Kai Jendrian

30 Jahre nach 1983 – oder die Rettung der Privatsphäre im Internet

Dreißig Jahre nach dem wegweisenden „Volkszählungsurteil" des Bundesverfassungsgerichts und der Formulierung des Grundrechts auf informationelle Selbstbestimmung ist die „Netzwelt" vom Schutz dieses Grundrechts weiter entfernt denn je. Der Beitrag stellt einige Möglichkeiten des Selbstschutzes vor, durch technische Maßnahmen einen Teil der eigenen Privatsphäre im Internet wirksam vor dem Zugriff Dritter zu schützen.

1 Privatsphäre im Internet

Abhörskandale wie PRISM[1], Tempora[2], DGSE[3] und die offensichtlich gängige Praxis mancher Anbieter im Internet, Inhalte von Nachrichten und Kommunikationen systematisch auszuwerten[4,5] bestätigen, was lange Zeit nur gemunkelt wurde. Inzwischen haben wir es schwarz auf weiß: Privatsphäre existiert im Internet von 2013 de facto nicht. Auch dem letzten Zweifler sollte klar geworden sein: wir leben heute in einer gläsernen Netzwelt – dreißig Jahre nach dem Volkszählungsurteil[6] ist das Grundrecht auf informationelle Selbstbestimmung[7] in der Praxis nur begrenzt und mit großen Mühen durchzusetzen.

Dieser Beitrag versucht keine rechtliche, keine politische und auch keine moralische Bewertung dieser Situation. Statt dessen sollen konkrete Anregungen gegeben werden, welche technischen Möglichkeiten heute bestehen, noch etwas Privatsphäre im Internet zu retten und zu beleuchten, wie weit das möglich ist.

Annahmen

In diesem Beitrag wird davon ausgegangen, dass Dritte in der Lage sind, sich beliebig unbemerkt Kenntnis von Daten während der Übertragung über das Internet sowie auf den Servern von Dienstleistern zu verschaffen. Es wird allerdings angenommen, dass die Plattform der Benutzer (PC, Laptop, Tablet, Smartphone) nicht durch Hintertüren oder Spionagesoftware korrumpiert ist.

Der letzte Aspekt wird bewusst ausgegrenzt, da einem System, das sich vollständig unter der Kontrolle Dritter befindet, keinerlei Vertrauen entgegen gebracht werden kann. Nur soviel: In begrenztem Umfang kann man sich bemühen, ein vertrauenswürdiges System zu pflegen, indem man ggf. nur offene Software einsetzt, deren Quelltext man vollständig versteht (wenn das denn möglich ist – siehe Kernel Bug in Linux 2003[8]). Zumindest sollte man aber über das Einspielen aktueller Patches das Risiko minimieren, indem man bekannte Schwachstellen bestmöglich beseitigt.

Wir gehen davon aus, dass das Hauptinteresse eines Dritten darin besteht, Informationen über die Kommunikation und das Kommunikationsverhalten von Personen im Internet zu sammeln. Dabei handelt es sich sowohl um Kommunikationsinhalte als auch um die Metadaten zu diesen Kommunikationsverbindungen. Unter diesen Metadaten werden alle Informationen verstanden, die Rückschlüsse darüber zulassen, wer wann wie lange mit wem kommuniziert hat (Verbindungsdaten). Aus solchen Informationen lassen sich durchaus aussagekräftige Profile bilden.

2 Schutzmöglichkeiten

Je nach Anforderung gilt es, zur Wahrung der Privatsphäre die Kommunikationsinhalte und ggf. noch die Metadaten der Kommunikation im Internet dem Zugriff Dritter zu entziehen.

Zum Schutz der Kommunikationsinhalte verschiedener Dienste werden im Folgenden einige (kryptografische) Werkzeuge vor-

1 http://de.wikipedia.org/wiki/PRISM
2 http://de.wikipedia.org/wiki/Tempora
3 http://de.wikipedia.org/wiki/Direction_G%C3%A9n%C3%A9rale_de_la_S%C3%A9curit%C3%A9_Ext%C3%A9rieure (kürzer: http://preview.tinyurl.com/DGSEFrance)
4 AGB Yahoo Abs. 2.6 http://info.yahoo.com/legal/de/yahoo/mail/mailplus/mailplus_atos_new.html (kürzer: http://preview.tinyurl.com/YahooAGB)
5 heise online zu Skype am 17.05.2013: http://www.heise.de/security/artikel/Mehr-Fakten-und-Spekulationen-zu-Skypes-ominoesen-Link-Checks-1865370.html (kürzer: http://preview.tinyurl.com/HeiseSkype)
6 http://openjur.de/u/268440.html
7 http://www.bmi.bund.de/DE/Themen/Gesellschaft-Verfassung/Datenschutz/Informationelle-Selbstbestimmung/informationelle-selbstbestimmung_node.html (kürzer: http://preview.tinyurl.com/InfoSelbstbestimmung)

8 http://lkml.indiana.edu/hypermail/linux/kernel/0311.0/0635.html

Kai Jendrian

Security Consultant bei der Secorvo Security Consulting GmbH, lizenzierter Auditor und Mitglied im Board des deutschen OWASP Chapters. Beratungsschwerpunkte: Information Security Management und Anwendungssicherheit.
E-Mail: kai.jendrian@secorvo.de

gestellt. Zwar ist es das Hauptziel, unberechtigte Zugriffs auf die Inhalte der Kommunikation möglichst zu verhindern. Gleichzeitig aber sind für eine breite Akzeptanz solcher Werkzeuge eine gute Benutzerfreundlichkeit sowie das Vertrauen in eine fehlerfreie Implementierung unabdingbar (siehe Fehler in Tool salt: RSA mit public exponent 1[9] und Fehler in Crypto.cat[10]).

Der Beitrag gibt einige Hinweise auf konkrete Schutzmaßnahmen gegen Eingriffe in die Privatsphäre. Einen darüber hinaus gehenden systematischen risikobasierten Ansatz stellt die Electronic Frontier Foundateion (EFF)[11] mit dem „Surveillance Self-Defense-Project"[12] vor. Zur Einschätzung des Umgangs großer Dienstleister mit privaten Daten kann der jährliche Report „Who has your back?"[13] ggf. Hilfestellung leisten.

Schutz von Metadaten

Der Schutz von Kommunikationsmetadaten setzt den Einsatz von Anonymisierungsdiensten wie Tor[14], I2P[15], JAP[16] oder von speziellen VPN-Lösungen voraus. Durch kryptografische Verfahren wird bei diesen Ansätzen verschleiert, woher ein Datenpaket stammt. Grundsätzlich dienen die reinen Anonymisierungslösungen allerdings nicht dem Schutz der Kommunikationsinhalte und sollten bei Bedarf grundsätzlich immer im Zusammenspiel mit VPN-Lösungen eingesetzt werden. Es ist aber zu beachten, dass durch den Einsatz von Anonymisierungsdiensten der Datendurchsatz einer Kommunikationsverbindung in der Regel stark beeinträchtigt wird – dadurch sind nicht alle Dienste mit Anonymisierungsdiensten sinnvoll nutzbar.

Weitere Metadaten fallen beim täglichen Surfen an – auch bei der Nutzung von Anonymisierungsdiensleistern. Die Auswertung der Metadaten, die durch die Browser beim Surfen bereitgestellt werden, ist allgemein unter dem Begriff Tracking bekannt. Wer sich überzeugen möchte, welche Daten er alleine über einen einfachen Webseitenaufruf übermittelt, sollte sich mal bei Panopticlick[17] des EFF umsehen.

Um sich vor Tracking zu schützen, sollte man zunächst eine Willenserklärung abgeben, dass man nicht getrackt werden möchte. Das ist technisch gar nicht so schwer, wie mancher sich vorstellen wird – die gängigen Browser bieten hierzu die Implementierung eines IETF Standard-Entwurfs, den sogenannten Do-Not-Track-Mechanismus[18] an. Zusätzlich kann man in seinem Browser durch den Einsatz spezieller Erweiterungen[19] die Preisgabe einschränken. An dieser Stelle sei aber auch darauf hingewiesen, dass der Einsatz solcher Plugins nicht unumstritten ist[2021]. Das Verwischen von Spuren beim Surfen ist daher heute eine echte Sisyphos-Arbeit.

9 https://github.com/saltstack/salt/commit/5dd304276ba5745ec21fc1e6686a0b28da29e6fc (kürzer: http://preview.tinyurl.com/SaltPubExp)
10 http://tobtu.com/decryptocat.php
11 https://www.eff.org
12 https://ssd.eff.org
13 https://www.eff.org/who-has-your-back-2013
14 https://www.torproject.org/
15 http://www.i2p2.de/
16 http://anon.inf.tu-dresden.de/
17 https://panopticlick.eff.org/
18 https://www.eff.org/deeplinks/2012/06/how-turn-do-not-track-your-browser
19 https://www.datenschutzzentrum.de/tracking/schutz-vor-tracking.html
20 http://www.heise.de/tr/artikel/Die-Geister-die-ich-rief-1890700.html
21 http://www.heise.de/newsticker/meldung/Schwere-Vorwuerfe-gegen-Werbeblocker-AdBlock-Plus-1897152.html (kürzer: http://preview.tinyurl.com/HeiseAdblockPlus)
22 http://www.cs.berkeley.edu/~tygar/papers/Why_Johnny_Cant_Encrypt/OReilly.pdf
23 http://de.wikipedia.org/wiki/Transport_Layer_Security, siehe auch Esslinger/Müller, DuD 12/1997, S. 691-697.
24 https://www.ssllabs.com/projects/best-practices/
25 https://www.ssllabs.com/ssltest/index.html
26 https://www.trustworthyinternet.org/ssl-pulse/
27 https://www.eff.org/https-everywhere
28 https://community.qualys.com/blogs/securitylabs/2013/06/25/ssl-labs-deploying-forward-secrecy
29 https://en.wikipedia.org/wiki/Transport_Layer_Security#Applications_and_adoption

Schutz von Kommunikationsinhalten

Zum Schutz von Kommunikationsinhalten ist es unerlässlich, nach dem TNO-Prinzip („Trust No One!") zu agieren. In der Praxis bedeutet das den Einsatz von Werkzeugen, die für einen gewünschten Kommunikationskanal eine sichere Ende-zu-Ende-Verschlüsselung auf der Grundlage aktuell als sicher geltender kryptografischer Verfahren anbieten. Es hat sich allerdings über die Jahre gezeigt, dass der Einsatz von Ende-zu-Ende-Verschlüsselung viele Benutzer in der Praxis überfordert (siehe: Why Johnny can't encrypt[22]).

3 Tools zur Absicherung

Im Folgenden werden einige Werkzeuge vorgestellt, mit denen sich – wenn auch nicht immer vollständig ohne Verständnis der grundlegenden kryptografischen Ideen – ein verbesserter Schutz der Privatsphäre erreichen lässt.

SSL/TLS

Neben einzelnen Anwendungen, die mit Verschlüsselung ein verbessertes Schutzniveau bieten, hat sich SSL/TLS[23] zur Absicherung verschiedener Internet-Kommunikationskanäle durchgesetzt. Anbietern von Diensten wie der Bereitstellung von Webseiten und E-Mail kann an dieser Stelle nur dringend angeraten werden, diese Dienste bestmöglich mit SSL/TLS zu schützen[242526]. Auf der anderen Seite sollte auch jeder Nutzer diese Angebote bestmöglich nutzen. Für Web-Browser gibt es hier beispielsweise das nützliche Plugin HTTPS Everywhere[27], das bei den beliebten Browsern Firefox und Chrome für eine bestmögliche SSL/TLS-Nutzung sorgt. Aber gerade auch bei E-Mail-Clients ist in der Regel eine sichere Konfiguration durch Nutzung von SSL/TLS möglich – dazu sollte man die Hilfe des jeweiligen Clients zu Rate ziehen.

Vor dem Hintergrund der aktuellen Diskussionen sei an dieser Stelle darauf verwiesen, dass bei der Nutzung von SSL/TLS zukünftig ein Feature mit dem vielversprechenden Namen „Forward Secrecy"[28] eine wichtige Rolle spielt. Hierbei handeln Client und Server regelmäßig einen neuen symmetrischen Schlüssel aus, der von beiden Seiten vergessen wird und über den sich ein Angreifer aufgrund der Verfahren zur Aushandlung weder zeitnah noch nachträglich Kenntnis verschaffen kann. Zur verbreiteten Nutzung dieser Technik ist allerdings eine flächendeckende Implementierung[29] von TLS 1.2 auf Seiten der Server und Clients eine grundlegende Voraussetzung.

Es soll aber nicht verschwiegen werden, dass der korrekte Umgang mit Zertifikaten eine der größten Herausforderungen für die

Sicherheit bei der Nutzung von SSL/TLS darstellt. Benutzer sollten sorgfältig darauf achten, dass Sie per SSL/TLS mit einer vertrauenswürdigen Gegenstelle kommunizieren.[30]

E-Mail

Ein weit verbreitetes Kommunikationsmedium ist heute immer noch die E-Mail. Und immer noch wird ein Großteil der E-Mails nicht verschlüsselt. Dabei stehen schon seit vielen Jahren mit GnuPG[31] und mit S/MIME[32] standardisierte Schutzmechanismen zur Verfügung, die in vielen E-Mail-Clients standardmäßig oder durch Plugins realisiert sind[33].

Selbst für Webmail-Lösungen stehen Javascript basierte Werkzeuge zur Verschlüsselung mit GnuPG, wie z. B. GPG Javascript Plugins für Webmail[34], Mailvelope[35] oder WebPG[36] zur Verfügung. Allerdings sei an dieser Stelle darauf hingewiesen, dass auch der Einsatz von Javascript Encryption[37] nicht unumstritten ist. Zumindest sollte jeder, der auf die Idee kommt, sich an die Programmierung einer solchen Lösung zu wagen, eine verbreitete und durch viele Experten getestete Bibliothek wie bspw. die Stanfort Javascript Crypto Library[38] einsetzen.

Cloud-Storage

Der beste Schutz von Daten in der Cloud ist die Nutzung einer eigenen Cloud. Diesem Ansatz trägt das Projekt mit dem sprechenden Namen ownCloud[39] Rechnung. Hiermit ist es möglich, sich seine eigene Cloud zur Speicherung von Daten aber auch von Kalendern und Aufgaben aufzubauen.

Eine Alternative hierzu ist es, seine Daten in der Cloud zu verschlüsseln. Es ist allerdings sicherzustellen, dass die Verschlüsselung auf dem Client stattfindet und auch nur der Client sich im Besitz der notwendigen Schlüssel befindet („Trust No One"). Ein Werkzeug, das einen solchen Ansatz realisiert, ist das Werkzeug BoxCryptor[40], das plattformübergreifend für verschiedene Cloud-Anbieter zur Verfügung steht.

Statt dessen kann man auch verschlüsselte Datencontainer in der Cloud ablegen. Dieses Verfahren erlaubt zwar kein solch komfortables Arbeiten, bietet aber ebenfalls ein hohes Schutzniveau. Das freie Werkzeug TrueCrypt[41] erlaubt die Anlage und Nutzung solcher vollverschlüsselter Datencontainer, die sich dann in der Cloud speichern lassen.

Soziale Netze

Bei Daten in sozialen Netzen ist guter Rat teuer. Keines der verbreiteten sozialen Netze wie Facebook, Google+, Xing, LinkedIn etc. bietet eine Möglichkeit an, Daten durch Verschlüsselung nur einem bestimmten Empfängerkreis zugänglich zu machen. Gerade auch für den Anbieter des sozialen Netzes ist hierdurch grundsätzlich ein vollständiger Zugriff auf alle Daten technisch möglich.

Eine Alternative zu den etablierten Platzhirschen wäre die Nutzung von sozialen Netzen auf der Basis von Peer-to-Peer-Technologien[42], wie zum Beispiel friendica[43]. Diese Ansätze befinden sich heute aber alle noch in den Anfängen und genießen bisher keine breite Akzeptanz.

Instant Messaging

Ähnlich verbreitet wie Soziale Netzwerke sind heute Instant Messaging Plattformen. Dienste wie WhatsApp, iMessage, Facebook Messaging, Google Chat und andere Jabber/XMPP sind aus dem Alltag heute kaum noch wegzudenken.

Im Bereich des Instant Messaging gibt es aber im Gegensatz zu sozialen Netzwerken Schutzmöglichkeiten für die Privatspähre. Zum einen lassen sich durch das Off-the-Record-Protokoll (OT-

30 http://patrol.psyced.org
31 http://www.gnupg.org/
32 http://tools.ietf.org/html/rfc5751
33 http://wiki.kairaven.de/open/krypto/gpg/p/gpg1
34 http://openpgpjs.org/
35 http://www.mailvelope.com/
36 http://webpg.org/
37 http://www.matasano.com/articles/javascript-cryptography/
38 http://crypto.stanford.edu/sjcl/
39 http://owncloud.org
40 https://www.boxcryptor.com/de/boxcryptor-verschl%C3%BCsselung-f%C3%BCr-die-cloud-einfach-und-sicher
41 http://www.truecrypt.org
42 https://de.wikipedia.org/wiki/Peer-to-Peer
43 http://friendica.com/

R)[44] XMPP-basierte Chats durch den Einsatz von Clients mit direkter OTR-Unterstützung oder durch entsprechende Plugins absichern.[45] Eine solche Lösung bietet allerdings keinen Schutz davor, dass ein Dienst wie WhatsApp, das übrigens kein OTR untersützt, alle Einträge des lokalen Telefonbuchs auf den heimischen Server überträgt.

Eine sichere Alternative zu asynchronen Messaging-Diensten wie iMessage oder WhatsApp auf iPhone bzw. Android-Handy bietet die schweizer Software Threema[46]. Die App will Instant-Messaging sicher und datenschutzgerecht gestalten. Der Einsatz der offenen Krypto-Bibliothek NaCl[47] zu diesem Zweck dient als gutes Beispiel, kryptografische Verfahren nicht selbst zu implementieren und dabei über diverse Fallstricke zu stolpern (wie bspw. das oben erwähnte Crypto.cat).

Schutz von Zugangsdaten

Zu guter Letzt bleibt noch die Absicherung der Zugangsdaten zu genutzten Diensten. Hierbei handelt es sich heute – trotz aller damit verbundenen Nachteile – vor allem weiterhin um Passwörter. Aufgrund der inzwischen verfügbaren Werkzeuge und Rechenkapazität zum Brechen von Passwörtern sind vor allem zwei Dinge wichtig: Passwörter müssen eine hohe Qualität[48] besitzen und sollten auf keinen Fall mehrfach verwendet[49] werden.

Die Anforderungen, die daraus an die Benutzer erwachsen, sind von Menschen kaum noch zu erfüllen[50]. Aus diesem Grund sollten zum Schutz von Passwörtern Werkzeuge eingesetzt werden, die diese mit kryptografischen Mitteln absichern. Ein Ansatz hierfür ist die Verwendung eines Passwort-Safes, wie zum Beispiel die kostenlose Open Source Lösung KeePass[51], die auch plattformübergreifend verfügbar ist.

Alternativ ist gerade für Passwörter auf Webseiten die Nutzung von PwdHash[52] zur Ableitung von Passwörtern in Abhängigkeit von der besuchten URL eine attraktive Möglichkeit – inklusive freiem Schutz vor Phishing.

44 http://www.cypherpunks.ca/otr/
45 http://de.wikipedia.org/wiki/Off-the-Record_Messaging#Verf.C3.BCgbarkeit
46 http://threema.ch
47 http://nacl.cr.yp.to/
48 https://xkcd.com/936/
49 http://xkcd.com/792/
50 http://www.secorvo.de/publikationen/passwortsicherheit-fox-schaefer-2009.pdf
51 http://keepass.info
52 http://www.pwdhash.com

4 Fazit

Als Fazit bleibt festzuhalten, dass der Einsatz kryptografischer Techniken zum Schutz der Privatsphäre unverzichtbar ist. Es darf allerdings auch nicht verschwiegen werden, dass gerade die Verwendung von Kryptografie nicht in allen Fällen einfach ist – und ggf. sogar erst verdächtig[53] macht.

Eine weitere Strategie besteht darin, Dienste und Daten möglichst unter eigener Hoheit halten. In vielen Fällen ist die Wahrung der Privatsphäre heute nur durch strikten Verzicht auf viele Angebote – insbesondere soziale Netzwerke – möglich. Die Nutzung von Alternativen ist heute noch sehr unattraktiv, da die Verbreitung sehr gering ist und viele der eigenen Kommunikationspartner häufig gar nicht zu einer sichereren Kommunikation zu bewegen sind. Es sollte trotzdem jedem bewusst sein, dass wir bei der Wahrung der Privatsphäre über die Wahrnehmung eines Grundrechtes reden.

Das kann man wohl nicht besser deutlich machen, als eine der Kernaussagen des „Volkszählungsurteils“[54] des Bundesverfassungsgerichts vom 15. Dezember 1983, in der gesellschaftliche Rahmenbedingungen postuliert werden, die von dem Einzelnen gerade eben nicht verlangen, dass er sich seine Privatsphäre mühsam erkämpfen muss:

„Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.

Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“

53 http://www.guardian.co.uk/world/interactive/2013/jun/20/exhibit-b-nsa-procedures-document
54 BVerfGE 65, 1 (43): http://openjur.de/u/268440.html