Fraunhofer SIT

FRAUNHOFER-INSTITUT FÜR SICHERE INFORMATIONSTECHNOLOGIE

SIT TECHNICAL REPORTS

Trend- und Strategiebericht

Privatsphärenschutz und Vertraulichkeit im Internet

Michael Herfert und Michael Waidner

CASED

EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN

Fraunhofer SIT

Privatsphärenschutz und Vertraulichkeit im Internet

Trend- und Strategiebericht

16. September 2013

Michael Herfert[1]
Abteilungsleiter Cloud, Identity & Privacy, Fraunhofer SIT
michael.herfert@sit.fraunhofer.de

Michael Waidner[1,2]
Institutsleiter Fraunhofer SIT und
Direktor EC SPRIDE und CASED
michael.waidner@sit.fraunhofer.de

[1] Fraunhofer-Institut für
Sichere Informationstechnologie SIT
Rheinstraße 75, 64295 Darmstadt

[2] Technische Universität Darmstadt,
Fachbereich Informatik/Fachgruppe SIT
Mornewegstraße 30, 64289 Darmstadt

IMPRESSUM

Kontaktadresse:
Fraunhofer-Institut für
Sichere Informationstechnologie SIT
Rheinstraße 75
64295 Darmstadt
Telefon 06151 869-213
Telefax 06151 869-224
E-Mail info@sit.fraunhofer.de
URL www.sit.faunhofer.de

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Hrsg. Michael Waidner
SIT Technical Reports
Trend- und Strategiebericht
Privatsphärenschutz und Vertraulichkeit im Internet
(SIT-TR-2013-03)
Michael Herfert und Michael Waidner
ISSN 2192-8169

Inhalt

1 Zusammenfassung

Seit Juni 2013 enthüllte der ehemalige US-Geheimdienstmitarbeiter Edward Snowden zahlreiche Details über die massenhafte Ausspähung von Daten im Internet durch die Geheimdienste *NSA* und *GCHQ*. Das Interesse an IT-Lösungen zum Schutz vor Ausspähung ist seither sprunghaft angestiegen. Viele sinnvolle IT-Lösungen existieren bereits, viele Probleme sind aber noch nicht ausreichend gelöst und erfordern weitergehende Forschung und Entwicklung in der Informationstechnologie.

Wir präsentieren eine Reihe von Problemen, die erforscht und gelöst werden müssen, um Vertraulichkeit und Privatsphärenschutz im Internet angesichts der Gefahr von Massenüberwachung sicherzustellen.

Massenüberwachung und der damit verbundene Verlust von Vertraulichkeit und Privatsphäre sind keineswegs die einzigen Gefahren, vor denen sich Bürger und Unternehmen im Internet schützen müssen. Viele weitere Aspekte von IT-Sicherheit und Privatsphärenschutz im Internet erfordern ebenfalls Forschung und Entwicklung.

2 Vorbemerkung

Seit Juni 2013 enthüllte der ehemalige US-Geheimdienstmitarbeiter Edward Snowden zahlreiche Details über Abhörprogramme insbesondere der amerikanischen und britischen Nachrichtendienste *NSA* und *GCHQ* [GM13, S13]. Verdachtsunabhängig und in großem Umfang werde der internationale Internetverkehr erfasst und ausgewertet. Zusätzlich werde auf privilegierte Weise auf Daten zugegriffen, die sich auf den Servern von US-Anbietern in den USA befänden. Genannt werden *Apple, AOL, Google, Facebook, Microsoft, Skype, Yahoo* und *YouTube*.

Als Folge hat in Deutschland das Vertrauen in Staat und Wirtschaft als Garanten von Vertraulichkeit und Privatsphärenschutz im Internet deutlich abgenommen [B13]. Viele Bürger empfinden die Abhörprogramme als unverhältnismäßige Eingriffe in ihre Grundrechte und fühlen sich von ihrer Regierung allein gelassen. Unternehmen und Verbände befürchten, dass die Programme auch der Industriespionage dienen könnten.

Die Nachfrage nach technischen Lösungen zum Schutz vor Überwachung – z. B. nach Verschlüsselung – ist sprunghaft angestiegen. Studien zeigen, dass im Bereich der IT-Sicherheit insgesamt ein hoher Nachholbedarf besteht. Sowohl im privaten [B13] als auch im gewerblichen [C13] Umfeld wird erschreckend oft selbst auf elementarste und leicht zugängliche IT-Sicherheitstechniken verzichtet.

Insgesamt wird der Markt für Informationstechnologie, IT-Sicherheit eingeschlossen, durch Anbieter aus den USA dominiert. Derzeit ist ein deutlicher Vertrauensverlust in IT-Produkte aus den USA festzustellen. Gleichzeitig scheint das Vertrauen in nationale IT-Dienstleistungen zu wachsen, da die hier geltenden Datenschutzgesetze als Schutz gegen die Ausspähung durch fremde Nachrichtendienste wahrgenommen werden. In Segmenten, in denen alternative nationale Angebote existieren, kann daher mit einer Verschiebung von Marktanteilen weg von den USA gerechnet werden. Beispielsweise erwarten Anbieter von Cloud-Computing-Diensten aus den USA aufgrund der Abhörprogramme bereits erhebliche Umsatzrückgänge, während europäische Anbieter teilweise deutliche Zuwächse feststellen [C13a, S13a, S13b]. Die sich daraus ergebenden Chancen für die europäische und insbesondere die deutsche IT-Branche sind offensichtlich.

Es gibt viele gute Angebote zur IT-Sicherheit, und Bürger und Unternehmen sollten ihren Schutzbedarf prüfen und die vorhandenen Angebote nutzen. Die Umsetzung existierender Angebote ist aber nur der erste notwendige Schritt.

Möchte man dauerhaft und umfassend Vertraulichkeit und Privatsphärenschutz im Internet sicherstellen, so sind noch zahlreiche Forschungsfragen zu beantworten. Für viele Probleme gibt es bereits erste, teilweise auch praktische Lösungen. Oft skalieren diese aber noch nicht ausreichend für den Einsatz im Internet, d. h. in einem sehr offenen und sehr großen Netz.

Im Folgenden präsentieren wir eine Reihe von Problemen, deren Lösung Forschung und Entwicklung in der Informationstechnologie erfordern und die wir für besonders wichtig und dringend erachten.

Wir haben uns bei der Auswahl dieser Probleme bewusst auf den Bereich „Vertraulichkeit und Privatsphärenschutz im Internet" beschränkt. Dieser Bereich ist zentral für die IT-Sicherheit und den Privatsphärenschutz insgesamt, aber keineswegs der einzige, der weiterer Forschung und Entwicklung bedarf. Weitere Forschungsfragen zur IT-Sicherheit findet man in [GL07, B09, D09, W13] und zum Privatsphärenschutz in [F11, A13].

Vertraulichkeit und Privatsphärenschutz im Internet können nicht alleine auf der Ebene der Informationstechnologie adressiert werden; es sind auch Ethik, Psychologie, Soziologie, Recht und Ökonomie gefragt. Alle diese Disziplinen müssen zusammenarbeiten, um Anforderungen zu präzisieren und Lösungen zu entwickeln.

In unserer Einschätzung zur Dringlichkeit eines Problems aus Forschungssicht betrachten wir sowohl technische als auch wirtschaftlich-juristische Lösungsmöglichkeiten. Technische Lösungen sind notwendig, wenn ein Dienst im größeren Umfang Daten in einen Rechtsraum transferiert, der keinen akzeptablen juristischen Schutz bietet. Technische Lösungen können zudem auch Sicherheit gegenüber Änderungen im politischen System bieten. Gelingt es, durch den Aufbau wirtschaftlicher Binnenangebote Daten und Dienste im Inland zu halten, so kann das inländische Recht möglicherweise bereits alleine einen ausreichenden Schutz bieten.

Dank. Für hilfreiche Kommentare danken wir Michael Kreutzer, Marit Hansen und Thorsten Strufe. Dieser Bericht entstand mit freundlicher Unterstützung des im Rahmen des LOEWE-Programms vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) geförderten Forschungszentrums CASED (www.cased.de) und des vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Cybersecurity-Kompetenzzentrums EC SPRIDE (www.ecspride.de).

3 Forschungsfragen

Im Folgenden stellen wir zwölf wichtige Fragen, zu deren Beantwortung Forschung und Entwicklung notwendig ist. Wir tun dies in vier Abschnitten, die sich grob daran orientieren, an welchen Stellen die Daten eines Nutzers ausgespäht werden können:

- Ausspähung von Inhaltsdaten im Netz (Abschnitt 3.1)
- Ausspähung von Verkehrs- und Nutzungsdaten (Abschnitt 3.2)
- Ausspähung von Inhaltsdaten in der Cloud (Abschnitt 3.3)
- Übergreifende Themen der IT-Sicherheit und des Privatsphärenschutzes (Abschnitt 3.4)

3.1 Ausspähung von Inhaltsdaten im Netz

Frage 1, Verteilung vertrauenswürdiger Schlüssel: Verschlüsselung schafft Vertraulichkeit – aber nur, wenn der Verschlüsselnde auch den richtigen Schlüssel verwendet. Wie können Nutzer, die voneinander lediglich eine Adresse (z. B. URL, E-Mail-Adresse) kennen, für ihr Gegenüber den richtigen Schlüssel bestimmen? ■

Das Internet dient dazu, zwei beliebige Nutzer nur anhand ihrer Adressen miteinander zu verbinden. Es existiert jedoch kein zu diesem Modell passender Schlüsselverteilmechanismus im Internet.

Der bislang beste Ansatz zur Lösung dieses Problems sind Public-Key-Infrastrukturen (PKIs). PKIs sind gut geeignet für *geschlossene* Gruppen, etwa Firmen. In einer Firma kann man eine zentrale Stelle einrichten, der alle vertrau-

en und die die Verteilung der Schlüssel übernimmt.[1] In offenen Gruppen wie dem Internet ist dies naturgemäß nicht so einfach. Aber genau auf der Existenz solcher zentraler, für alle vertrauenswürdiger Stellen beruhen die Funktionsweise und Sicherheit einer PKI.

Dementsprechend gibt es keine internetweit verwendbare PKI für Nutzer. Wer von seinem Gegenüber nur eine E-Mail-Adresse kennt, hat im Allgemeinen keine Möglichkeit, für dieses Gegenüber auf einfache und vertrauenswürdige Weise einen Schlüssel zu bestimmen.

Für den sicheren Abruf von Webseiten mittels *https* werden allerdings PKIs verwendet. Diese PKIs sind vorwiegend dazu gedacht, Schlüssel an Webserver zu verteilen. Die Browser von *Apple, Google, Microsoft, Mozilla* und *Opera* sind so voreingestellt, dass sie Dutzende solcher PKIs akzeptieren – die meisten sind dem durchschnittlichen Internetnutzer völlig unbekannt. Ein Nutzer müsste eigentlich stets bewusst entscheiden, ob die verwendete PKI für die gerade mit *https* abgerufene Webseite ausreichend vertrauenswürdig ist. In der Realität tut das so gut wie niemand, alle voreingestellten PKIs werden für alle Zwecke akzeptiert. Im Prinzip kann daher jede im Browser vorkonfigurierte PKI für jeden denkbaren Webserver im Internet einen Schlüssel erzeugen – keineswegs nur die PKI, die dazu von diesem Web-Server beauftragt wurde. Hierdurch entstehen falsche Zertifikate, durch die ein Angreifer die Identität eines Web-Servers übernehmen kann. Solche falschen Zertifikate wurden tatsächlich schon erstellt, beispielsweise durch die niederländische PKI *DigiNotar.* Diese Delegierung von Vertrauensentscheidungen an den Browser-Hersteller ist an sich schon problematisch, erscheint aber doppelt fragwürdig angesichts der Überwachungsprogramme fremder Nachrichtendienste.

Es besteht also ein dringender Bedarf nach Schlüsselverteilverfahren, die für große und offene Gruppen wie das Internet geeignet sind. Die Verfahren müssen sich, zusammen mit der eigentlichen kryptographischen Funktion, in Dienste wie Web (SSL/TLS), E-Mail (OpenPGP, S/MIME), VPN, VoIP-Telefonie usw. ohne Minderung der Benutzbarkeit integrieren lassen. Wichtig ist dabei, dass die Schlüsselverteilung eine Ende-zu-Ende-sichere Kommunikation zwischen Nutzern ermöglicht, nicht nur eine Kommunikation zwischen Nutzern und Servern bzw. von Servern untereinander.

[1] Genau genommen zertifizieren diese zentralen Stellen, die sogenannten Certification Authorities, lediglich die öffentlichen Schlüssel. Diese und ähnliche Details sind für unsere Diskussion allerdings nicht von Belang.

Schlüsselverteilung ist ein altes Problem, und man kann sich daher fragen, ob eine praktische Lösung überhaupt möglich ist. Unsere Hoffnung auf eine positive Antwort gründet sich auf zwei Beobachtungen.

Erstens könnte Schlüsselverteilung auf existierende Vertrauensinfrastrukturen aufsetzen, z. B. kommerzielle Strukturen von ISPs oder auch informelle Strukturen wie Freundschaftsgraphen in Social Networks. Entsprechende Forschungsansätze gibt es bereits. In Deutschland existiert mit dem neuen Personalausweis zudem eine staatliche Infrastruktur, die zur Schlüsselverteilung genutzt werden kann.

Zweitens geht es uns hier vorrangig um *Massen*überwachung, und eine solche setzt stets hochskalierbare Überwachungstechnologien voraus: Die marginalen Kosten für jeden weiteren zu Überwachenden müssen vernachlässigbar klein sein. Umgekehrt betrachtet: Auch Verfahren, die oft, aber nicht immer Sicherheit garantieren, können Massenüberwachung deutlich erschweren. Deshalb können hier auch Ansätze zur Schlüsselverteilung betrachtet werden, die zu Beginn einer Kommunikationsbeziehung manchmal nur schwache Sicherheit garantieren, diese aber mit der Zeit verstärken und auf Dauer Unsicherheit zumindest erkennbar machen. Zur Verhinderung gezielter Einzelüberwachungen genügen solche schwachen Ansätze allerdings nicht.

Dringlichkeit. Wir halten dies für das dringendste Problem im Zusammenhang mit dem Schutz vor Massenüberwachung. Ein Schutz von Kommunikationsinhalten ist ohne Schlüsselverteilung praktisch unmöglich. Dies gilt auch für Nachrichten, die innerhalb desselben Landes verschickt werden, da im heutigen Internet auch solche Nachrichten oft mehrfach die Landesgrenze überschreiten.

Für geschlossene Systeme ist dieses Problem gut verstanden. Im Prinzip ist es möglich, eine nationale PKI für alle Bürger eines Landes aufzubauen und damit einen vermutlich sehr großen Teil der Kommunikation der Bürger dieses Landes zu schützen. In der Praxis sind entsprechende Versuche bislang allerdings immer gescheitert. Für das Internet insgesamt ist das Problem ungelöst.

Frage 2, Sichere Verschlüsselung: Heutige Verschlüsselungsverfahren sind auf die Fähigkeiten heutiger Angreifer ausgelegt. Zukünftige Angreifer verfügen über bessere Analysetechniken und leistungsfähigere Soft- und Hardware. Wie können Nutzer Daten so verschlüsseln, dass sie auch in der Zukunft sicher sind? ■

Heute übliche kryptographische Verfahren wie RSA und AES mit ausreichend langen Schlüsseln gelten in der Forschung als kryptographisch sicher. Selbst Nachrichtendiensten wie der *NSA*, die als führend in der Kryptoanalyse gilt,

wird nicht zugetraut, diese Verfahren im für die Massenüberwachung notwendigen großen Stil kryptographisch brechen zu können.[2]

Die Sicherheit dieser Verfahren sinkt aber mit der Zeit: Was heute als sehr sicher erscheint, könnte in 20 Jahren leicht brechbar sein. Die Analyse kryptographischer Verfahren ist ein überaus aktives Forschungsgebiet, und Fortschritte sind auf Dauer sehr wahrscheinlich. Zudem profitiert die Kryptoanalyse von jedem Fortschritt in der Leistungsfähigkeit von IT. Dies gilt sogar überproportional für Fortschritte in der Rechnerarchitektur, etwa bei Quantenrechnern. Wiederholt hat sich zudem gezeigt, dass im algorithmischen Sinne sichere kryptographische Systeme oft auf der Implementierungsebene – z. B. als Programmcode in einem Web-Server, als Smartcard – erfolgreich angegriffen werden können (z. B. über Seitenkanäle, Protokollfehler, absichtliche Hintertüren).

Dringlichkeit. Es besteht ein Bedarf an der Entwicklung kryptographischer Verfahren, die beweisbare, längerfristige Sicherheit bieten. Forschungsprojekte dieser Art existieren bereits, auch in Deutschland, und müssen wegen des dauerhaften Charakters dieses Problems entsprechend dauerhaft fortgesetzt werden. Hier sind sowohl Grundlagenforschung als auch angewandte Forschung notwendig.

[2] *NSA* und *GCHQ* sollen dennoch in der Lage sein, in vielen Fällen verschlüsselte Nachrichten zu entschlüsseln. Allerdings soll dies nicht auf kryptographischer Ebene geschehen, sondern durch Ausnutzung von zufällig oder absichtlich eingebauten Design- und Implementierungsschwächen in Algorithmen zur Erzeugung von Pseudozufallszahlen und in Programmen zur Verschlüsselung [B13a]. Es ist unklar, ob diese Fähigkeit zur Massenüberwachung eingesetzt oder nur für Einzelüberwachungen und nachträgliches Entschlüsseln einzelner Nachrichten verwendet werden kann.

3.2 Ausspähung von Verkehrs- und Nutzungsdaten im Netz

Frage 3, Beobachtbarkeit im Netz: Auch verschlüsselte Kommunikation ist beobachtbar: Wer Zugriff auf die Datenpakete hat, der kann anhand von Metadaten erkennen, wer wann mit wem wie lange kommuniziert hat, im Fall von E-Mail sogar die Betreff-Zeile der Nachricht. Wie können Nutzer, die voneinander lediglich eine Adresse kennen, unbeobachtbar per Web, E-Mail, VoIP usw. kommunizieren? ■

Ein Prinzip zur Lösung dieses Problems ist seit den 1980er Jahren bekannt: Statt Nachrichten direkt vom Sender zum Empfänger zu übertragen, werden diese über eine Reihe von Servern, *Mixe* genannt, vermittelt. Jeder dieser Mixe ent- und verschlüsselt die Nachrichten inklusive Metadaten. Setzt man die Idee richtig um, dann müssten alle verwendeten Mixe zusammenarbeiten, um eine Nachricht direkt durch das Netz verfolgen zu können.

Die Idee ist umgesetzt in dem bekannten und allgemein zugänglichen System *TOR (The Onion Router),* aber auch in anderen Angeboten, z. B. dem in Deutschland entwickelten *JAP* (auch bekannt als *JonDo).* Allerdings lösen diese Systeme das Problem nur teilweise.

Zum einen sind die Systeme nicht darauf ausgelegt, einen signifikanten Teil des Internetverkehrs zu übernehmen. Die Installation und Verwendung ist relativ kompliziert. Die spezielle Architektur der Systeme ist für Kommunikation mit hohen Anforderungen an Bandbreite und Verzögerungszeiten – wie etwa bei VoIP oder Videoanwendungen – wenig geeignet. Der Zugriff auf Web-Seiten mit eingebetteten dynamischen Inhalten ist problematisch. Eine echte Integration mit anderen Kommunikationsdiensten wird meist nicht unterstützt. Zudem lassen sich diese Dienste relativ leicht durch die Netzbetreiber blockieren.

Zum anderen wurden diese Systeme unter der Annahme entworfen, eine umfassende Überwachung der Kommunikation sei unmöglich. Andernfalls existieren Korrelationsangriffe, mit denen ein Angreifer statistisch erkennen kann, wer mit wem kommuniziert. Die Überwachungsprogramme von *NSA* und *GCHQ* lassen diese Annahme in neuem Licht erscheinen.

Es besteht weiterer Forschungs- und Entwicklungsbedarf. Die bekannten Methoden und Systeme müssen so weiterentwickelt werden, dass sie für einen breiten Einsatz unter Wahrung der Dienstqualität tauglich werden.

Es muss auch erforscht werden, wie die dafür notwendige Infrastruktur bereitgestellt werden kann. Denkbar wäre etwa, dass nationale Telekommunikationsanbieter durch eine leichtgewichtige Form von Mixen und ein Routing, das

Nachrichten nicht unnötig über Landesgrenzen schickt, ihre Kunden vor der Beobachtung durch fremde Nachrichtendienste schützen.

Wertvoll für die Nutzer wäre auch eine Information durch den Diensterbringer, inwieweit die Vertraulichkeit der (Verkehrs-)Daten garantiert wird und inwieweit Zugriffsmöglichkeiten für Nachrichtendienste, eigene Scanning-Dienste oder auch andere Unternehmen bestehen. Eine solche Transparenz stärkt das Bewusstsein der Nutzer für Risiken und befähigt sie dazu, Dienste entsprechend ihres Schutzniveaus auszuwählen bzw. eigene Schutzmaßnahmen zu ergreifen.

Dringlichkeit. Das Problem ist im begrenzten Umfang gelöst, im vollen Umfang praktisch ungelöst. Pragmatische Lösungen wie die in den beiden vorigen Abschnitten angedeuteten scheinen aber möglich und sollten zügig umgesetzt werden.

Frage 4, Bewegungsprofile in Mobilfunknetzen: In heutigen Mobilfunknetzen (GSM, UMTS, LTE) kann der Betreiber den Aufenthaltsort des Nutzers relativ genau bestimmen. Wie kann der Nutzer mobil kommunizieren, ohne dass der Betreiber ein detailliertes Bewegungsprofil erstellen kann? ■

In heutigen Netzen ist dieses Problem unvermeidbar. Die massenhafte Erstellung von Bewegungsprofilen durch einen fremden Nachrichtendienst setzt allerdings voraus, dass dieser direkten Zugriff auf den Mobilfunkbetreiber erhält. Dies ist zwar nicht ausgeschlossen, erscheint aber aufgrund der Rechtslage innerhalb Europas unwahrscheinlich. Das Einräumen eines solchen Zugriffs wäre nicht nur illegal, es könnte sich bei Bekanntwerden auch verheerend auf die Reputation des Mobilfunkbetreibers auswirken.

Auch in der Forschung gibt es für dieses Problem noch keine ausreichend effizienten Lösungen. Wir sehen daher einen zwar umfangreichen, aber eher langfristigen Forschungsbedarf.

Dringlichkeit. Dies ist ein wichtiges Problem, das eine für heute vermutlich ausreichende juristische Lösung besitzt. Eine langfristig zufriedenstellende technische Lösung erfordert neue Ideen und neue Forschung.

Frage 5, Tracking: Nutzer können oft und unbemerkt von Internet-Diensten wiedererkannt und über unterschiedliche Dienste hinweg verfolgt werden. Hierdurch entstehen detaillierte Bewegungs- und Interessensprofile. Wie können Nutzer dieses „Tracking" erkennen und kontrollieren? ■

Nutzer können im Internet, selbst wenn sie sich nirgendwo registrieren oder anmelden, durch eine Vielzahl von Methoden wiedererkannt und verfolgt werden. Die einfachsten nutzen explizit gesetzte Web-Cookies. Komplexere Methoden lesen – vom Nutzer unbemerkt – bestimmte Eigenschaften der Soft- und Hardware des Nutzers aus und ermöglichen damit meist eine sehr genaue Identifizierung.

Ein Schutz vor diesem Tracking und damit vor dem ungewollten Erstellen von Bewegungs- und Interessensprofilen ist mit heutigen Web-Browsern nicht möglich. Die Werbewirtschaft scheint zwar prinzipiell bereit, eine über die Browser kommunizierte "Do not track"-Option zu standardisieren. Die Bedeutung und Verbindlichkeit dieser Option sind jedoch noch heftig umstritten.

Es besteht Bedarf an der Erforschung von Mechanismen, die vor dieser Art von Tracking schützen, die möglichst systemunabhängig funktionieren und die den Schutz automatisch an neue Gegebenheiten anpassen. Die Mechanismen haben nicht die Aufgabe, alle „Tracker" pauschal zu unterdrücken. Vielmehr sollen sie den Nutzer in die Lage versetzen, eine bewusste und dann für die Dienstanbieter verbindliche Entscheidung zu treffen.

Neben dem Tracking über die Eigenschaften von Soft- und Hardware können Nutzer auch über ihre persönlichen Eigenschaften identifiziert werden, expliziten wie Name, Adresse und Alter und impliziten wie ihren speziellen Schreibstil oder die in ihren Texten ausgedrückten Vorlieben und Meinungen.

Explizite Eigenschaften lassen sich durch kryptographische Pseudonyme und sogenannte attributbasierte Credentials (ABC) verbergen. Eine einfache Variante hiervon findet sich z. B. im neuen deutschen Personalausweis. Komplexere Varianten existieren in Forschungsprototypen und wurden im praktischen Versuch getestet, konnten sich aber bislang aufgrund ihrer Komplexität, noch unzureichenden Benutzbarkeit und teilweise auch unklarer Geschäftsmodelle nicht durchsetzen. Das Verbergen impliziter Eigenschaften ist ein offenes Forschungsproblem.

Auch hier besteht weiterer Bedarf an Forschung und Entwicklung. Die bekannten Methoden zum Verbergen expliziter Eigenschaften müssen benutzbarer und in ökonomisch sinnvolle Anwendungsfälle integriert werden**.** Es muss auch erforscht werden, wie die dafür notwendigen

Infrastrukturen bereitgestellt werden können. Methoden zum Verbergen impliziter Eigenschaften müssen erfunden und entwickelt werden.

Dringlichkeit. Dieses Problem ist sehr wichtig und im praktischen Sinne ungelöst. Eine nationale, juristische Lösung ist schwer vorstellbar, da die Dienste, innerhalb derer das Tracking stattfindet, zu einem großen Teil grenzüberschreitend erbracht werden. Es braucht also technische Lösungen.

3.3 Ausspähung von Inhaltsdaten in der Cloud

> **Frage 6, Speichern und Teilen in der Cloud:** Wie können Nutzer ihre Daten sicher auf fremden, nicht notwendigerweise vertrauenswürdigen Servern im Internet speichern und vertraulich und gezielt mit anderen Nutzern teilen? ■

Speicherdienste wie *Dropbox* und *Amazon S3* erlauben es, bestimmte Informationen im Internet zu speichern und festzulegen, wer wann welchen Zugriff darauf haben soll.

Der Zugriff auf diese Dienste erfolgt meist über *https* und ist damit im Prinzip vor dem Abhören durch Unbeteiligte geschützt.[3] Die Dienste sind den Nutzern bekannt, was das Schlüsselverteilproblem stark vereinfacht (mit „certificate pinning“ sogar bei Verwendung von Webbrowsern).

Neben dem vom Nutzer definierten Kreis hat aber in den meisten angebotenen Diensten auch der Betreiber Zugriff auf die Daten. Je nach Lokation des Dienstes bzw. der vom Dienst verwendeten Server können fremde Nachrichtendienste unter Umständen die Herausgabe der Daten verlangen.

Ganz unabhängig von dieser Ausspähbarkeit durch den Betreiber selbst wurden viele Dienste schon erfolgreich angegriffen oder waren fehlerhaft realisiert, so dass dann zumindest zeitweise auch unberechtigte Dritte Zugriff hatten.

Zu diesem Problem existieren einige Teillösungen, die kurz- und mittelfristig umgesetzt und verbessert werden sollten.

Der einfachste Fall besteht darin, dass Daten nur gespeichert, aber nicht mit anderen Nutzern geteilt werden sollen. Der Nutzer kann seine Daten daher vor

[3] Vgl. Fußnote 2 auf Seite 10.

dem Abspeichern in der Cloud selbst mit nur ihm bekannten Schlüsseln verschlüsseln und damit vor dem Zugriff durch Dritte schützen. Entsprechende Angebote existieren – werden allerdings in der Praxis bislang kaum eingesetzt. Selbst in diesem einfachsten Fall besteht also ein gewisser Forschungsbedarf.

Sollen Daten auch geteilt werden, so müssen alle Empfänger passende Schlüssel erhalten. Auch hierfür existieren bereits einige, auch kommerzielle Lösungen. Damit der Cloud-Betreiber die gespeicherten Daten nicht lesen und damit auch nicht an fremde Nachrichtendienste weitergeben kann, muss der Nutzer die Schlüsselverteilung selbst übernehmen oder an eine dritte, vom Cloud-Betreiber unabhängige und für den Nutzer vertrauenswürdige Stelle delegieren. In kommerziellen Lösungen wird diese Sicherheit aber oft zugunsten besserer Benutzbarkeit vollständig aufgegeben, so dass der Cloud-Betreiber doch die Schlüssel verwaltet.

Dringlichkeit. Angesichts der Gefahr der Ausspähung von Nutzerdaten direkt bei den Dienstanbietern halten wir auch diese Frage für sehr dringend. Viele der notwendigen technischen Konzepte sind bekannt, es mangelt aber an der Benutzbarkeit und der Integration mit anderen Diensten und mit IT-Managementsystemen (also der Standardisierung). Hier ist also insbesondere die angewandte F&E angesprochen.

Neben technischen Ansätzen spielen hier auch wirtschaftlich-juristische Lösungen eine Rolle: Dienste zum sicheren Speichern in der Cloud werden bereits innerhalb Deutschlands angeboten und unterliegen dann dem deutschen Recht.

Frage 7, Berechnen in der Cloud: Wie können Nutzer die Vorteile des Cloud Computing nutzen, ohne blind dem Betreiber der Cloud vertrauen zu müssen? Wie kann verhindert werden, dass ihre Daten und Prozesse durch den Betreiber missbraucht werden können? ■

Diese Frage ist in der Praxis im engeren Sinne unbeantwortet. Sie betrifft Infrastrukturangebote wie *Amazon AWS*, aber auch Software-as-a-Service wie *Google Suche, Google Mail, Google Docs* und *Microsoft 365* und Social Networks wie *Facebook* und *Google+.*

Cloud-Betreiber adressieren das Problem heute vorwiegend durch den Aufbau einer guten Reputation, z. B. durch Offenlegung ihrer IT-Architektur, Zertifizierungen nach anerkannten Standards, regelmäßige Veröffentlichung von Auditierungen und insbesondere durch Vermeidung des Bekanntwerdens reputationsschädigender Sicherheitsvorfälle. Reputation alleine schafft ohne weitere Maßnahmen allerdings nur blindes Vertrauen statt wirkliche Vertrauenswürdigkeit – es gibt keine Garantien.

Cloud-Anbieter mit Sitz und Servern ausschließlich in Deutschland können darauf verweisen, dass deutsches Recht die Daten der Nutzer im Allgemeinen vor der Herausgabe an fremde Nachrichtendienste schützt. Dies stellt für viele Anwendungen eine praktikable juristische Schutzmaßnahme dar. Ähnliches gilt für andere europäische Staaten, wobei es jedoch angesichts der Aktivitäten von *GCHQ* in *UK* unklar ist, inwieweit Daten innerhalb der EU grenzüberschreitend tatsächlich geschützt sind.

In der Forschung werden auch technische Ansätze zu einer Lösung verfolgt, die auf besonderen kryptographischen Verfahren oder auf der Verwendung besonderer Hardware beruhen. Diese Ansätze sind recht weit von einem praktischen Einsatz entfernt, und es bedarf mittel- bis langfristig noch erheblicher Forschungsanstrengungen.

Für bestimmte Dienste existieren bereits einfachere Lösungen, die oft als Erweiterung vorhandener Dienste konzipiert sind, z. B. zum sicheren Teilen von Information in *Facebook* oder zum sicheren Suchen in *Google* und *Bing*. In der Praxis werden diese Erweiterungen allerdings kaum verwendet, und teilweise wehren sich die Dienstanbieter auch gegen diese Ansätze, indem sie ihren Einsatz in den Nutzungsbedingungen untersagen oder sie technisch blockieren.

Ein generelles praktisches Problem besteht darin, dass viele Cloud-Angebote, z. B. Kalender und E-Mail, auf der Nutzerseite nur in einem Webbrowser laufen, nicht in einem eigenen Programm. Ein Großteil der Daten des Nutzers und der Funktionalität bleibt auf dem Server. Hier sind Lösungen zu entwickeln, wie trotz dieser Architektur die Sicherheit des Nutzers gegenüber dem Server hergestellt werden kann.

Dringlichkeit. Dieses Problem ist für unterschiedliche Arten von Clouds unterschiedlich dringend.

Dienste, die lediglich Rechenleistung in der Cloud anbieten (Infrastructure as a Service), können und werden bereits national in kompetitiver Weise angeboten. Sie unterliegen ausschließlich dem deutschen Recht und sind damit rechtlich dem direkten Zugriff durch fremde Nachrichtendienste entzogen. Für die IT-Sicherheit im weiteren Sinne spielt der Ort der Cloud allerdings keine Rolle, d. h. auch für solche nationalen Clouds sind technische Lösungen, die ohne blindes Vertrauen auskommen, anzustreben.

Komplexere Dienste, insbesondere Social Networks, sind erfahrungsgemäß nicht leicht durch nationale Angebote zu ersetzen. Daher sind technische Lösungen notwendig.

Frage 8, Aggregierende Dienste: Internet-Dienste basieren zunehmend darauf, den aktuellen Kontext (z. B. Ort, nahe Geräte) und Daten aus anderen Diensten (z. B. Kalender, E-Mail) zueinander in Beziehung zu setzen. Angebote wie *Google Now* sind ohne solch umfassende Integration von Quellen und Diensten kaum vorstellbar. Wie kann die Privatsphäre ohne blindes Vertrauen in den Betreiber geschützt werden? ■

Frage 8 ist letztlich eine erweiterte Version von Frage 7: Diese Dienste stellen sehr komplexe Cloud-Angebote dar, für die meist keine europäischen Alternativangebote existieren. Auch hier besteht ein sehr hoher und dringender Forschungs- und Entwicklungsbedarf.

Dringlichkeit. Dies ist eines der dringendsten Probleme. Es gibt bislang weder technische Lösungen noch lassen sich Dienste dieser Art leicht durch nationale, sich selbst finanzierende Angebote ersetzen.

3.4 Übergreifende Themen der IT-Sicherheit und des Privatsphärenschutzes

Sollen Vertraulichkeit und Privatsphärenschutz im Internet durch technische Maßnahmen sichergestellt werden, so stellen sich ganz unabhängig vom Detailproblem immer einige sehr generelle Fragen. Ihre Beantwortung erfordert einen erheblichen Forschungsbedarf, eine detailliertere Diskussion würde aber den Rahmen dieses Papieres sprengen.

Dringlichkeit: Die folgenden vier Fragen gehören zu den Kernproblemen der IT-Sicherheit und des Privatsphärenschutzes.

Frage 9, System- und Softwaresicherheit: Vertraulichkeit und Privatsphärenschutz setzen voraus, dass Bürger und Unternehmen über ausreichend sichere IT verfügen: Absichtlich eingebaute Hintertüren in Soft- und Hardware, über die gezielt oder gar massenhaft Daten ausspioniert werden können, müssen erkannt und geschlossen werden. Soft- und Hardware soll keine Schwachstellen enthalten, die zu Angriffen missbraucht werden können. Angriffe von innen und außen dürfen zu keinen signifikanten Datenabflüssen oder anderen Schäden führen. Wie kann man dies erreichen? ■

Frage 10, Benutzbarkeit. Mechanismen für IT-Sicherheit und Privatsphärenschutz werden von Nutzern häufig ignoriert, falsch verwendet oder umgangen. Häufig erscheinen sie den Nutzern unangemessen kompliziert und hinderlich und der Gegenwert – besserer Schutz – wird nicht wahrgenommen oder zumindest nicht ausreichend wertgeschätzt. Wie kann man IT-Dienste so entwerfen, dass ihre Schutzfunktionalität für den Nutzer keine zusätzliche oder gefühlt unnötige Last bedeutet und Fehlbedienungen und Versehen weitgehend vermieden werden? ■

Frage 11, Transparenz und Intervenierbarkeit. IT-Dienste sind für die Nutzer häufig „Black Boxes": Die möglichen Konsequenzen für Sicherheit und Privatsphäre sind unklar. Die Qualität und Vertrauenswürdigkeit der IT-Sicherheit und des Privatsphärenschutzes ist für den Nutzer meist unsichtbar und kann daher nicht zur Auswahl zwischen unterschiedlichen Diensten beitragen. Auf die Möglichkeit, dass Nutzerdaten vom Diensterbringer gescannt und eventuell an Dritte weitergegeben werden, wird oft nur sehr versteckt hingewiesen. Viele Dienste bieten den Nutzern zudem keine ausreichende Möglichkeit, das Angebot auf einfache Weise im eigenen Sinne sicherer und privatsphärenfreundlicher zu gestalten oder Fehler und unerwünschte Effekte im Nachhinein zu korrigieren (z. B. gespeicherte Daten zu löschen). Wie kann man erreichen, dass Nutzer ein ausreichendes Verständnis für die Auswirkungen ihres Handelns entwickeln und sich bewusst entscheiden können? Wie kann man berechtigtes Vertrauen in IT herstellen? Wie kann man erreichen, dass Nutzer ungewollte Auswirkungen im Nachhinein korrigieren können? ■

Frage 12, Finanzierbarkeit. Maßnahmen für IT-Sicherheit und Privatsphärenschutz erzeugen zwar häufig Mehrkosten, oft aber keinen unmittelbar erfahrbaren Nutzen. Der Unterschied zwischen sicheren und weniger sicheren IT-Angeboten ist im Allgemeinen nicht sichtbar, da es kaum entsprechende Bewertungsstandards gibt. Insbesondere private Nutzer vermeiden deshalb oft proaktive Investitionen in die eigene IT-Sicherheit und den eigenen Privatsphärenschutz – erst nach einem Schaden ändert sich zumindest kurzfristig diese Einstellung. Der Verlust von Vertraulichkeit und Privatsphärenschutz ist normalerweise nicht einmal feststellbar, so dass selbst diese Motivation meist entfällt. Wie kann man also die notwendigen technischen Maßnahmen motivieren und finanzieren? ■

4 Schlussbemerkung

Vertraulichkeit und Privatsphärenschutz im Internet erfordern einen umfassenden und verlässlichen Schutz vor Abhörmaßnahmen und Massenüberwachung durch fremde Nachrichtendienste. Einiges kann bereits durch die Umsetzung bekannter Ansätze erreicht werden, aber alleine genügt dies nicht: Es ist weitere Forschung und Entwicklung notwendig. Die hier gestellten 12 Fragen fassen die aus unserer Sicht wichtigsten und drängendsten Probleme zusammen.

Wir verstehen dieses Dokument als einen Beitrag zu einer umfassenden Forschungsagenda zu Vertraulichkeit und Privatsphärenschutz im Internet.

Wissenschaft, Staat und Industrie müssen eine solche Agenda gemeinsam schaffen und in die Realität umsetzen. Europa und insbesondere Deutschland sind in einer sehr guten Position, hier eine Vorreiterrolle zu spielen: Das Problembewusstsein im Markt ist sehr hoch. IT-Sicherheitslösungen „made in Germany“ haben einen deutlichen Vertrauensvorteil gegenüber Lösungen aus anderen Ländern. Die Forschung und mittelständische IT-Sicherheitsindustrie in Deutschland sind in der Lage, eine solche Forschungsagenda umzusetzen und praktische Lösungen zu entwickeln.

5 Referenzen

[A13] Privatheit im Internet: Chancen wahrnehmen, Risiken einschätzen, Vertrauen gestalten; acatech POSITION, Berlin, Mai 2013; *http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Publikationen/Stellungnahmen/acatech_POS_neu_Internet_Privacy_WEB.pdf*

[B09] Arbeitsprogramm IT-Sicherheitsforschung; BMBF und BMI, Berlin 2009; *http://www.bmbf.de/pub/arbeitsprogramm_it_sicherheitsforschung.pdf*

[B13] BITKOM: Sicherheit und Vertrauen im Netz; BITKOM, Berlin, 2013; *http://www.bitkom.org/files/documents/BITKOM_PK_Sicherheit_im_Netz_Charts_25_07_2013.pdf*

[B13a] James Ball, Julian Borger, Glenn Greenwald, Nicole Perlroth, Scott Shane, Jeff Larson: US and UK Spy Agencies Defeat Privacy and Security on the Internet; The Guardian, 5. September 2013; *http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security*

[C13] Studie: Industriespionage 2012; Corporate Trust, München, 2013; *http://corporate-trust.de/pdf/CT-Studie-2012_FINAL.pdf*

[C13a] Daniel Castro: How Much will PRISM Cost the U.S. Cloud Computing Industry?; ITIF, Washington, DC, 8/2013; *http://www2.itif.org/2013-cloud-computing-costs.pdf*

[D09] A Roadmap for Cybersecurity Research; US DHS, Washington 2009; *http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf*

[F11] Simone Fischer-Hübner, Chris Jay Hoofnagle, Ioannis Krontiris, Kai Rannenberg, Michael Waidner: Online Privacy: Towards Informational Self-Determination on the Internet; Dagstuhl Report 1/2 and Dagstuhl Manifesto 1/1, Schloss Dagstuhl 2011; *http://drops.dagstuhl.de/opus/volltexte/2011/3205/pdf/dagman_v001_i001_p001_11061.pdf*

[GL07] Seymour E. Goodman, Herbert S. Lin (Hrsg.): Toward a Safer and More Secure Cyberspace; National Research Council and National

Academy of Engineering, Washington 2007;
http://books.nap.edu/catalog.php?record_id=11925

[GM13] Glenn Greenwald, Ewen MacAskill: NSA Prism Program Taps in to User Data of Apple, Google and others; The Guardian, 7. Juni 2013;
http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

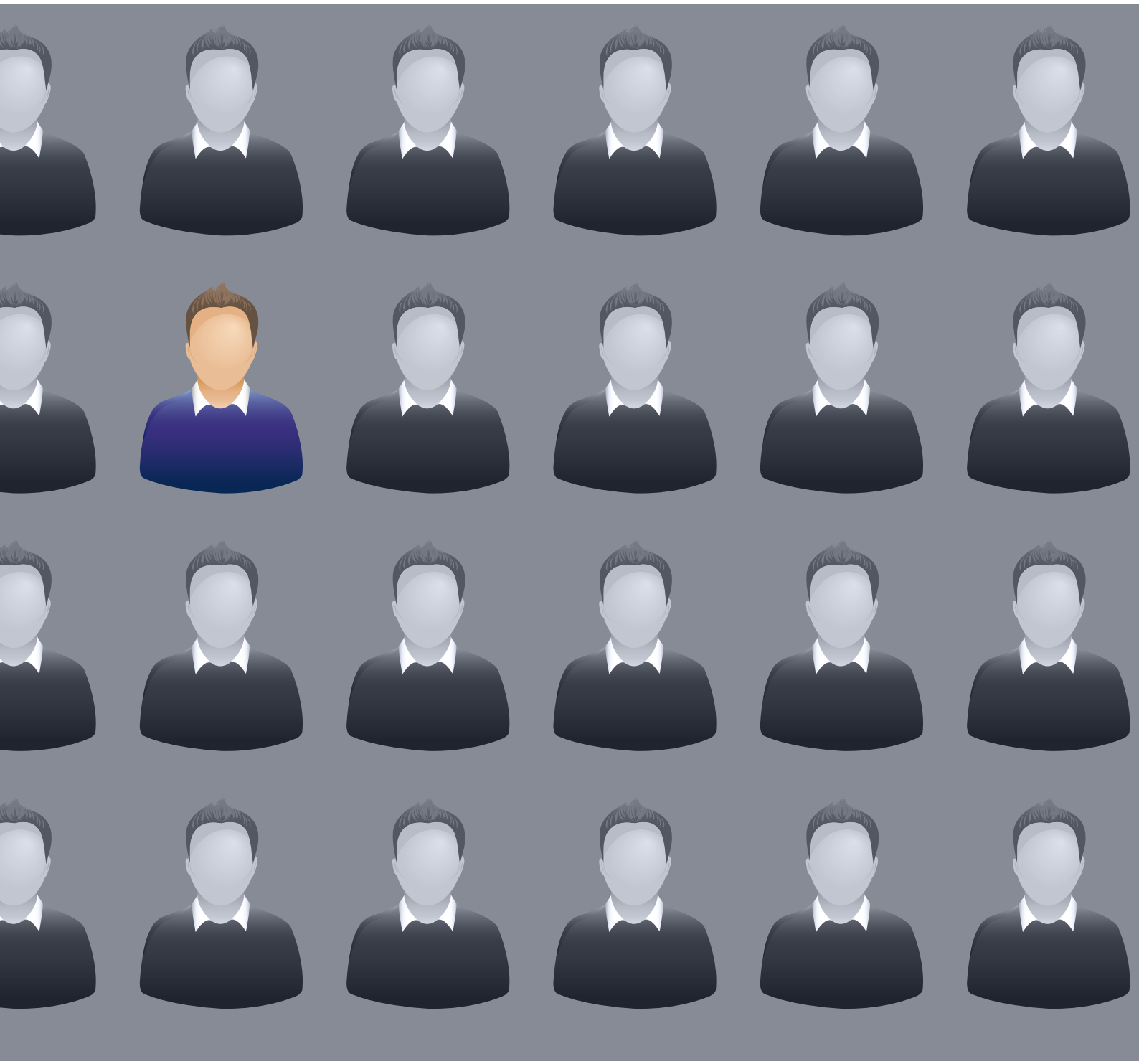
[S13] Dossier zur NSA-Überwachung auf SPIEGEL Online;
http://www.spiegel.de/thema/nsa_ueberwachung

[S13a] Achim Sawall: NSA-Skandal kostet Cloud-Anbieter 35 Milliarden US-Dollar; auf golem.de, 6. August 2013;
http://www.golem.de/news/usa-nsa-skandal-kostet-cloud-anbieter-35-milliarden-us-dollar-1308-100818.html

[S13b] James Staten: The Cost of PRISM Will Be Larger Than ITIF Projects; Forrester Research, 2013;
http://www.forbes.com/sites/forrester/2013/08/15/the-cost-of-prism-will-be-larger-than-itif-projects/?goback=.gde_1864210_member_270698204

[W13] Michael Waidner, Michael Backes, Jörn Müller-Quade (Hrsg.): Entwicklung sicherer Software durch Security by Design; SIT Technical Report, Fraunhofer Verlag, München 2013;
https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Trendbericht_Security_by_Design.pdf

Fraunhofer
SIT



Fraunhofer SIT
Institut für Sichere
Informationstechnologie

Rheinstraße 75
64295 Darmstadt

Tel. +49 6151 869-399
Fax +49 6151 869-224

info@sit.fraunhofer.de
www.sit.fraunhofer.de