgerufen am 09.09.2015.

DoctorBeet's Blog 2013: „LG Smart TVs logging USB filenames and viewing info to LG servers“, Blogeintrag vom November 2013. Online verfügbar unter: http://doctorbeet.blogspot.co.uk/2013/11/lg-smart-tvs-logging-usb-filenames-and.html; zuletzt abgerufen am 09.09.2015.

DoctorBeet's Blog 2014: „LG Disables Smart TV features in the EU to force users to accept new oppressive Privacy policy”, Blogeintrag vom November 2014. Online verfügbar unter: http://doctorbeet.blogspot.de/2014/05/lg-disables-smart-tv-features-in-eu-to.html; zuletzt abgerufen am 09.09.2015.

Eckert, Claudia; Krauß, Christoph 2011: „Sicherheit im Smart Grid“, in: DuD 8/2011, S. 535-541.

Eckert, Claudia; Krauß, Christoph 2012: „Sicherheit im Smart Grid. Sicherheitsarchitekturen für die Domänen Privatkunden und Verteilnetz und Berücksichtigung der Elektromobilität“, Alcatel-Lucent Stiftung.

Edmundson, Anne; Simpson, Anna; Kroll, Joshua; Felten, Edward 2014: „Security Audit of Safeplug Tor in a Box“. 4th USENIX Workshop on Free and Open Communications on the Internet (FOCI 14).

Eikenberg, Ronald 2014: „Spion im Wohnzimmer. Privacy und Sicherheit bei Internetfähigen TVs“, in: c’t 4/2014, S. 78–81.

Eggert, Christian 2014: „Nicht nur im Museum: iBeacon wird unser Leben verändern“. Online verfügbar unter: www.huffingtonpost.de/-v_b_5436171.html; zuletzt abgerufen am 09.09.2015.

eMarketer 2013: „Connected TVs Reach One in Four Homes“, eMarketer Meldung vom 03. 01 2013. Online verfügbar unter: http://www.emarketer.com/Article/Connected-TVs-Reach-One-Four-Homes/1009581; zuletzt abgerufen am 09.09.2015.

Engel, Tobias 2014: „SS7: Locate. Track. Manipulate.”, Vortrag auf dem 31. Chaos Computer Congress 2014. Folien und Video verfügbar auf http://events.ccc.de/congress/2014/Fahrplan/events/6249.html; zuletzt abgerufen am 09.09.2015.

Ertel, Sebastian; Venzke-Caprarese, Sven 2014: „Google Universal Analytics. On- und Offline-Profilbildung anhand von User-IDs“, in: DuD, 3/2014, S. 181–185.

Fokusgruppe Connected Home des Nationalen IT-Gipfels 2014: „Vor dem Boom – Marktaussichten für Smart Home. Ergebnisdokument der Fokusgruppe Connected Home UAG Breitband, AG 8“, Nationaler IT Gipfel Hamburg 2014.

Forum Privatheit 2014: „White Paper Selbstdatenschutz“, Forum Privatheit, 2. Auflage. Online verfügbar unter: http://www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums.php; zuletzt abgerufen am 09.09.2015.

Froböse, Rolf 2014: „VDE-Institut setzt Standards für das intelligente Haus“, The Huffington Post vom 12.08.2014. Online verfügbar unter: http://www.huffingtonpost.de/rolf-froboese/vdeinstitut-setzt-standar_b_5668197.html; zuletzt abgerufen am 09.09.2015.

Froitzhuber, Kilian 2014: „Redtube-Abmahnungen: Eine überflüssige Saga neigt sich dem Ende zu“. Online verfügbar unter: https://netzpolitik.org/2014/redtube-abmahnungen-eine-ueberfluessige-saga-neigt-sich-dem-ende-zu; zuletzt abgerufen am 09.09.2015.

Gallagher, Ryan; Greenwald, Glenn: „How the NSA Plans to Infect Millions of Computers with Malware“, The Intercept vom 12.03.2014. Online verfügbar unter: http://interc.pt/1oM1dEC; zuletzt abgerufen am 09.09.2015.

Gaycken, Sandro 2014: „Sachverständigengutachten IT-Infrastruktur", Technischer Bericht, Deutscher Bundestag, 1. Untersuchungsausschuss der 18. Wahlperiode.

Gellman, Barton; Soltani, Ashkan 2013: „NSA tracking cellphone locations worldwide, Snowden documents show“, Dezember 2013. Online verfügbar unter: http://wapo.st/1g7lbdq; zuletzt abgerufen am 09.09.2015.

Gerling, Rainer W. 2014: „De-Mail und E-Mail made in Germany sind ein konsequenter Schritt“, in: DuD, 2/2014, S. 109–111.

Ghiglieri, Marco 2014: „Incorrect HTTPS Certificate Validation in Samsung Smart TVs”, Technical Report TU Darmstadt TUD-CS-2014-0802.

Ghiglieri, Marco; Lange, Benjamin; Simo, Hervais; Waidner, Michael 2015: „Security und Privacy bei Smart TVs – Bedrohungspotential und technische Lösungsansätze“, in: Weiterdenken – Heinrich-Böll-Stiftung Sachsen (Hrsg.): Digitale Schwellen – Privatheit und Freiheit in der digitalen Welt, S. 67-84.

Ghiglieri, Marco; Oswald, Florian; Tews, Erik 2013a: „HbbTV - I Know What You Are Watching“, 13. Deutscher IT-Sicherheitskongress des BSI, Bonn.

Ghiglieri, Marco; Oswald, Florian; Tews, Erik 2013b: „HbbTV: Neue Funktionen mit möglichen Nebenwirkungen“, in: FKT - Die Fachzeitschrift für Fernsehen, Film und elektronische Medien, 10/2013, S. 563-566.

Ghiglieri, Marco; Simo, Hervais; Waidner, Michael 2012: „Technical Aspects of Online Privacy“, Technischer Bericht, Fraunhofer Institut für Sichere Informationstechnologie.

Ghiglieri, Marco; Tews, Erik 2014: „A Privacy Protection System for HbbTV in Smart TVs”, in: 11th Consumer Communications and Networking Conference (CCNC), Las Vegas, S. 648-653. Ghiglieri, Marco; Oswald, Florian; Tews, Erik 2013a: „HbbTV - I Know What You Are Watching“, 13. Deutscher IT-Sicherheitskongress des BSI, Bonn.

Golbeck, Jennifer 2015: „Introduction to Social Media Investigation: A Hands-on Approach“, Syngress.

Goldhammer, Klaus; Wiegand, André; Birkel, Matthias 2012: „Potenziale von Smart TV-Plattformen für lokale Fernsehsender“, Studie für Bayerische Landeszentrale für neue Medien (BLM). Goldmedia Berlin.

Goldmedia 2012: „Web-TV-Monitor 2012: Web-TV-Markt gewinnt an Professionalität – mobile Nutzung steigt“, Goldmedia Pressemeldung vom 25.10.2012, München/Berlin.

Goldschlag, David; Reed, Michael; Syverson, Paul 1996: „Hiding routing information“, in: Information Hiding, 1996, S. 137-150, Springer Berlin.

Grattafiori, Aaron; Yavor, Josh 2013: „The Outer Limits: Hacking the Samsung Smart TV“, Black Hat US, Las Vegas.

Greenberg, Andy 2014: „Now Everyone Wants to Sell You a Magical Anonymity Router. Choose Wisely“. Online verfügbar unter: http://www.wired.com/2014/10/anonymity-routers; zuletzt abgerufen am 09.09.2015.

Greenwald, Glenn 2014: „Die globale Überwachung - Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen “, Droemer Verlag.

Greenwald, Glenn; MacAskill, Ewen 2013: „NSA Prism Program Taps in to User Data of Apple, Google and others”, The Guardian, 07.06.2013. Online verfügbar unter: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data; zuletzt abgerufen am 09.09.2015.

Hansen, Marit 2014: „Datenschutz nach dem Summer of Snowden – Schlussfolgerungen für Politik und Praxis“, in: DuD 38/2014, S. 439-444

Herrmann, Dominik; Wendolsky, Rolf; Federrath, Hannes 2009: „Website fingerprinting: attacking popular privacy enhancing technologies with the multinomial naïve-bayes classifier“, in: Proceedings of the 2009 ACM Workshop on Cloud Computing Security, S. 31-42.

Hoffmann-Riem, Wolfgang 2014: „Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses am 22. Mai 2014“.

IRT GmbH 2014: „HbbTV mit Second-Screen-Funktion“, IRT Meldung vom 11. 09 2014. Online verfügbar unter: https://www.irt.de/no_cache/de/aktuell/news/view/article/hbbtv-mit-second-screen-funktion.html; zuletzt abgerufen am 09.09.2015.

Jacoby, David 2014: „IoT: How I hacked my home“, Artikel vom 21.08.2014. Online verfügbar unter: https://securelist.com/analysis/publications/66207/iot-how-i-hacked-my-home; zuletzt abgerufen am 09.09.2015.

Janssen, Jan Keno; Porteck, Stefan; Scherschel, Fabian 2014: „Geheimdienst. Messenger-Apps mit Ende-zu-Ende-Verschlüsselung“, in: c't, 72014, S. 139–144.

Jendrian, Kai 2014: „Sicheres Instant Messaging. Alternativen zu WhatsApp und iMessage“, in: DuD 5/2014, S. 301–304.

Johnson, Aaron; Wacek, Chris; Jansen, Rob; Sherr, Micah; Syverson, Paul 2013: „Users get routed: Traffic correlation on Tor by realistic adversaries“, in: Proceedings of the ACM SIGSAC Conference on Computer & Communications Security, S. 337-348.

Kaps, Reiko 2014: „Gezähmte Monster. Datenspione ins lokale Netz einsperren“, in: c't 5/2014, S. 78–81.

Kim, Seungjoo; Lee, SeungJin 2013: „Smart tv security - #1984 in 21st century“, CanSecWest Vancouver. Online verfügbar unter: http://cansecwest.com/slides/2013/SmartTV Security.pdf; zuletzt abgerufen am 09.09.2015.

Klinger, Roland 2012: „Moderne Technik unterstützt selbstständiges Wohnen im Alter“; in: KVJS 2012, S. 4-5.

Knoke, Felix 2010: „Intelligente Stromzähler als Einfallstor für Hacker“, Spiegel Online Netzwelt-Ticker vom 30.03.2010. Online verfügbar unter: http://www.spiegel.de/netzwelt/web/-a-686431.html; zuletzt abgerufen am 09.09.2015.

Korte, Jan; Jelpke, Ulla; Petermann, Jens; Sitte, Petra; Tempel, Frank; Wawzyniak, Halina: 2013: „Kleine Anfrage der Abgeordneten Jan Korte, Ulla Jelpke, Jens Petermann, Dr. Petra Sitte, Frank Tempel, Halina Wawzyniak und

der Fraktion DIE LINKE: Datenschutzprobleme bei Spielkonsolen“, Drucksache 17/14116 vom 25.06.2013. Online verfügbar unter: http://dip21.bundestag.de/dip21/btd/17/141/1714116.pdf; zuletzt abgerufen am 09.09.2015.

Kossel, Axel 2015: „Datenschutzbeauftragter: Schülern fehlt die Medienkompetenz“, Heise Meldung vom 08.02.2015. Online verfügbar unter: http://heise.de/-2543695; zuletzt abgerufen am 09.09.2015.

Kramer, Nicole; Utz, Sonja 2009: “The privacy paradox on social network sites revisited: The role of individual characteristics and group norms.” Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 3(2), article 2.

Kuhlen, Dorothea 2012: „Betreutes Wohnen mit ‚Smart Living Manager‘ - Quartiersmanagement plus Technik als innovatives Angebot“; in KVJS 2012, S. 22-25.

Kuhlmann, Ulrike 2014: „Smart Home“, in: c’t 19/2014, S. 72.

Kuri, Jürgen 2013: „CE Week: Der Kampf um den ‚Second Screen‘“. Heise Meldung vom 28. 06 2013. Online verfügbar unter: http://www.heise.de/-1902324.html; zuletzt abgerufen am 09.09.2015.

KVJS 2012: „My smart home is my castle - Wohnqualität durch benutzerfreundliche Technik“, Dokumentation der Fachtagung des Kommunalverbandes für Jugend und Soziales Baden Württemberg (KVJS) am 22.05.2012. Online verfügbar unter: http://www.bundesanzeiger-verlag.de/betreuung/aktuelles/aktuelle-meldungen/newsdetails/artikel/my-smart-home-is-my-castle-wohnqualitaet-durch-benutzerfreundliche-technik-6789.html; zuletzt abgerufen am 09.09.2015.

Lamb, Logan 2014: „Home Insecurity: No Alarms, False Alarms, and SIGINT“, in: DEF Con 22, 2014.

Lemos, Robert 2010: „Angriff der Killerbiene. Technology Review“, Infotech vom 13.4.2010. Online verfügbar unter: http://www.heise.de/-974224.html; zuletzt abgerufen am 09.09.2015.

Lendino, Jamie 2014: „Panasonic Unveils Voice-Activated TVs With Facial Recognition“. PCMag Meldung vom 06. 01 2014. Online verfügbar unter: http://www.pcmag.com/article2/0,2817,2429165,00.asp; zuletzt abgerufen am 09.09.2015.

Leyendecker, Hans; Mascolo, Georg 2014: „Gedränge am Daten-Drehkreuz“, Süddeutsche Zeitung vom 27.06.2014. Online verfügbar unter: http://www.sueddeutsche.de/digital/geheimdienst-kooperation-gedraenge-am-daten-drehkreuz-1.2016514; zuletzt abgerufen am 09.09.2015.

Lindskog, Stefan; Winter, Philipp 2014: „Spoiled Onions: Exposing Malicious Tor Exit Relays“, Technischer Bericht, Karlstad University. Online verfügbar unter: http://veri.nymity.ch/spoiled_onions/techreport.pdf; zuletzt abgerufen am 09.09.2015.

Lischka, Konrad; Rosenbach, Marcel 2011: „Hacker klauen Daten von Zoll-Server“, Spiegel Meldung vom Juli 2011. Online verfügbar unter: http://www.spiegel.de/netzwelt/web/cyber-attacke-hacker-klauen-daten-von-zoll-server-a-773189.html; zuletzt abgerufen am 09.09.2015.

Lösche, Ulf; Morgenstern, Maik; Schiefer, Michael 2014: „AV-TEST-Studie. 7 Smart-Home-Starter-Kits im Sicherheits-Test“, AV-Test.

Mansmann, Urs 2014: „E-Mail-Provider stellen auf Transportverschlüsselung um“, Heise-Meldung vom 30.03.2014. Online verfügbar unter: http://heise.de/-2157950; zuletzt abgerufen am 09.09.2015.

Mascolo, Georg 2015: „BND half NSA beim Ausspähen von Frankreich und EU-Kommission“, Süddeutsche Zeitung vom 29. April 2015. Online verfügbar unter: http://www.sueddeutsche.de/politik/geheimdienst-affaere-bnd-half-nsa-beim-ausspaehen-von-frankreich-und-eu-kommission-1.2458574; zuletzt abgerufen am 09.09.2015.

Meier, Jörg 2012: „Kommunikationsformen im Wandel. Brief - E-Mail – SMS“, in: Werkstatt Geschichte, 60/2012, S. 58–75, 2012.

Michéle, Benjamin; Karpow, Andrew 2014: „Watch and be Watched: Compromising All Smart TV Generations,“ in: 11th Consumer Communications and Networking Conference (CCNC), Las Vegas, USA, S. 642-647, IEEE, 2014.

Nikiforakis, Nick; Kapravelos, Alexandros; Joosen, Wouter; Kruegel, Christopher; Piessens, Frank; Vigna, Giovanni 2013: „Cookieless monster: Exploring the ecosystem of web-based device fingerprinting”, in: 2013 IEEE Symposium on Security and Privacy, S. 541-555.

Nohl, Karsten; Page, Chris. 2010: “GSM – SRSLY?”, 26th Chaos Communication Congress, Berlin, Vortrag und Folien. Online verfügbar unter: https://events.ccc.de/congress/2009/Fahrplan/events/3654.en.html; zuletzt abgerufen am 09.09.2015.

Nohl, Karsten 2010: „Attacking phone privacy”, BlackHat USA 2010. Online verfügbar unter: https://media.blackhat.com/bh-us-10/whitepapers/Nohl/BlackHat-USA-2010-Nohl-Attacking.Phone.Privacy-wp.pdf; zuletzt abgerufen am 09.09.2015.

Norcie, Greg; Blythe, Jim; Caine, Kelly; Camp, L. Jean 2014: „Why Johnny Can’t blow the Whistle: Identifying and Reducing Usability Issues in anonymity Systems“, Technischer Bericht, Internet Society. Online verfügbar unter: http://www.internetsociety.org/doc/why-johnny-cant-

blow-whistle-identifying-and-reducing-usability-issues-anonymity-systems; zuletzt abgerufen am 09.09.2015.

OECD 2013: „Working Party on Communication Infrastructures and Services Policy“, Technischer Bericht, OECD. Online verfügbar unter: www.ift.org.mx/iftweb/wp-content/uploads/2014/07/presen-OCDE-Infraestructura-140613.pdf; zuletzt abgerufen am 09.09.2015.

Ohland, Günther 2014: „Wie sicher ist das Smart Home?“, PC-Magazin Meldung vom 13.1.2014. Online verfügbar unter: http://www.pc-magazin.de/ratgeber/sicherheit-vernetztes-heim-smart-home-sicher-1934188.html; zuletzt abgerufen am 09.09.2015.

Oren, Yossef; Keromytis, Angelos D. 2014: „From the Aether to the Ethernet—Attacking the Internet using Broadcast Digital Television“, USENIX Security 14, San Diego, USA.

Pitts, Josh 2014: „The case of the modified binaries“, Blog vom 23.10.2014. Online verfügbar unter: http://www.leviathansecurity.com/blog/the-case-of-the-modified-binaries; zuletzt abgerufen am 09.09.2015.

PwC 2013: „Media Trend Outlook Smart TV: Mehrwert für den Konsumenten, mehr Umsatz für die Medienbranche“, Technischer Bericht, Partner im weltweiten Verbund.

Radicati, Sara 2015: „Email Statistics Report, 2015-20192“, Technischer Bericht, The Radicati Group.

Ramsdell, Blake 1999: „S/MIME Version 3 Message Specification“, RFC 2633, June 1999. Online verfügbar unter: https://www.ietf.org/rfc/rfc3851.txt; zuletzt abgerufen am 09.09.2015.

Renaud, Karen; Volkamer, Melanie; Renkema-Padmos, Arne 2014: „Why Doesn’t Jane Protect Her Privacy?“, Privacy Enhancing Technologies Symposium, Amsterdam.

Rieger, Frank 2010: „Vorratsdatenspeicherung: Du kannst dich nicht mehr verstecken“, Frankfurter Allgemeine Zeitung vom 02.03.2010. Online verfügbar unter: http://www.faz.net/-1937442.html; zuletzt abgerufen am 09.09.2015.

Rosenbach, Marcel; Stark, Holger 2014: „Der NSA-Komplex. Edward Snowden und der Weg in die totale Überwachung“, Deutsche Verlags-Anstalt.

Roßnagel, Alexander; Jandt, Silke; Richter, Philipp 2014: „Die Zulässigkeit der Übertragung personenbezogener Daten in die USA im Kontext der NSA-Überwachung“, in: DuD 38/2014, S. 545-551.

Saeltzer, Gerhard 2014: „Vorsicht! Krimineller ‚Datenschutz' und gefährliche ‚Datensicherheit', in: DuD 5/2014, S. 333–339.

Sasse, M. Angela; Flechais, Ivan 2005: „Usable Security: Why Do We Need it? How Do We Get it?", in: Cranor & Garfinkel 2005, S. 13-30.

Sattler, Claus 2011: „Smart TV: Wer erringt die Portalhoheit auf dem Fernseher", Goldmedia Innovation GmbH, Düsseldorf, 2011.

Schröder, Burkhard 2013: „Verschlüsselung - nein danke!", Heise Artikel vom 08.07.2013. Online verfügbar: http://www.heise.de/tp/artikel/39/39466/1.html; zuletzt abgerufen am 09.09.2015.

Schäfer, Ulrich 2010: „Geheimaktion ‚Clipper' - Obermanns Prüfung", Süddeutsche Zeitung vom 17.05.2010. Online verfügbar unter www.sueddeutsche.de/wirtschaft/-1.213711; zuletzt abgerufen am 09.09.2015.

Scherschel, Fabian 2015: „PowerSpy: Handy-Ortung über den Strom-Verbrauch", Online verfügbar unter: http://heise.de/-2570509; zuletzt abgerufen am 09.09.2015.

Schleipfer, Stefan 2014: „Facebook-Like-Buttons. Technik, Risiken und Datenschutzfragen", in: DuD 5/2014, S. 318–324.

Schmidt, Jürgen 2015a: „Die Schlüssel-Falle. Gefälschte PGP-Keys im Umlauf", in: c't 6/2015, S. 160-163.

Schmidt, Jürgen 2015b: „Lasst PGP sterben!", in: c't 6/2015, S. 3.

Schmundt, Hilmar 2014: „Glotze glotzt zurück", in: Der Spiegel, 8/2014, S. 128.

Schulze, Eva 2012: „Wohntechnik – Voraussetzungen für Akzeptanz und Nutzen", in: KVJS 2012, S. 6-16.

Sheng, Steve; Broderick, Levi; Koranda Colleen A.; Hyland, Jeremy J. 2006: „Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software", Technischer Bericht, Carnegie Mellon University.

Sousedek, Jan 2008: „Why Johnny can't encrypt: A Usability Study of PGP", Technischer Bericht, Technische Universität Berlin, 2008.

Spiegel 2013: „NSA-Überwachung", Dossier auf SPIEGEL Online. Online verfügbar unter: http://www.spiegel.de/thema/nsa_ueberwachung; zuletzt abgerufen am 09.09.2015.

Statista 2010: „Wie wird sich der Markt für Smart Home bis 2020 entwickeln?", Statista Artikel. Online verfügbar unter: http://de.statista.com/statistik/daten/studie/183271/umfrage/prognose-zur-entwicklung-

von-smart-home-aus-sicht-der-hersteller; zuletzt abgerufen am 09.09.2015.

Statista 2011a: „Anzahl der Smart TV-Haushalte in Deutschland im Jahr 2010 und Prognose bis 2016 (in Millionen)“, Statista Artikel. Online verfügbar unter: http://de.statista.com/statistik/daten/studie/208236/umfrage/prognose-zur-entwicklung-der-smart-tv-haushalte-in-deutschland; zuletzt abgerufen am 09.09.2015.

Statista 2011b: „Prognose zur Anzahl der Haushalte mit mind. einem an das Internet angeschlossenen HbbTV-Gerät von 2011 bis 2016 (in Millionen)“, Statista Artikel. Online verfügbar unter: http://de.statista.com/statistik/daten/studie/271953/umfrage/prognose-zur-entwicklung-der-hbbtv-haushalte-in-deutschland; zuletzt abgerufen am 09.09.2015.

Strotman, Carsten 2015: „Hilfestellung. Wie DNSSEC und DANE die Mail-Verschlüsselung erleichtern“, in c’t 5/2015, S. 154-155.

Stumpf, Frederic 2012a: „Ausgewählte Projekte zu Smart Meter Security“, in: Smart Letter 2012 – Sondernewsletter des Fraunhofer AISEC zu Smart Grid und Smart Meter, Fraunhofer AISEC, S. 5-6.

Stumpf, Frederic 2012b: „Smart Meter Security“, in: Smart Letter 2012 – Sondernewsletter des Fraunhofer AISEC zu Smart Grid und Smart Meter, Fraunhofer AISEC, S. 3-4.

Telekom 2013: „Fakten Mobilfunktechnik, Oktober 2013“, Telekom Meldung. Online verfügbar unter: http://www.telekom.com/static/-/9982/3/fakten-mobilfunktechnik-si; zuletzt abgerufen am 09.09.2015.

Urban, Tobias; Riedel, René; Robles, Antonio G.; Pohlmann, N. 2014: „Vorgehensweise zur Erstellung eines Smart Meter Gateways“, Institut für Internet-Sicherheit.

Waidner, Michael 2014: „Stellungnahme zur Anhörung des NSA Untersuchungsausschusses am 26. Juni 2014“, Technischer Bericht, Deutscher Bundestag, 1. Untersuchungsausschuss der 18. Wahlperiode.

Warren, Jonathan 2012: „Bitmessage: A Peer-to-Peer Message Authentication and Delivery System“, Technischer Bericht. Online verfügbar unter: https://bitmessage.org/bitmessage.pdf; zuletzt abgerufen am 09.09.2015.

Warren, Jonathan 2013: „Proposed Bitmessage Protocol Technical Paper“, Technischer Bericht. Online verfügbar unter: https://bitmessage.org/Bitmessage%20Technical%20Paper.pdf; zuletzt abgerufen am 09.09.2015.

Weichert, Thilo 2014: „Internet-TV und Datenschutz“, in: DuD, 8/2014, S. 528–535.

Whitten, Alma; Tygar, Doug 1999: „Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0", Technischer Bericht. Online verfügbar unter: www.gaudior.net/alma/johnny.pdf; zuletzt abgerufen am 09.09.2015.

Wocher, Martin 2014: „Ein Schutzschild fürs private Heim", Handelsblatt vom 10.09.2014. Online verfügbar unter: http://www.handelsblatt.com/technik/vernetzt/smart-home-ein-schutzschild-fuers-private-heim/10674844.html; zuletzt abgerufen am 09.09.2015.

Zahneisen, Anton 2012: „SOPHIA – ein Konzept, das soziale Betreuung und Technikeinsatz verbindet", in: KVJS 2012, S. 17-21.

Zetter, Kim 2014: „How thieves can hack and disable your home alarm system", Meldung bei Wired.com vom 23.7.2014. Online verfügbar unter: http://www.wired.com/2014/07/hacking-home-alarms; zuletzt abgerufen am 09.09.2015.