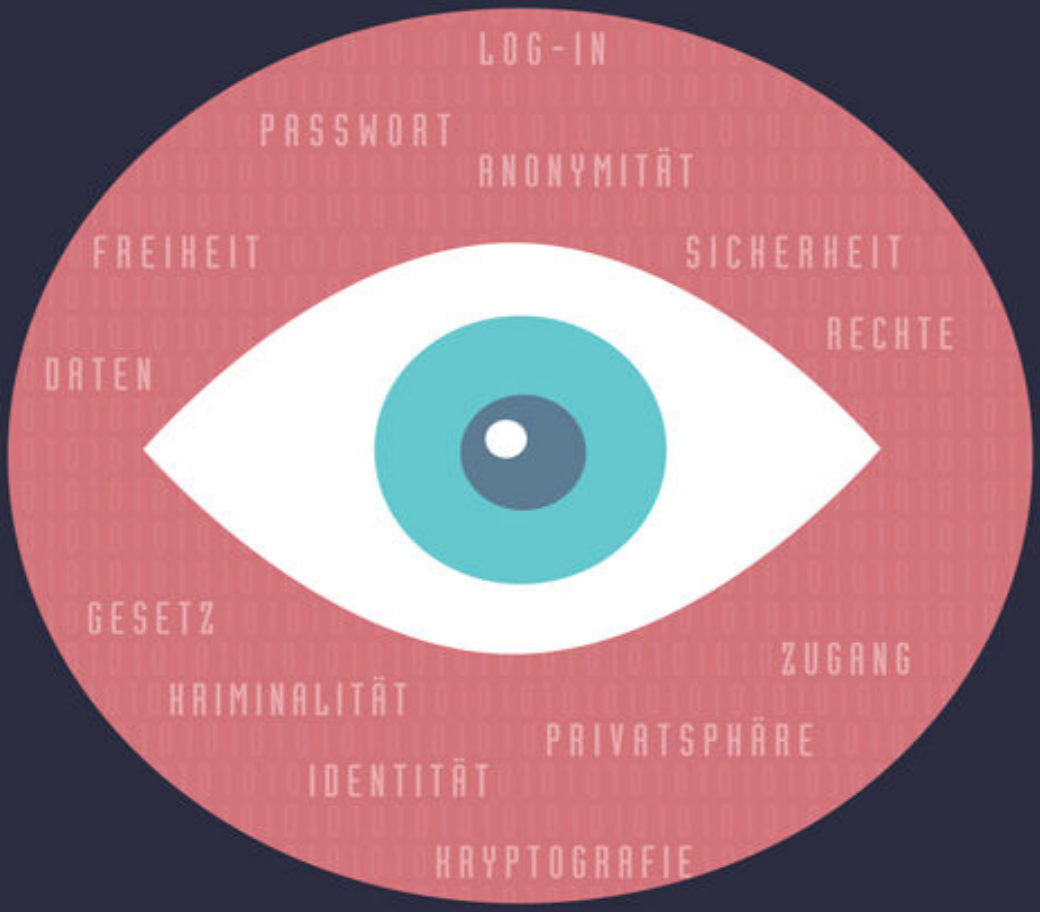
Christina Czeschik ◆ Matthias Lindhorst ◆ Roswitha Jehle

GUT GERÜSTET GEGEN ÜBERWACHUNG IM WEB

Wie Sie verschlüsselt mailen, chatten und surfen



SYBEX
A Wiley Brand

Johanna Christina Czeschik, Matthias Lindhorst und Roswitha Jehle

Gut gerüstet gegen Überwachung im Web – Wie Sie verschlüsselt mailen, chatten und surfen.

Fachkorrektur von Isolde Kommer

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.

1. Auflage 2016

Wir möchten Sie mit diesem Buch optimal unterstützen und freuen uns daher über Ihre Anregungen und Verbesserungsvorschläge. Notwendige Korrekturen veroffentlichen wir im Interesse aller Leser umgehend unter *www.sybex.de* und berücksichtigen sie bei der nächsten Auflage. Herzlichen Dank für Ihre Unterstützung!

Ihr Sybex-Lektoratsteam

lektorat@lektorat@wiley.com

Coverbild: bloomua/Fotolia.com

Korrektur: Harriet Gehring

Satz: inmedialo Digital- und Printmedien UG, Plankstadt

ePub ISBN: 978-3-527-69227-9

mobi ISBN: 978-3-527-69226-2

Print: ISBN: 978-3-527-76061-9

Vorwort

Liebe Leserinnen und Leser!

Wir danken Ihnen herzlich für den Kauf unseres Buches zum Thema »Sichere Kommunikation im und über das Internet«. Aber vor allem möchten wir Ihnen gratulieren! Gratulieren dazu, dass Sie nach all den Überwachungsskandalen und dem folgenden Schock in der digitalen Gesellschaft durchgehalten haben und sich mit dem vermeintlich so komplizierten Thema der Verschlüsselung beschäftigen möchten. Dazu, dass Sie nach dem Bekanntwerden der beängstigenden technischen Möglichkeiten von staatlichen Institutionen und Geheimdiensten nicht untätig die Hände auf die Tastatur gelegt haben, da »man eh nichts machen kann«, sondern dass Sie sich informieren und Gegenmaßnahmen ergreifen wollen.

Vielleicht haben Sie vor einem Geheimdienst sogar »nichts zu verbergen«, aber Sie fühlen sich dennoch unwohl dabei, dass Ihnen fremde Personen bei allem, was Sie »im Internet« tun, über die Schulter schauen können. Eventuell haben Sie auch erkannt, dass Sie ein großer wirtschaftlicher Schaden treffen kann, wenn Konkurrenten über Ihre geschäftlichen Absichten, Pläne oder internen Probleme informiert wären, wenn diese beispielsweise Einsicht in Ihre Termine, E-Mails, Chatprotokolle und wichtigen Dokumente hätten, die Sie in der »Cloud« gespeichert haben.

In der bisherigen Diskussion um die Überwachungsskandale lag der Schwerpunkt auf politischen Aspekten wie der Legitimation, dem Ausmaß und den Folgen staatlicher Überwachung. Die Auswirkungen von Wirtschaftsspionage (zum Teil staatlich gefördert, zum Teil durch kriminelle Organisationen) dürfen allerdings hierbei ebenfalls nicht vernachlässigt werden. Wirtschaftlicher Schaden durch Überwachung betrifft eine große Anzahl von Personen und Unternehmen: Sei es, dass Sie ein Berufsgeheimnis zu wahren haben (Anwaltskanzleien, Arztpraxen, Psychologen und Psychologinnen, Coaches oder Berater und Beraterinnen), sei es, dass Sie auf vertrauliche Informationen angewiesen sind (Journalisten und Blogger) oder dass Sie eine Firma haben, deren wirtschaftlicher Erfolg und Vorsprung vor der Konkurrenz auf innovativen Ideen oder Patenten beruht. Und nicht zuletzt können Kriminelle es auf uns alle als Privatpersonen abgesehen haben und erfreuen sich beispielsweise an abgefischten Konto- und Kreditkartendaten, E-Mail- und anderen Zugangsdaten.

Aber wir haben eine gute Nachricht für Sie: Egal, ob Sie sich vor einer angeblich legalen Überwachung durch den Staat oder einer illegalen durch Konkurrenten oder Kriminelle schützen wollen – die Verschlüsselung der eigenen Kommunikation ist keine Raketenwissenschaft – jeder kann sie mit etwas Aufwand umsetzen.

Wir richten uns daher in diesem Ratgeber an Leser, die keine IT-Spezialisten sind, sondern einfach mit einem Computer (und gegebenenfalls einem Smartphone) umgehen können. Umgehen können heißt, dass Sie einen Computer zum Schreiben von E-Mails und für die Internetrecherche und gegebenenfalls einen Chat wie Skype verwenden können und dass Sie bereits Programme aus dem Internet heruntergeladen und erfolgreich installiert haben. Mehr technisches Vorwissen brauchen Sie nicht! Systemadministratoren, Hobbymathematiker, Programmierer oder IT-Spezialisten sind nicht unsere Zielgruppe, aber natürlich herzlich eingeladen, Kritik zu üben und Vorschläge zu machen.

Noch einige Hinweise, bevor es losgeht:

Wir können Ihnen in diesem Buch nur die Empfehlungen und den Stand der Technik aus dem Jahr 2015 darstellen. Es kann also gut sein, dass mit der weiteren technischen Entwicklung (Stichwort Entwicklung von Quantencomputern) die heute angewandten Verschlüsselungsmethoden in Zukunft überholt sind und Ihre heute verschlüsselten E-Mails in einigen Jahrzehnten lesbar sein werden (ob diese E-Mails dann mehr als nur noch historischen Wert haben, müssen Sie selbst einschätzen).

Auch wenn Sie selbst auf neue Anwendungen gestoßen sind, die wir vorstellen sollten, wenn Sie einen Fehler entdeckt haben oder Lob, Anregungen und Kritik loswerden möchten, dann erreichen Sie uns unter: gutgeruestet@cryptocheck.de

Auf www.cryptocheck.de werden Sie mit der Zeit außerdem einige Zusatzmaterialien zu diesem Buch finden.

Wie im realen Leben, so gilt auch für die digitale Sicherheit, dass Sie mit entsprechendem Aufwand und Willen auch in Fort Knox einbrechen können. Das heißt, mit entsprechenden Mitteln und entsprechender Zeit wird man auch eine digitale verschlüsselte Kommunikation abhören können.

Die digitale Kommunikation ist ein relativ neues Medium – wir alle wissen schlichtweg immer noch zu wenig über die Technik, die längst unsere Welt bewegt und unseren Alltag prägt. Wir hoffen daher sehr, dass Sie nach der Lektüre dieses Buches die digitale Technik besser

verstehen und bewusstere Entscheidungen zu Ihrer digitalen Kommunikation treffen. Vielleicht versenden Sie einfache Einkaufslisten oder Grüße weiterhin unverschlüsselt per Mail oder im Chat, aber nicht (mehr) die Kreditkartenabrechnung vom letzten Urlaub, die Vorschläge für einen Bankkredit oder den ausgefüllten Gesundheitsfragebogen für die private Krankenversicherung.

Das Internet ist entgegen landläufiger Meinung kein Ort, den man betreten kann, sondern ein Medium, das von Menschen genutzt wird, zum Guten wie zum Schlechten – das heißt, es ist nichts anderes als Telefon, Radio oder Postkutsche. Die digitale Technik hat unsere Welt in den letzten Jahrzehnten stark verändert, sie macht aus uns vielleicht andere Menschen mit anderen, neuen Fähigkeiten – aber sie macht uns weder zu besseren (auch wenn das in der Euphorie der Anfangszeit des Internets manchmal nahegelegt wurde) noch zu schlechteren Menschen (auch das wird manchmal nahegelegt).

Am Ende ist wichtig, dass Sie in der Diskussion zur Überwachung und zur digitalen Kommunikation unterscheiden zwischen der objektiven Sicherheit (die es im Leben nie absolut gibt) und Ihrem subjektiven Sicherheitsgefühl. Die immer bestehende Lücke zwischen beidem können Sie nur mit Vertrauen füllen. Wir hoffen, dass wir mit diesem Buch das Wissen über die neuen Medien und damit auch das Vertrauen in die Technik vergrößern können und unsere Leser zu denjenigen gehören werden, die neue Technologien mit Selbstvertrauen, Mut und Neugier ausprobieren, aber auch mit gesunder Skepsis anwenden und kritisch bewerten.

In diesem Sinne wünschen wir Ihnen eine gute Lektüre und freuen uns auf den Dialog mit Ihnen unter der oben genannten E-Mail-Adresse und Webseite!

Christina Czeschik, Matthias Lindhorst, Roswitha Jehle

Essen und Berlin im Juli 2015

Danksagung

Wir bedanken uns bei den Mitgliedern der CCC-Erfas Essen und Düsseldorf, von denen wir (auch, aber nicht nur bei der Veranstaltung von Cryptoparties) viele wertvolle Anregungen erhalten haben. Unseren Lektorinnen Christine Siedle und Isolde Kommer sowie dem Lektor Christoph Kommer danken wir für ihre Anmerkungen und Verbesserungsvorschläge, durch die unser Buch an Klarheit und Lesbarkeit gewonnen hat. Sandra Bollenbacher, Marcel Ferner, Andrea Baulig und Hartmut Gante vom Wiley-Verlag danken wir für ihr Interesse an unserem Thema und die entschlossene Umsetzung des Projekts sowie für die unkomplizierte Zusammenarbeit. Nicht zuletzt danken wir auch unseren Familien und unseren Freunden für Verständnis und Unterstützung nicht nur, aber vor allem in den heißen Phasen vor der Fertigstellung des Manuskripts.

Kapitel 1 Warum es die Öffentlichkeit nichts angeht, dass Sie nichts zu verbergen haben

Die technische Entwicklung der letzten 25 Jahre ist Segen und Fluch zugleich. In Minuten können Sie sich von Ihrem Sofa aus Wissen aneignen, für das Sie sonst eine Bibliothek hätten aufsuchen müssen. Durch die Nutzung von Diensten wie Facebook, WhatsApp und Twitter halten Sie über große Entfernungen hinweg den Kontakt zu Freunden und Verwandten. Aber nicht nur unsere Erfahrungen aus der realen, »analogen« Welt und unser Bildungssystem, auch die Gesetzgebung hält mit der rasanten technischen Entwicklung kaum Schritt. Für viele rechtliche Fragestellungen der letzten Jahre existieren schlichtweg noch keine Gesetze. Wenn dann doch irgendwann entsprechende Regelungen gefunden werden, gelten diese meistens nur für das Land, in dem Sie leben, bestenfalls für ganz Europa. Das Internet kennt aber, wie Sie wissen, weder Grenzen noch Öffnungszeiten. Genau das macht es unter anderem zu einer der größten Errungenschaften der Menschheit. Dieser Umstand erfordert aber auch globale Regelungen, und diese zu treffen ist schwierig.

Das weltweite Netz ist sicher nicht der von vielen Politikern in Schnappatmung beschworene rechtsfreie Raum. Genau genommen ist es ein Medium (und kein Ort) und daher wertfrei. Die meisten auf elektronischem Wege verübten Straftaten sind weltweit als solche anerkannt und werden wie die Straftaten der »analogen« Welt entsprechend sanktioniert.

Wenn es allerdings um individuelle Ansichten wie beispielsweise Religion, Ethik, Moral, Ordnung, Höflichkeit und Privatsphäre geht, wird es kompliziert. Diese können ja bereits zwischen zwei Einzelpersonen sehr stark variieren. Was also in einem Land durch die freie Meinungsäußerung gedeckt ist, kann in einem anderen Land als Majestätsbeleidigung gewertet und hart bestraft werden. Die Grenzen dessen, was Sie als (digitale) Privatsphäredefinieren, also letztendlich die Entscheidung, mit wem Sie wann Informationen teilen, ist ebenfalls von Mensch zu Mensch verschieden. Ob Ihnen der Gedanke staatlicher Überwachung nun eine Heidenangst einjagt oder ob Sie regelmäßig Einträge Ihrer Krankenakte auf Facebook posten und auch sonst meinen, »nichts zu verbergen« zu haben, ist ganz allein Ihre Sache. Wichtig ist

lediglich, dass Sie frei entscheiden können, welche Informationen Sie zu welchem Zeitpunkt an wen weitergeben.

Die Realität sieht allerdings anders aus. In vielen Fällen treffen Sie diese Entscheidung gar nicht selbst, das tun andere für Sie – Unternehmen, Behörden, Geheimdienste und ungewollt sogar Ihre Freunde und Verwandten. Und wenn Sie ehrlich zu sich selbst sind, haben Sie sehr wohl etwas zu verbergen – und das ist auch gut so!

> »Wir tun nichts Böses, wenn wir Sex haben oder zur Toilette gehen. Wir verbergen nicht absichtlich etwas, wenn wir ruhige Orte aufsuchen, um nachzudenken oder ein Gespräch zu führen. Wir führen private Tagebücher, singen in der Abgeschiedenheit unserer Dusche, schreiben Briefe an heimliche Geliebte und verbrennen diese Briefe wieder. Privatsphäre ist ein grundlegendes menschliches Bedürfnis.«

Bruce Schneier[1]

Gründe, sich gerade jetzt mit sicherer Kommunikation zu beschäftigen, gibt es mehr als genug: Wahrscheinlich haben Sie die Geschichte des ehemaligen NSA-Mitarbeiters Edward Snowden in den Nachrichten verfolgt. Über die unrühmliche Rolle, die große Konzerne wie Google, Facebook und Microsoft bei der anlasslosen Überwachung von Millionen von Menschen spielten, wurde ebenfalls ausgiebig berichtet. Dieses Thema birgt interessante politische Hintergründe und Verflechtungen. Da dieses Buch allerdings ein praxisorientierter Ratgeber sein soll, wird es sich lediglich mit den technischen Konsequenzen auseinandersetzen, die Sie aus diesen Entwicklungen ziehen sollten.

1.1 Was Sie in diesem Buch finden werden (und was nicht)

Sie haben diese Seiten soeben vielleicht zum ersten Mal aufgeschlagen und fragen sich, ob Sie auch tatsächlich das finden werden, was Sie suchen. Während der Recherchen zu diesem Buch haben wir uns natürlich ein paar Gedanken darüber gemacht, was Sie wohl von uns erwarten und welche Vorkenntnisse Sie mitbringen. Außerdem war für uns wichtig, aus welchen Beweggründen Sie sich näher mit Ihrer digitalen Privatsphäre beschäftigen wollen.

Dieser Ratgeber wird Ihnen also definitiv weiterhelfen, wenn ein paar der folgenden Punkte auf Sie zutreffen:

- Sie benutzen regelmäßig oder zumindest gelegentlich einen Computer, und auf Ihrem Gerät läuft Windows, Linux oder Apples Betriebssystem OS X. Sie benutzen eventuell einen E-Mail-Desktop-Client, also ein E-Mail-Programm, auf Ihrem Rechner (wie Mozilla Thunderbird, Microsoft Outlook oder Mail auf einem Mac). Zudem haben Sie auch bereits das eine oder andere Programm selbst auf Ihrem Rechner installiert oder wissen zumindest, wie Sie das bewerkstelligen.
- Sie nutzen regelmäßig einen Internetzugang, surfen im Web, kaufen online ein oder nutzen Facebook oder andere soziale Medien, um mit Ihren Freunden in Kontakt zu bleiben.
- Sie haben eine oder auch mehrere E-Mail-Adressen, die Sie beruflich und/oder privat nutzen.
- Eventuell besitzen Sie auch ein Smartphone, versenden damit SMS oder E-Mails und haben vielleicht auch schon mal einen Messenger wie *WhatsApp* oder *Threema* ausprobiert oder die iMessage-Funktion auf Ihrem iPhone aktiviert.
- Sie haben in den Nachrichten immer wieder von flächendeckender Überwachung und Datendiebstahl gehört und wollen sich dagegen schützen.
- Sie sind weder Informatiker noch Experte für Kryptografie und möchten es auch nicht werden. Sie sind vielmehr daran interessiert, die in diesem Buch beschriebenen Maßnahmen praktisch anzuwenden, ohne deren Theorie bis ins kleinste Detail durchdringen zu müssen. Trotzdem möchten Sie sich die groben Zusammenhänge leicht verständlich erklären lassen.

Dieses Buch soll eine einfache und praxisorientierte Einführung in die wichtigsten Aspekte der digitalen Privatsphäre bieten. Daher wird es weder die Grundlagen der Computerbedienung erläutern noch Details zu kryptographischen Algorithmen und deren programmatischer Umsetzung erklären.

Kryptografie, also die Wissenschaft der Verschlüsselung, besteht zu großen Teilen aus komplexen mathematischen Prinzipien, mit denen ganze Lehrbücher gefüllt werden und die wir hier nicht im Detail besprechen möchten. Allerdings sollten Sie die zugrunde liegenden Mechanismen verstanden haben, um Anwendungsfehler zu vermeiden. Wir werden daher versuchen, Ihnen die nötigen Grundlagen anschaulich und leicht verständlich zu vermitteln. Wenn Sie sich dann doch dazu entschließen sollten, tiefer in die Materie einzusteigen,

existieren eine Menge guter Fachbücher zu den Themen Verschlüsselung und Computersicherheit, mit deren Hilfe Sie Ihre Kenntnisse ausbauen können.

1.2 Reden ist Silber – Ihre persönlichen Daten als Ware und Zahlungsmittel

Sie erinnern sich vielleicht noch an die Zeit, als man für ein Ortsgespräch 30 Pfennig in ein öffentliches Telefon werden musste? Wenn das Geld aufgebraucht war, brach die Telefonverbindung einfach ab. Als das Internet in den 1990er-Jahren dann schließlich massentauglich wurde, kamen die ersten Internetcafés auf. Hier konnte man Computer mit Internetzugang im Halbstundentakt mieten, um daran zu »chatten« oder E-Mails zu schreiben. Der Tarif lag anfangs um die 6 DM für eine halbe Stunde! AOL, in dieser Zeit wohl einer der größten Provider, berechnete ebenfalls einen Betrag pro Zeiteinheit und zusätzlich eine Gebühr pro Modemeinwahl.

Mittlerweile sind Internetzugänge deutlich billiger, die Übertragungsraten sind im Vergleich zu den damaligen Verhältnissen enorm gestiegen – trotzdem kostet ein solcher Anschluss noch immer Geld. Wenn Sie allerdings erst mal online sind, stehen Ihnen alle möglichen Dienstleistungen kostenfrei zur Verfügung.

Sie können, eingeloggt in Ihren Google- oder Facebook-Account, Freunden Nachrichten schicken, mit ihnen Bilder und Videos teilen oder die Beiträge der anderen kommentieren. Dabei lernen Algorithmen, welche Inhalte Sie bevorzugen und schlagen Ihnen beim nächsten Mal vielleicht noch lustigere Katzenvideos vor. Dass Unternehmen diese Dienste nicht aus Nächstenliebe anbieten, ist Ihnen dabei natürlich klar – ihre kostenlose Stadtteilzeitung finanziert sich ja auch aus Werbeanzeigen.

Die Geschäftsmodelle von Google und dem Anzeigenblatt Recklinghausen-Süd ähneln sich oberflächlich gesehen tatsächlich. Beide erzielenWerbeeinnahmen aus geschalteten Anzeigen – das eine Unternehmen online, das andere auf bedrucktem Papier. Google (oder ein vergleichbarer Dienst) hat bei der Vermarktung von virtuellen Werbeflächen aber einen entscheidenden Vorteil: Es kennt Sie, oder besser gesagt Ihre Vorlieben, genau. Der Inhalt Ihrer Suchanfragen, Ihres Terminkalenders, Ihrer E-Mails und Chat-Nachrichten, Ihre in einem Dienst gespeicherten Lesezeichen oder YouTube-Videos, die Sie mögen oder ausblenden – all

das zeichnet ein sehr genaues Bild davon, welche Art von Mensch, welche Art von *Kunde* Sie sind.

Unternehmen, die ihre Waren oder Dienstleistungen an den Mann, die Frau oder das Kind bringen wollen, haben ein entscheidendes Problem: Sie treffen zunächst auf eine große Masse von Menschen, die sich größtenteils nicht für ihre Produkte interessieren. Wie oft sind Sie selbst an Werbeplakaten für ein neues Automodell vorbeigelaufen, ohne diese wirklich zu sehen? Erst wenn Sie mit dem Gedanken spielen, sich ein neues Fahrzeug anzuschaffen, nehmen Sie entsprechende Plakate wirklich wahr und entscheiden sich für die Probefahrt eines bestimmten Modells. (Dieses Beispiel ist ein wenig vereinfacht – Werbung hat natürlich auch die Absicht, das Bedürfnis erst in Ihnen zu wecken.) Sie können sich sicher vorstellen, dass es sich für einen Autohändler nun nicht besonders lohnt, Klein-Mia aus der zweiten Klasse der städtischen Grundschule in regelmäßigen Abständen Plakatwerbung für das neueste Coupé vor die Nase zu hängen. Genauso nutzlos wäre Werbung bei der frischgebackenen Neuwagenbesitzerin, die gerade vom Hof des Vertragshändlers fährt.

Eine vielversprechende Zielgruppe für Autowerbung wären doch eher die Leute, die an der Bushaltestelle vor einer KFZ-Werkstatt warten – die aufmunternden Worte des Mechanikers noch im Ohr: »Die Scheibenwischer gehen noch, den Rest können Sie vergessen.« Oder?

Wechseln Sie nun einmal die Perspektive – stellen Sie sich vor, Sie sind nicht der Kunde, sondern arbeiten in der Marketingabteilung eines Automobilhändlers. Wo würden Sie Ihre Plakate aufhängen? Wenn Sie klug vorgehen, verlassen Sie sich nicht auf die Empfehlung von drei Leuten, die bloß ein Buch über Internetsicherheit geschrieben haben und keine Ahnung von Autos (oder Werbung) haben – dann könnten Ihnen nämlich mögliche Käufer entgehen. Vielleicht gibt es auch Aspekte, die Sie übersehen haben – eventuell hat Mia aus der zweiten Klasse sehr wohl ein Wörtchen mitzureden, welches Auto ihre Eltern anschaffen?

Ihre Werbung können Sie besser platzieren, wenn Sie handfeste Daten darüber haben, welche Menschen an Ihren Angeboten interessiert sind und wo Sie diese finden. Auf das Internet bezogen lautet die Frage dann logischerweise nicht mehr, an welcher Bushaltestelle Ihre potenziellen Autokäufer stehen. Vielmehr interessiert Sie nun, welche Webseiten sie besuchen, nach welchen Begriffen sie suchen, welche Produkte sie bereits gekauft haben und so weiter.

Spinnen Sie dieses Gedankenexperiment noch ein wenig weiter. Stellen Sie sich vor, Sie verkaufen Ihre Autos nicht nur in Recklinghausen-Süd, sondern über Ihre Website in ganz

Deutschland. Natürlich möchten Sie nun Anzeigen auf verschiedenen Internetseiten schalten, damit sie von Menschen wahrgenommen werden, die wahrscheinlich in nächster Zeit ein Auto kaufen wollen. Sie könnten nun einfach Anzeigenflächen auf allen deutschsprachigen Webseiten mieten, die Ihnen in den Sinn kommen, und diese dann wahllos zu verschiedenen Tages- und Nachtzeiten einblenden lassen – eine ziemlich teure Strategie.

Nehmen Sie an, Sie könnten tatsächlich feststellen, dass jemand, der eine Google-Mail-Adresse besitzt, zuvor Werbevideos und Testberichte über den neuen Golf auf YouTube angesehen und positiv bewertet hat. Zudem könnte diese Person vielleicht über Google nach »lohnt sich die Reparatur einer Zylinderkopfdichtung« gesucht und in E-Mails an die Schwester in Übersee davon erzählt haben, dass das alte Auto wohl bald den Geist aufgeben wird. Wäre es nicht sehr, sehr wahrscheinlich, dass besagte Person demnächst ein Auto kaufen möchte?

Da sich Autos nur recht schwer mit der Post verschicken lassen, möchten Sie Ihre Werbung nur in der Umgebung Ihres Autohauses einblenden – beispielsweise im Ruhrgebiet. Sie könnten in diesem Fall genau den Besuchern von Webseiten mit Google-Werbeflächen in den Feierabendstunden Ihre Werbung anzeigen lassen, die

- die neue Golf-Werbung mochten,
- ein Problem mit der Zylinderkopfdichtung haben und
- im Ruhrgebiet wohnen.

Sie bezahlen dafür einen überschaubaren Betrag an Google und werden hoffentlich bald viele Autos an glückliche Käufer loswerden.

Genau dieses Geschäftsmodell – die Nutzung von Userdaten zur zielgenauen Verbreitung von Werbung – ist der Grund, warum Google neben einigen anderen Unternehmen innerhalb weniger Jahre zu einem der größten und reichsten Internetkonzerne der Welt werden konnte.

Kehren Sie nun zu Ihrer eigenen Perspektive zurück. Sie sind wieder der private Internetnutzer, der Google für seine Standardinternetsuche benutzt, weil das in Ihrem Chrome- oder Firefox-Browser bereits so eingestellt war. Sie schauen YouTube-Videos und kommentieren diese vielleicht sogar. Sie nutzen Facebook, um sich mit Ihren Freunden zu verabreden und Ihnen die neusten Urlaubsfotos zu zeigen. Zusätzlich rufen Sie oft die großen bekannten Newsportale (bild.de, spiegel.de, zeit.de oder golem.de) ab und informieren sich über das allgemeine Weltgeschehen. Auf Ihrem Handy nutzen Sie regelmäßig die Google-Maps-Navigation, wenn Sie mit dem Auto unterwegs sind. Die meisten dieser Dienste kosten Sie

keinen Cent, da sie durch Werbung finanziert werden und teilweise Daten erheben, die ihnen helfen, diese Werbung noch gezielter zu steuern.

In diesem Geschäftsmodell stecken Sie also zunächst an keiner Stelle Geld ins System. Stattdessen werden die digitalen Fußabdrücke, die Sie hinterlassen, dazu verwendet, Bedürfnisse zu wecken oder diese vorauszusagen, um Ihnen zur richtigen Zeit die passende Anzeige zu präsentieren. Nüchtern betrachtet sind Sie also nicht der Kunde. Sie, beziehungsweise Ihre Aufmerksamkeit, sind die Ware. Sie bezahlen für diese Dienste nicht mehr die Preise der Deutschen Post oder von AOL wie in alten Zeiten, aber Sie bezahlen mit Ihren Daten – man könnte auch sagen, mit einem Teil Ihrer Freiheit. Wenn Unternehmen Ihnen kostenlose Dienste anbieten, tun Sie das ist den meisten Fällen nicht aus Selbstlosigkeit. Fragen Sie sich vor der Benutzung des jeweiligen Angebots selbst, welchen Vorteil das Unternehmen daraus zieht, dass Sie es nutzen.

Wie verdient das Unternehmen sein Geld? Sind Sie wirklich Kunde, oder doch eher Ware?

Versuchen Sie, bewusst zu entscheiden, ob Sie auf diesen Handel eingehen wollen oder nicht, und verzichten Sie einfach, wenn Ihnen Zweifel kommen.

Oft hört man, dass die Betreiber sozialer Netzwerke und anderer Dienste Nutzerdaten angeblich an Dritte verkaufen. Zum Zeitpunkt des Erscheinens dieses Buchs ist zumindest von Google und Facebook nicht bekannt, dass sie Nutzerdaten direkt verkaufen oder je verkauft haben. Im Gegenteil: Dieses Vorgehen wäre für die Konzerne kontraproduktiv, denn Daten über Nutzer sind ihr Kapitel und deren Auswertung ihr Geschäftsmodell. Wenn beispielsweise Facebook Ihre privaten Daten weiterverkaufen würde, wäre das in etwa so, als würde ein Bauer seine einzige Eier legende Henne verkaufen – denkbar, aber unklug.

Speziell bei Facebook gibt es allerdings Ausnahmen. Sogenannte Facebook-Apps, also Spiele oder andere Anwendungen, die in den Kontext von Facebook eingebettet werden können, unterliegen nicht der Kontrolle von Facebook selbst. Sie werden von Drittanbietern[2] bereitgestellt und kommunizieren über Schnittstellen mit dem sozialen Netzwerk. Erteilen Sie einer solchen App entsprechende Berechtigungen, kann diese beispielsweise auf Ihre Fotos zugreifen und sie auf einem Server irgendwo in der Welt ablegen. Weder Sie noch Facebook können dann noch auf die Daten zugreifen oder ihre Löschung erzwingen. In den Bedingungen, die für Facebook-Apps gelten, wird ein solches Verhalten zwar explizit untersagt, und seriöse Unternehmen bieten Ihnen die Möglichkeit, doch noch an Ihre

Daten zu kommen. Es gibt allerdings auch Drittanbieter, die sich einfach nicht daran halten und die so gewonnenen Daten wirklich weiterverkaufen.

Darüber hinaus müssen Sie wissen, dass Sie beim Hochladen eines Bildes Facebook das uneingeschränkte Nutzungsrecht (zum Beispiel für Werbung oder zur Auswertung der Bildinhalte) geben. Sie als Urheber behalten dabei Ihre Nutzungsrechte – Facebook hat diese aber nun ebenfalls.

Sie sollten daher bei jeder App, die Sie verwenden möchten, genau darüber nachdenken, auf welche Daten sie zugreifen kann und ob Sie dies tatsächlich gestatten wollen. Im Zweifelsfall heißt die Antwort eben einfach »nein«.

1.3 Das Recht, Dinge für sich zu behalten

Stellen Sie sich vor, Sie kommen von der Arbeit nach Hause, leeren den Briefkasten und stellen fest, dass Ihre Bank Ihnen die Kontoauszüge des letzten Monats geschickt hat. Nicht genug damit, dass Sie feststellen müssen, dass Sie Ihr Konto überzogen haben – der Umschlag ist bereits aufgerissen und jemand hat die Auszüge achtlos wieder hineingestopft. Wer auch immer sich an Ihrer Post zu schaffen gemacht hat, weiß jetzt, dass Sie diesen Monat zu viel Geld ausgegeben haben. Ihm ist nun bekannt, in welchen Supermärkten Sie mit Ihrer EC-Karte einkaufen waren und an welchen Geldautomaten Sie gewöhnlich Geld abheben. Außerdem weiß er oder sie nun, dass Sie offenbar häufiger mit Ihrem Geld nicht auskommen, weil Sie letzte Woche einen Kredit von 500 Euro an eine Privatperson zurückgezahlt haben (an Ihren Arbeitskollegen? Besten Freund? Erbonkel?).

Empört überlegen Sie, ob Sie sich zuerst Ihre Bank oder den Briefträger vorknöpfen, als Sie bemerken, dass Sie auch einen Brief von Ihrer Hausärztin bekommen haben. Auch er ist geöffnet. Nachdem Sie ihn gelesen haben, wissen Sie, dass sich nun noch mindestens eine andere Person außer Ihnen und Ihrer Hausärztin eine Meinung zu Ihrem Reizdarmsyndrom bilden konnte.

Bei beiden Beispielen sind Sie sicher unserer Meinung, dass es sich um ein unverschämtes Eindringen in Ihre Privatsphäre handelt und dass der Verantwortliche identifiziert und zur Rechenschaft gezogen werden sollte. Bestimmt würden Sie auch überlegen, wie Sie ähnliche Vorfälle in Zukunft verhindern können (vielleicht ist Ihr Briefkastenschlitz einfach zu groß, und Sie sollten einen neuen Briefkasten anbringen).

Was aber, wenn Sie nur gelegentlich mal bei dem einen oder anderen Brief das Gefühl hätten, dass jemand sich am Umschlag zu schaffen gemacht hat – dass zum Beispiel die obere Lasche etwas wellig ist – genau an der Stelle, wo sich der Kleber befindet. Oder wenn Ihnen in der Woche, nachdem Sie den Kredit an Ihren besten Freund zurückgezahlt haben, zum ersten Mal in Ihrem Leben eine Werbung für Verbraucherkredite ins Haus flattert, obwohl außer Ihrem Freund und Ihnen keiner etwas von der Leihgabe wusste? Würden Sie versuchen, Gegenmaßnahmen zu ergreifen, oder das ungute Gefühl immer wieder herunterschlucken und sich sagen, dass bisher ja kein handfester Schaden für Sie entstanden ist?

So oder so ähnlich ist momentan die Situation bei der internetbasierten Kommunikation. Wie leicht E-Mails und andere unverschlüsselte Informationen abgefangen werden können, hat sich mittlerweile herumgesprochen. Für Menschen mit entsprechendem technischem Know-how ist das Mitlesen einer unverschlüsselten E-Mail nicht viel schwieriger zu bewerkstelligen als das Lesen einer Postkarte für den Postboten.

1.3.1. Vorhersagen durch Statistik: der Blick in die Glaskugel

Auch Informationen, die Sie auf den ersten Blick für nicht so sensibel halten wie Ihren Kontoauszug oder einen ärztlichen Bericht, können weitreichende Schlüsse über Ihre Person erlauben, wenn sie miteinander in Zusammenhang gesetzt werden.

Berühmt wurde der Fall der US-amerikanischen Supermarktkette Target, die sich zum Ziel gesetzt hatte, Schwangerschaften ihrer Kundinnen aufgrund des Einkaufsverhaltens vorherzusagen (Charles Duhigg, »How Companies Learn Your Secrets«, New York Times, 16.2.2012) und dabei außerordentlich erfolgreich war. Routinemäßig hatte die Supermarktkette jedem Kunden, bei dem dies möglich war, eine Identifikationsnummer zugeteilt. Unter dieser Nummer speicherte das Unternehmen alle Informationen, die über diesen Kunden gewonnen werden konnten:

- Name und Adresse anhand der Kreditkarte oder durch die Teilnahme an Gewinnspielen oder Rabattaktionen
- demografische Informationen wie die Entfernung von der Wohnung bis zur nächsten Filiale
- Familienstand und ungefähres Einkommen aus Umfragen oder Gewinnspielen

- Einkaufsgewohnheiten durch die Einlösung von personalisierten Rabattgutscheinen und so weiter

Zusätzlich können, wenn einige Basisdaten bekannt sind, weitere Informationen über den jeweiligen Kunden oder die Kundin hinzugekauft werden, beispielsweise ein Kreditrating (entsprechend der SCHUFA-Auskunft in Deutschland). Welche Arten von Informationen genau in den Datenbanken des Konzerns gespeichert waren und sind, darüber wollte Target auf Nachfrage des Journalisten der New York Times keine Auskunft geben. Anhand dieser gesammelten Daten konnte Target nun relativ genau die Gewohnheiten einzelner Kunden vorhersagen – ob und in welchem Zeitabstand beispielsweise dem Kunden zugeschickte Rabattgutscheine eingelöst werden würden. Marketingaktionen konnten nun an diese Gewohnheiten angepasst und somit viel zielgerichteter durchgeführt werden.

Noch lohnenswerter, als die Gewohnheiten seiner Kunden zu untersuchen, ist es allerdings, diese Gewohnheiten zugunsten des Unternehmens zu steuern. Eine Zeit, in der die Gewohnheiten erwachsener Menschen auf den Kopf gestellt werden, sind Schwangerschaft und Geburt eines Babys – das sagt einem bereits der gesunde Menschenverstand, wurde aber auch von der Marktforschung bestätigt. Da frischgebackene Eltern mit Werbung und gut gemeinten Ratschlägen von allen Seiten überhäuft werden, entwickelten die Marketingspezialisten von Target die Strategie, werdende Eltern bereits vor der Geburt anzusprechen. Die Marktforschungsabteilung hatte beispielsweise festgestellt, dass werdende Mütter im zweiten Drittel der Schwangerschaft große Mengen an geruchsfreier Hautlotion und Wattebäuschen kaufen. Falls man sie dazu bewegen könnte, diese bei Target einzukaufen, könnte man sie zukünftig mit gezielter Werbung dazu bringen, auch andere Dinge des täglichen Lebens dort einkaufen. Ergebnis einer solchen Gewohnheitsbildung wären viele neue treue Kundinnen und Kunden.

Es existiert ein ganzes Fachgebiet, das sich entlang der Grenzen zwischen Informatik, Statistik und Wirtschaft bewegt. Es wird »Predictive Analytics« genannt und beschäftigt sich mit der Vorhersage der Zukunft, beispielsweise des menschlichen Verhaltens, aus großen Datenmengen.

Um erste Anhaltspunkte dafür zu gewinnen, wie man schwangere Kundinnen vom Rest der Kundschaft unterscheiden kann, verwendete Target zunächst die Daten von Kundinnen, die mehr oder weniger explizit zugegeben hatten, schwanger zu sein. Target bietet seiner

Kundschaft nämlich Baby-Shower-Listen an, also Listen von Geschenken, die werdende Eltern sich zur Geburt ihres Babys wünschen. Die Einkaufsgewohnheiten von Frauen, die eine solche Liste eröffnet hatten, also schwanger waren, konnten daher als Modell für alle schwangeren Kundinnen dienen. Die Daten zeigten zum Beispiel, wann die Kundinnen besagte Lotion in großen Mengen kauften und wann Vitaminpräparate, Waschlappen und andere Hygieneprodukte in ihrem Einkaufswagen landeten.

Der federführende Statistiker machte seinen Job so gut, dass er nicht nur die Schwangerschaft selbst, sondern auch den ungefähren Schwangerschaftsmonat vorhersagen konnte.

Um zu illustrieren, wie treffsicher seine Vorhersagen waren, erzählte der Statistiker dem Reporter der New York Times folgende Anekdote:

In einer Supermarktfiliale habe sich ein aufgebrachter Vater darüber beschwert, dass seiner Tochter, die noch zur High School ging, Rabattgutscheine für Windeln und Kinderwagen zugeschickt worden seien. Die bunten Werbebroschüren mit Fotos von glücklichen Babygesichtern würden seine Tochter womöglich dazu verleiten, schwanger zu werden, warf er der Geschäftsleitung vor. Man entschuldigte sich also bei ihm und versprach, man werde der Tochter zukünftig keine solchen Angebote mehr zuschicken. Einige Tage später rief der Geschäftsführer den Mann nochmals an, um sich ein weiteres Mal zu entschuldigen. Am anderen Ende der Leitung meldete sich ein sehr verlegener Vater: Er habe in der Zwischenzeit ein Gespräch mit seiner Tochter geführt, und sie sei tatsächlich schwanger.

1.3.2. Wenn die Glaskugel irrt

Scheinbar harmlose Informationen, die miteinander in Zusammenhang gebracht werden, erlauben also tiefe Einblicke in die Privatsphäre einzelner Menschen. Aus solchen Daten können potenziell aber auch fehlerhafte Rückschlüsse gezogen werden, die Ihnen dann unverschuldet zum Nachteil ausgelegt werden. Ein Beispiel dafür ist das Scoring-System, mit dem die SCHUFA und andere Unternehmen die Kreditwürdigkeit einer Person bewerten. Schon die Kombination einer Adresse, die in einer Gegend liegt, in der überdurchschnittlich viele Personen mit schlechter Kreditwürdigkeit wohnen, mit einem Vornamen, der auf eine eher junge Person hindeutet, kann zu einer schlechten Bonitätsbewertung führen (Sabine Hockling, »Manche Namen senken Scorewert für Kreditwürdigkeit«, Die Welt, 23.3.2013).

In dem Zeitungsartikel wird das Beispiel eines jungen Ingenieurs angeführt, der sich leichtsinnigerweise dazu entschloss, auf der Reeperbahn zu wohnen – diese Adresse, zusammen mit seinem männlichen Geschlecht und seinem jugendlichen Alter führte zu einer negativen SCHUFA-Bewertung. Und das, obwohl er noch nie in seinem Leben Schulden gemacht, geschweige denn diese nicht zurückgezahlt hatte. Eine negative SCHUFA-Bewertung wiederum kann bekanntlich dazu führen, dass der Abschluss eines Handyvertrages nicht mehr möglich ist, Kredite werden plötzlich nicht gewährt werden oder die dafür verlangten Zinsen unverhältnismäßig hoch sind, weil die Bank das Risiko eines Kreditausfalls falsch bewertet.

Wenn anhand solch prinzipiell harmloser Daten negative Schlüsse über Sie gezogen werden, kann sich das nicht nur empfindlich auf Ihre persönlichen Beziehungen und Ihren Geldbeutel auswirken. Es kann Sie auch ohne eigenes Verschulden in Konflikt mit der Polizei bringen (Holger Bleich, »Globaler Abhörwahn«, c't Magazin 16/2013).

Beispielsweise wurde 2012 ein Kanadier marokkanischer Abstammung, Saad Allami, festgenommen, als er seinen kleinen Sohn aus der Schule abholen wollte. Seine Wohnung wurde gestürmt und durchsucht, seiner Frau wurde mitgeteilt, sie sei mit einem Terroristen verheiratet. Seine Arbeitskollegen, die gerade auf einer Geschäftsreise in die USA waren, wurden mehrere Stunden lang an der Grenze zwischen den USA und Kanada festgehalten und über ihn befragt.

Als die kanadische Polizei (hinterher) den Fall genauer durchleuchtete, stellte sich Folgendes heraus:

Der Geschäftsmann hatte drei Tage zuvor die besagten Arbeitskollegen, die zu einer Messe nach New York reisten, per SMS angefeuert: Sie sollten die Konkurrenz »wegblasen«. Im Original verwendete er, da es sich hier um die französischsprachige Provinz Québec handelte, das Wort »exploser«. Den US-Behörden hatte dies offenbar in Kombination mit Allamis muslimischem Namen genügt, um einen geplanten terroristischen Anschlag zu vermuten und die kanadische Polizei um Amtshilfe zu bitten. Aufgrund dieses Vorfalls wurde Herrn Allami von der Provinzpolizei danach kein einwandfreies Führungszeugnis mehr ausgestellt, und er konnte daher seinen Beruf als Vertriebsleiter einer Telekommunikationsfirma nicht weiter ausüben. In der Zwischenzeit hat er die Provinzregierung deshalb auf 100.000 Dollar Schadenersatz verklagt.

Die ZEIT-Online-Redakteurin Tina Groll schrieb 2014 einen Artikel über ihren eigenen Fall (»Identitätsdiebstahl führt Jahre später zu falschen Forderungen«): Sie war 2009 das Opfer von Identitätsdieben geworden und hatte noch 2014 mit den Folgen zu kämpfen. Den Dieben war es anscheinend nur mithilfe von Grolls Namen und Geburtsdatum gelungen, Waren im Wert von mehreren tausend Euro an eine fremde Adresse zu bestellen, unter der sie die Waren dann entgegennahmen und weiterverkauften – natürlich ohne sie zu bezahlen. Die Mahnungen gingen dann an Frau Groll selbst, die dazu schreibt: »Mehr als 400 Arbeitsstunden und jede Menge Geld für Anwälte kostete es mich damals, meinen guten Namen wieder herzustellen.«

Doch mit dem damaligen finanziellen Schaden war die Sache noch nicht ausgestanden. Nach dem Vorfall hatte Groll sich für einen vierteljährlichen SCHUFA-Update-Service angemeldet, der sie alle drei Monate über Änderungen ihrer Kreditwürdigkeit informierte. Noch vier Jahre nach dem Vorfall, im Jahr 2013, fiel ihr Score plötzlich auf nur neun Prozent ab, weil ein Inkassounternehmen eine alte Forderung hatte eintragen lassen – ohne dass man sie selbst vorher darüber informiert hatte. Auch hier kostete es sie wieder Zeit und Geld, ihre Daten von diesem unberechtigten Eintrag bereinigen zu lassen.

Allen genannten Beispielen ist gemein, dass Informationen verwendet wurden, die für sich allein ganz harmlos wirken. Wie viele Flaschen Lotion Sie im Supermarkt kaufen, wie Ihr Vorname lautet oder der Inhalt einer etwas flapsigen SMS an die Arbeitskollegen sind laut dem gesunden Menschenverstand nichts, das Sie unbedingt geheim halten müssten, oder? Die Verkettung einzelner Informationen führt jedoch dazu, dass Unternehmen oder Behörden sich in der Lage fühlen, ihre eigenen Schlüsse zu ziehen. Im besseren (?) Fall sind dies richtige Schlüsse, die »nur« Ihre Privat- oder Intimsphäre verletzen. Es können aber auch falsche Erkenntnisse dabei herauskommen, die Sie in schlechtem Licht dastehen lassen und ganz handfeste negative Folgen für Sie haben.

1.3.3. Ein bisschen Privatsphäre, bitte!

Was ist das überhaupt, Ihre Privatsphäre? Dass bestimmte Informationen über eine Person schützenswert sind, fanden schon die Menschen im antiken Griechenland. So wurde beispielsweise etwa bereits 400 Jahre vor Christus im *Hippokratischen Eid* (benannt nach dem griechischen Arzt Hippokrates) festgehalten, dass ein Arzt das, was er »bei der Behandlung oder auch außerhalb der Praxis im Umgange mit Menschen sieht und hört, das man nicht

weiterreden darf«, »verschweigen und als Geheimnis bewahren« soll. Ähnliche Regelungen gab es vielleicht auch in früheren Kulturen in- und außerhalb von Europa. Der hippokratische Eid ist allerdings eines der ersten schriftlichen Zeugnisse, die uns über das Konzept des Datenschutzes überliefert sind. Im Laufe der Geschichte wurde die Privatsphäre dann mal mehr, mal weniger wichtig genommen. Im Mittelalter war es beispielsweise nicht ungewöhnlich, dass sich mehrere Menschen nicht nur einen Raum, sondern auch ein Bett teilten. Während des Absolutismus in Frankreich hielt der König sogar Audienzen ab, während er auf dem Klo saß (seit Einführung der Smartphones scheint dieser Trend eine gewisse Renaissance zu erleben). Auch das eigene Einkommen oder Vermögen geheim zu halten, wie es in vielen westlichen Ländern zum guten Ton gehört, ist in anderen Kulturen gar nicht möglich oder wünschenswert – beispielsweise, wenn Sie in einem Kibbuz in Israel leben. Und als aktuelles Beispiel gibt es in der westlichen Welt die Vertreter der »Post Privacy«-Bewegung, die die Geheimhaltung persönlicher Informationen im Internetzeitalter nicht nur für sinnlos halten, sondern als kontraproduktiv für die Meinungsfreiheit und den technischen Fortschritt ansehen.

Wenn mit der Privatsphäre also so unterschiedlich umgegangen wurde und wird, ist sie dann nicht irgendwie beliebig? Wir denken nicht, und zwar aus den folgenden drei Gründen:

1. Dass sich einige Menschen aus freien Stücken dazu entscheiden, in bestimmten Bereichen auf ihre Privatsphäre zu verzichten, ist kein ausreichender Grund, um dies allen anderen Menschen vorzuschreiben. Wir finden nicht, dass Sie Ihre persönlichen Daten geheim halten *müssen* – ob Sie es tun oder nicht, sollte aber Ihre Entscheidung sein und nicht die eines anderen.

2. Wenn Sie sich dazu entschließen, mit sechs anderen Menschen Ihr Schlafzimmer zu teilen, geben alle Beteiligten ein Stück ihrer Privatsphäre auf. Diese Situation ist eine grundlegend andere, als wenn eine für Sie gesichtslose Behörde entscheidet, Ihre E-Mails mitzulesen, ohne Sie vorher um Erlaubnis zu fragen. Hierdurch entsteht ein erhebliches Macht-Ungleichgewicht.

3. In der Geschichte beruhten Eingriffe in die Privatsphäre nicht immer auf Gegenseitigkeit, sondern erfolgten oft durch Autoritäten, die über mehr Ressourcen als eine einzelne Person verfügten. Daraus folgt dann noch folgender Punkt: Wie Sie in diesem Kapitel bereits gelernt haben, kann die Verknüpfung von scheinbar wertlosen Informationsschnipseln mithilfe der heute zur Verfügung stehenden Technologie weitreichendere Konsequenzen haben als jemals zuvor in unserer Geschichte. In vergangenen Jahrzehnten und Jahrhunderten wurden

normalerweise einzelne Menschen von einzelnen Menschen ausgespäht und ausgehorcht. Selbst das Abhören von DDR-Bürgern durch die Stasi war immer noch kaum automatisiert, sodass in einigen Akten vermerkt ist, welche weiteren Überwachungsmaßnahmen einer Zielperson an Personalmangel gescheitert sind (Interview mit Helmut Müller-Enbergs, DIE ZEIT, 15.10.2014). Heute können dagegen mit geringem Aufwand mehr Informationen über mehr Menschen als je zuvor gesammelt werden. Das hat zur Folge, dass zum einen ein viel größerer Anteil der Menschen in einem Land in den Fokus von Überwachung geraten kann und zum anderen über jeden dieser Menschen wesentlich mehr Daten gesammelt werden können. Wie wir weiter oben beschrieben haben, können ausreichend viele belanglose Details eine mindestens so große Gefahr für die Privatsphäre darstellen wie ein großer zusammenhängender Block sensibler Informationen.

Auch aufgrund der Erfahrungen, die ein Teil unserer Landsleute mit der Stasigemacht haben, hat die Privatsphäre in der deutschen Rechtsprechung einen hohen Stellenwert (jedenfalls theoretisch). Jeder Bundesbürger hat das »Recht auf informationelle Selbstbestimmung« – dies wurde vom Bundesverfassungsgericht 1983 im Volkszählungsurteil anerkannt. Aufgrund dieses Urteils wurde das schon seit 1977 bestehende Bundesdatenschutzgesetz noch einmal gründlich überarbeitet. Datenschutz ist in Deutschland jedoch eigentlich Ländersache, sodass es außer dem Bundesdatenschutzgesetz auch noch die Landesdatenschutzgesetze gibt. Das Bundesdatenschutzgesetz ist nur ein Sicherheitsnetz, nach dem man sich richtet, wenn ein bestimmter Sachverhalt nicht im jeweiligen Landesdatenschutzgesetz geregelt ist. Als erstes Bundesland hatte Hessen bereits 1970 ein Landesdatenschutzgesetz verabschiedet. Auch nach dem Volkszählungsurteil waren die Hessen wieder Vorreiter und novellierten ihr Gesetz bereits 1986, um dem neuen Grundrecht auf informationelle Selbstbestimmung zu genügen.

Geschützt sind gesetzlich vor allem sogenannte *personenbezogene Daten*. Das sind laut Bundesdatenschutzgesetz »Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person«. Eine bestimmte Person ist eine, die namentlich genannt wird. Bestimmbar bedeutet, dass die Person aufgrund der über sie gespeicherten Daten identifiziert werden kann, beispielsweise mittels Versichertennummer, Kundennummer oder Autokennzeichen. »Einzelangaben über persönliche und sachliche Verhältnisse« umfassen alle möglichen Lebensbereiche und müssen nicht einmal der Wahrheit entsprechen. Die sogenannte Artikel-29-Datenschutzgruppe der Europäischen Kommission hat

in ihrer Stellungnahme 4/2007[3] eine ganze Reihe von Beispielen für personenbezogene Daten zusammengestellt.

Beispiele für personenbezogene Daten

1. Berufliche Gepflogenheiten und Praktiken: Inhalt der Rezepte, die ein Arzt ausstellt, auch wenn der Patient anonymisiert ist (dies sind also auch personenbezogene Daten *des Arztes*)
2. Telefonbanking: Tonbandaufzeichnungen von Anweisungen, die ein Kunde seiner Bank am Telefon erteilt hat
3. Videoüberwachung: Bilder von Personen, wenn die Personen zu erkennen sind
4. Zeichnung eines Kindes: Bei einem Psychiater angefertigte Zeichnung eines Kindes, das seine Familie zeigt, enthält personenbezogene Daten des Kindes *und* der Familie
5. Wert einer Immobilie: Für sich genommen oder im Vergleich mit den Immobilienpreisen einer Gegend nicht personenbezogen, in Bezug auf einen bestimmten Besitzer aber schon, da von ihm beispielsweise die Steuer abhängt, die der Besitzer entrichten muss
6. Kundendienst-Scheckheft für ein Fahrzeug: Wenn durch eine Rechnung ein Zusammenhang zwischen Fahrer und Fahrzeug hergestellt wird, enthält das Scheckheft personenbezogene Daten über den Fahrer; in Verbindung mit dem für das Fahrzeug zuständigen Mechaniker und der Qualität seiner Arbeit enthält es personenbezogene Daten des Mechanikers

Das Bundesdatenschutzgesetz verbietet die »Erhebung, Nutzung oder Verarbeitung« Ihrer personenbezogenen Daten, wenn Sie kein Einverständnis dazu gegeben haben. Wir verwenden hier einfach den Begriff »Datenverarbeitung« für alle drei Fälle. Es gibt einige wenige Ausnahmen von diesem Verbot: Die wichtigsten sind Datenverarbeitung für Beschäftigungsverhältnisse und für eigene Geschäftszwecke. Ihr Arbeitgeber und der Onlineschuhhändler Ihres Vertrauens dürfen also Ihre Adresse und Bankverbindung in einer Personal- beziehungsweise Kundendatenbank speichern (damit sie das beim einen verdiente Geld beim anderen wieder ausgeben können), ohne dass Sie vorher explizit um Erlaubnis gefragt wurden.

Aber auch in den Fällen, in denen die Verarbeitung Ihrer personenbezogener Daten gesetzlich erlaubt ist, haben die Datensammler nicht freie Hand. Das Bundesdatenschutzgesetz schreibt nämlich *Datensparsamkeit* und *Datenvermeidung* vor. Das bedeutet, dass nicht mehr Daten

erhoben und gespeichert werden dürfen, als benötigt werden, um den Zweck der Datenverarbeitung zu erfüllen.

Wenn Sie online beispielsweise ein Paar Schuhe bestellen (oder realistischerweise besser drei und noch ein Paar Stiefel dazu, schließlich soll sich der Weg für den Postboten auch lohnen), benötigt der Versandhändler zwingend eine Versandadresse, an die er die Schuhe liefern kann. Wenn Sie einen Newsletter mit der Englischvokabel des Tages abonnieren, benötigt der Verfasser des Newsletters unbedingt Ihre E-Mail-Adresse. Wenn Sie online das Profihoroskop »Stationen des Lebens« von Erika Berger bestellen möchten, muss Frau Berger auch Ihr Geburtsdatum speichern dürfen (jedenfalls nehmen wir das als Horoskop-Laien einfach mal an).

Fragwürdig wird es allerdings, wenn der Schuhhändler Ihr Geburtsdatum speichern will oder wenn Sie bei der Bestellung des Englisch-Newsletters nach Ihrer Telefonnummer gefragt werden. In beiden Fällen werden Daten abgefragt, die zur Erfüllung des Auftrags nicht notwendig sind. Beide Firmen verstoßen gegen die Grundsätze der Datenvermeidung und Datensparsamkeit, und Sie sollten überlegen, ob Sie dies akzeptieren wollen oder Ihre Schuhe lieber woanders kaufen.

Auch wenn die Daten bereits erhoben wurden, haben Sie als Besitzer oder Besitzerin der personenbezogenen Daten (im Datenschutzgesetz und in der europäischen Datenschutzrichtlinie werden Sie »Betroffener« genannt) bestimmte Rechte:

1. Sie müssen über die Datenspeicherung informiert werden.
2. Sie dürfen den Inhalt der gespeicherten Daten erfahren.
3. Sie haben das Recht, falsch gespeicherte Daten zu korrigieren oder korrigieren zu lassen.
4. Sie dürfen die gespeicherten Daten sperren lassen.
5. Sie haben das Recht, die gespeicherten Daten löschen zu lassen.

Zum Sperren werden Daten mit dem Vermerk versehen, dass sie nicht weiter bearbeitet oder genutzt werden dürfen. Beim Löschen werden sie dagegen unwiderruflich zerstört.

Nach deutschem und europäischem Recht dürfen Sie die Löschung Ihrer Daten also jederzeit von einer Firma verlangen. Für außereuropäische Firmen gilt dies also erst einmal nicht. 2014 musste Google, das in Europa Zweigstellen unterhält, sich allerdings dem Europäischen Gerichtshof beugen und allen EU-Bürgern ermöglichen, Links zu ihren personenbezogenen

Daten aus dem Index seiner Suchmaschine entfernen zu lassen. Anlass für dieses Urteil des Gerichtshofes war die Klage eines Spaniers, der nicht akzeptieren wollte, dass noch 15 Jahre nach der Zwangsversteigerung seines Hauses dieser Sachverhalt in den Google-Suchergebnissen zu seinem Namen auftauchte.

Facebook hat seinen europäischen Sitz in Irland und unterliegt also auch den europäischen Datenschutzregelungen. Dem Unternehmen wurden bereits einige Datenschutzverstöße nachgewiesen (Thilo Weichert, »Datenschutzverstoß als Geschäftsmodell – der Fall Facebook«, Datenschutz und Datensicherheit 10/2012). Unter anderem wurden Einwilligungen zur Datenverarbeitung von Benutzern nicht oder nicht ausreichend eingeholt. Das Unternehmen ist der Pflicht zur vollständigen Löschung von Daten in vielen Fällen nicht nachgekommen. Bei anderen Gelegenheiten wurden die Rechte Dritter verletzt, da Facebook ihre personenbezogenen Daten verarbeitete, ohne dass sie überhaupt einen Facebook-Account besaßen.

Es lohnt sich also, sich zumindest einen groben Überblick über die Datenspeicherungs- und Löschpraktiken eines Anbieters zu verschaffen, bevor Sie sich dort einen Account anlegen. Sollten Sie schon einen solchen Zugang besitzen und mit der Verarbeitung Ihrer Daten nicht (mehr) einverstanden sein, zögern Sie nicht, Ihre gesetzlich festgeschriebenen Rechte in Anspruch zu nehmen.

1.4 Die vier Ziele der Computersicherheit

Jetzt haben wir Ihnen schon fast ein ganzes Kapitel lang damit in den Ohren gelegen, warum es wichtig ist, dass Sie Ihre Daten und Ihre Kommunikation vor fremdem Zugriff in Sicherheit bringen können. Aber was heißt das überhaupt, »Sicherheit«?

Informatiker beschäftigen sich schon eine ganze Weile mit der Frage, was Computersicherheit bedeutet und wie man diese herstellen kann. Aus den dabei formulierten Zielen haben wir die für Sie relevanten Punkte herausgepickt, um sie einmal genauer zu betrachten. Sie lauten:

- Authentizität
- Integrität
- Vertraulichkeit
- Verfügbarkeit

Angenommen, Sie haben bei einer Versicherungsgesellschaft eine Lebensversicherung abgeschlossen und Ihr Makler möchte Ihnen nun auf elektronischem Wege eine Bestätigung und die Rechnung zukommen lassen. Im Bezug auf die vier oben genannten Schutzziele möchten Sie für die E-Mail des Vertreters nun folgende Dinge gewährleisten:

Die *Authentizität* (also Echtheit) der E-Mail sollte sichergestellt sein, damit Sie wissen, dass die Nachricht tatsächlich von Ihrem Versicherungsvertreter kommt und nicht von irgendeinem anderen Absender, der nur vorgibt, für Ihre Versicherung zu arbeiten. Jemand könnte beispielsweise vortäuschen, Ihr Versicherungsvertreter zu sein, um an Ihre Bankverbindung und weitere persönliche Informationen zu kommen.

Wichtig für Sie ist auch die *Integrität* der Nachricht, also ihre Unversehrtheit. Das bedeutet, dass die Nachricht unterwegs nicht von einem Dritten geändert wurde. Sonst könnte zum Beispiel ein böswilliger Angreifer den Rechnungsbetrag und die Bankverbindung auf dem Schriftstück so ändern, dass Sie eine hohe Summe auf sein Konto überweisen, Ihre Versicherung aber leer ausgeht.

Auch die *Vertraulichkeit* der Nachricht liegt Ihnen und Ihrem Versicherungsagenten sicher am Herzen. Ihnen, weil Sie wahrscheinlich nicht öffentlich machen wollen, über welche Summe Sie eine Lebensversicherung abgeschlossen haben – Ihrem Versicherungsagenten vielleicht deshalb, weil er nicht möchte, dass die Konkurrenz zu gut über die Angebote seiner Firma informiert ist.

Zuletzt spielt auch die *Verfügbarkeit* der Nachricht noch eine gewisse Rolle, da Sie die Nachricht ja auch tatsächlich in dem Moment aus Ihrer Mailbox aufrufen wollen, in dem Sie sich am Sonntagabend vor Ihren Rechner gesetzt haben, um die Rechnung per Onlineüberweisung zu bezahlen.

In unserem Beispiel ist die Verfügbarkeit zwar nicht ganz so kritisch (wenn es nicht klappt, versuchen Sie es eben fünf Minuten später oder am nächsten Tag noch einmal) – in anderen Zusammenhängen ist sie aber mindestens so wichtig oder sogar noch wichtiger als die anderen Schutzziele.

Welche Ziele bei der Computersicherheit wichtig genommen werden und welche man eher vernachlässigen kann, hängt also ganz vom Anwendungsgebiet ab. Denken Sie beispielsweise an eine elektronische Fahrplanauskunft – da nur öffentlich zugängliche Daten verwendet werden, spielt die Vertraulichkeit keine Rolle, so lange keine persönlichen Daten der Kunden

gesammelt werden. Dafür ist aber die Verfügbarkeit umso wichtiger. Da es in diesem Buch hauptsächlich um Kommunikation geht (ob nun mit anderen Personen oder automatisierten Webdiensten), befassen wir uns vor allem mit den Schutzzielen Authentizität, Integrität und Vertraulichkeit.

Oft müssen bei der digitalen Kommunikation verschiedene Mittel eingesetzt werden, um die einzelnen Ziele der Computersicherheit zu erreichen.

Vertraulichkeit wird in der E-Mail-Kommunikation beispielsweise durch Verschlüsselung hergestellt, Authentizität und Integrität durch eine elektronische Signatur.

Es hat übrigens Vorteile, dass Sie die Schutzziele auch getrennt erreichen können. So ist es zum Beispiel mithilfe von Public-Key-Verschlüsselung (was das genau ist, erklären wir im nächsten Kapitel) möglich, dass Sie jemandem eine verschlüsselte, also vertrauliche, Nachricht zusenden können, ohne dass der Empfänger feststellen kann, dass Sie tatsächlich der Absender sind. Er kann also die Authentizität der Nachricht nicht beweisen. Das hat es Edward Snowden zum Beispiel ermöglicht, den Journalisten Glenn Greenwald und Laura Poitras erste Hinweise zum NSA-Skandal zukommen zu lassen, ohne ihnen gleich seine Identität zu verraten.

Auch der umgekehrte Fall ist denkbar: Vielleicht möchten Sie beweisen, dass Sie Urheber oder Urheberin eines Dokuments sind, das Sie der Öffentlichkeit zur Verfügung stellen wollen. In so einem Fall ist Authentizität erwünscht, Vertraulichkeit nicht.

1.5 Sicherheit vs. Bequemlichkeit

Wie Sie wissen, ist in den letzten Jahren bekannt geworden, dass der amerikanische Geheimdienst NSA (in Zusammenarbeit mit einigen Verbündeten) auch deutsche Staatsbürger ausspioniert hat. Berühmt wurde beispielsweise der Fall vom abgehörten Mobiltelefon der Bundeskanzlerin Angela Merkel. Selbstverständlich hat die NSA zuvor bei keinem der Betroffenen höflich angefragt, ob es wohl genehm sei, dass das eine oder andere Gespräch aufgezeichnet wird. Auch in der DDR war es nicht üblich, dass Stasi-Mitarbeiter zuvor die Erlaubnis der Leute eingeholt haben, deren Wohnungen abgehört werden sollten.

Ganz anders gehen dagegen die Datensammler bei Google, Facebook und anderen Internetgrößen vor. Hier wird keiner gezwungen, ein Profil anzulegen und damit seine Daten preiszugeben. Selbst wenn Ihnen an Ihrem Arbeitsplatz dringend nahegelegt wird, sich einen Google-Account einzurichten, damit Sie den firmeneigenen Google-Kalender einsehen können,

könnten Sie es einfach dabei bewenden lassen, den Zugang nur für diese eine Sache zu verwenden. Warum also nutzen so viele Leute Google-Dienste wie Mail, Maps und Drive oder präsentieren sich, ihren Nachwuchs und ihr Abendessen auf Facebook? Ganz einfach – weil es ihr Leben vereinfacht und unterhaltsamer macht.

Angenommen, Sie besitzen einen Google- und einen Facebook-Account. Sie verschicken Mails über Google Mail und nutzen regelmäßig Google Maps auf dem Smartphone zur Navigation zu Fuß und im Auto. Sie verabreden sich mit Freunden auf Facebook und teilen dort hinterher die Schnappschüsse vom Abend in Ihrer gemeinsamen Lieblingskneipe. Auf Twitter sind Sie auch angemeldet und setzen gelegentlich mal einen Tweet ab, der eine Ortsangabe enthält, um sich über den jüngsten Streik bei der Bahn aufzuregen und Leute zu warnen, die möglicherweise den gleichen Zug nehmen wollten.

Wenn Sie es absolut vermeiden wollten, Datenspuren zu hinterlassen, müssten Sie zunächst Ihre Mailadresse ändern. Dann müssten Sie sich eine Alternative zu Google Maps suchen, die vielleicht kostenpflichtig oder weniger komfortabel ist und die ganzen nützlichen Orte, die Sie in Google Maps eingespeichert haben, nicht kennt. Dann könnten Sie Ihren Google-Account kündigen. Ihren Facebook-Account müssten Sie ebenfalls stilllegen und vorher allen Ihren Freunden mitteilen, dass Sie in Zukunft nur noch telefonisch oder per E-Mail erreichbar sind (hoffentlich denken die dran, dass Sie ja eine neue Mailadresse haben!). Die Bilder, die Sie auf Facebook geteilt haben, und die Bilder Ihrer Freunde, auf denen Sie markiert sind, müssten Sie noch schnell herunterladen, denn mit dem Löschen des Accounts wären diese für Sie nicht mehr abrufbar. Das Gleiche gilt für die alten Nachrichten. Zum Beispiel die Nachricht, in der Ihre beste Freundin aus Grundschultagen Ihnen die ersten Fotos ihres Babys geschickt hat? Wäre doch zu schade. Wenn Ihre Freunde den nächsten Kneipenabend wie üblich in der entsprechenden Facebook-Gruppe ankündigen, denkt hoffentlich jemand daran, dass Sie ja gar nicht mehr mitlesen können, und ruft Sie rechtzeitig an.

Wenn Sie konsequent sein möchten, sollten Sie als Nächstes auch Ihr Smartphone abschaffen, welches dank des eingebauten GPS-Chips stets weiß, wo Sie sich gerade aufhalten. Genau genommen sollten Sie gar kein Handy benutzen, denn auch anhand der Mobilfunkzelle, in der Ihr Telefon sich befindet, kann Ihr Standort mehr oder weniger genau bestimmt werden. Ihre Freunde können Sie also nur noch auf dem Festnetztelefon anrufen. Besser, Sie kaufen sich wieder einen Anrufbeantworter – willkommen zurück in den 90ern!

Wir wollen Ihnen in diesem Buch nicht ein- oder ausreden, Ihren Facebook-Account zu löschen, um Ihre Privatsphäre zu schützen. Wenn Sie diesen Schritt gehen wollen, ist das ganz allein Ihre Entscheidung. Und auch, wenn Sie sich zwei Wochen nach Anschaffung Ihres Smartphones schon gefragt haben, wie Sie jemals ohne ausgekommen sind, ist der Besitz eines solchen Gerätes auch heute noch nicht überlebensnotwendig. Wenn Sie sich zutrauen, Ihr digitales Leben zu entrümpeln, dann möchten wir Sie ausdrücklich dazu ermutigen.

Wir plädieren aber sehr dafür, dass Sie sich in Sachen Datenschutz keine unrealistischen Ziele setzen – allzu drastische Maßnahmen halten meistens auch nicht lange vor. Wenn Sie sich nach der Lektüre dieses Buches dafür entscheiden, sogar ganz auf digitale Kommunikation zu verzichten, ist das durchaus eine respektable Entscheidung. Sie sollte aber nicht aus einer diffusen Angst heraus, sondern nach sorgfältigem Abwägen des Für und Wider gefällt werden. Wie so oft im Leben macht auch hier die Dosis das Gift. Ein vollständiger Abschied aus dem digitalen Leben ist unserer Meinung nach letztendlich genau so übertrieben wie »Post Privacy«[4].

Ein handfestes Beispiel für die Abwägung zwischen Sicherheit und Bequemlichkeit sind Passwörter. Es ist zwar lobenswert, dass viele Unternehmen mittlerweile eingesehen haben, dass Computersicherheit ein wichtiger Baustein ihrer allgemeinen Sicherheitsstrategie, ähnlich der Einrichtung einer ordentlichen Schließanlage, ist. In vielen Fällen nehmen diese Bestrebungen aber auch absurde Formen an. Plötzlich wird von Mitarbeitern erwartet, Passwörter aus Buchstaben, Zahlen und Sonderzeichen zu wählen, die eine bestimmte Länge haben. Zusätzlich müssen diese dann auch noch alle drei Monate (oder häufiger!) geändert werden. Sich ein derartiges Kennwort zu merken, ist schon für jemanden schwierig, dessen gesamter Arbeitsalltag sich um einen Computer dreht. Ein Mitarbeiter, der nur sporadisch Zugang zu einem Rechner benötigt, wird sich vor lauter Frustration vielleicht irgendwann das gerade gültige Passwort auf einem Zettel notieren und diesen unter der Tastatur »verstecken«. Es soll auch schon vorgekommen sein, dass besonders desillusionierte Nutzer sich das Post-it mit dem Kennwort einfach direkt an den Computermonitor klebten. Nicht selten werden Passwörter auch einfach weitergegeben, und dabei muss nicht, wie im XKCD-Comic zu dem Thema, immer Zwang im Spiel sein:

Abb. 1.1 Mit freundlicher Genehmigung von Randall Munroe, xkcd.com (Quelle:https://xkcd.com/538/)

Sie sehen, dass gut gemeinte, aber zu hoch gesteckte Ziele sich in der Internetsicherheit auch in ihr Gegenteil verkehren können. Oft wird unterschätzt, wie faul und vergesslich Menschen sind. »Faul« ist in diesem Fall übrigens nicht despektierlich gemeint – im Gegenteil, es ist klug, seine Kraft auf die Dinge zu konzentrieren, die man selbst für wichtig hält, und Passwortsicherheit steht für die allermeisten Leute nun mal nicht auf Platz 1 dieser Liste. Da es hier um die Sicherheit Ihrer Daten geht und nicht der irgendeines Unternehmens, müssen Sie also nicht das Verhalten Ihrer Mitarbeiter korrekt einschätzen. Sie sollten sich lediglich Ihrer eigenen Macken bewusst sein, was übrigens schon schwer genug ist. Wenn Sie irgendeine Maßnahme treffen, um Ihre Daten besser zu schützen, gestehen Sie sich eine Probezeit zu, um sich an die neuen Handgriffe und Klicks zu gewöhnen. Wenn Sie merken, dass Sie ein neues Tool gar nicht benutzen oder schärfere Sicherheitsumstellungen regelmäßig umgehen, dann müssen Sie entweder ein ernsthaftes Selbstgespräch führen und sich zur Ordnung rufen oder nach einer benutzerfreundlicheren Lösung suchen.

[1] http://www.schneier.com

[2] Das können sowohl Unternehmen als auch Gruppen oder Einzelpersonen sein.

[3] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf

[4] Philosophie und die dazugehörige gesellschaftliche Bewegung, die Privatsphäre für ein überholtes Konzept hält; siehe auch Glossar

Kapitel 2 Grundregeln und Hintergründe der digitalen Privatsphäre

Im vorangegangenen Kapitel haben Sie erfahren, was digitale Privatsphäre ist und wie andere Menschen diese gewollt oder ungewollt verletzen können. Völlig zu Recht fragen Sie sich jetzt wahrscheinlich, wie Sie sich gegen derartige Eingriffe schützen können.

2.1 Grundlagen der Kryptografie

Zunächst möchten Sie sicherstellen, dass niemand Ihre Nachrichten ohne Ihr Wissen und ausdrückliche Erlaubnis liest oder sogar verändert. Kryptografie (von griechisch »geheim schreiben«) ist hierfür das Mittel der Wahl. Um es richtig einzusetzen, müssen Sie kein Mathematikgenie sein, sollten aber ein paar grundlegende Dinge über Verschlüsselung wissen.

2.1.1. Bob trifft Alice

Wenn von Kryptografie gesprochen wird, geht es meistens um zwei Personen, die miteinander Nachrichten austauschen wollen, die kein Dritter mitlesen soll. Damit wir nicht durcheinandergeraten, nennen wir die Absenderin »Alice« und den Empfänger »Bob«. In vielen Szenarien kommt noch eine dritte Person hinzu, die Alices Botschaften mitlesen will – sie trägt den Namen »Eve« (von englisch »eavesdropper« = Lauscher).

Hintergrund

Die Namen Alice und Bob wurden in diesem Zusammenhang das erste Mal von Ronald L. Rivest in einem 1977 veröffentlichten Artikel über das *RSA-Kryptosystem* in der Fachzeitschrift »*Communications of the ACM*«, geprägt. Wie Sie sehen, sind die Anfangsbuchstaben auch die ersten Buchstaben des Alphabets und entsprechen dem *A*- und *B-Teilnehmer* eines Kommunikationssystems.

Der A-Teilnehmer ist in diesem Sinn derjenige, der die Kommunikation (z. B. Anruf oder Nachricht) initiiert. Das Ziel wird B-Teilnehmer genannt. C- und D-Teilnehmer sind weitere Stellen, die in diese Kommunikation involviert werden.

Neben Alice, Bob und Eve kennt man noch weitere fiktive Personen:

- *Carol*, *Carlos* oder *Charlie* sind *C-Teilnehmer* eines Kommunikationssystems.
- *Chuck* ist ebenfalls ein C-Teilnehmer, der im Gegensatz zu den anderen schlechte Absichten verfolgt.
- *Craig* ist ein Passwort-Cracker. Dieser Name findet meistens Verwendung im Zusammengang mit Angriffen auf gespeicherte Passwortdaten.
- *Dan* oder *Dave* sind *D-Teilnehmer* eines Kommunikationssystems.
- *Mallet* oder *Mallory* sind bösartige Angreifer, die im Gegensatz zu Eve aktiv in die Kommunikation eingreifen können. Sie haben die Absicht, Nachrichten in ihrem Wortlaut zu verändern. Es ist schwieriger, ein System gegen Mallet oder Mallory zu schützen als gegen Eve.
- *Peggy* (englisch »prover«) oder *Victor* (englisch »verifier«) sind Zeugen, die beweisen können, dass eine Kommunikation stattgefunden hat.
- *Trent* (englisch »trusted entity«) ist ein vertrauenswürdiger Dritter, beispielsweise ein Notar.

Eine Nachricht von Alice an Bob kann im *Klartext*, also in menschenlesbarer Form vorliegen. Ihr verschlüsseltes Pendant bezeichnet man als *Geheimtext*. Ein Verfahren zur Verschlüsselung wird auch als *Chiffre* oder *Code* bezeichnet.

Alice, Bob und Eve werden Ihnen im Folgenden dabei helfen, nachzuvollziehen, wie verschiedene Chiffres zur Umwandlung von Klar- in Geheimtext und zurück funktionieren.

2.1.2. Symmetrische Verschlüsselung – ein Tresor für Nachrichten

Eine der einfachsten Arten der Verschlüsselung ist es, jeden Buchstaben durch einen anderen zu ersetzen. In diesem Fall bietet es sich natürlich an, für jeden zu ersetzenden Buchstaben ein Zeichen zu wählen, das in einem bestimmten Abstand weiter hinten oder vorne im Alphabet steht. Da schon die alten Römer auf diese Art geheime Nachrichten ausgetauscht haben sollen, wird diese Methode als Caesar-Chiffre (oder auch als Verschiebechiffre) bezeichnet. Der Schlüssel, mit dem eine so codierte Nachricht wieder lesbar gemacht werden kann, entspricht also der Anzahl der Zeichen im Alphabet, um die der Geheimtext verschoben werden muss, um den Klartext zu erhalten. Hier ist ein kleines Beispiel:

Bei einem Schlüssel von 2 passiert Folgendes:

a → c
b → d
c → e
..
y → a
z → b

Wichtig ist, dass bei der Caesar-Chiffre die Schlüssel zum Ver- und Entschlüsseln der Nachricht gleich sind. Wenn Alice also jeden Buchstaben um sieben Zeichen zum Ende des Alphabets hin verschoben hat, muss Bob diesen wieder um sieben Zeichen in die entgegengesetzte Richtung schieben, um ihre Nachricht lesen zu können.

Nehmen Sie einmal an, dass Sie Alice ziemlich genau kennen und daher wissen, dass sie ihre Nachrichten am liebsten mit dem Schlüssel 5 codiert.

Können Sie ihre folgende Nachricht entschlüsseln?

InjLjifspjsxnsikwjn
bjwpfssxnjjwwfyjs?
Xnjkqnjmjsatwgjn
bnjsfjhmyqnhmjXhmfyyjs.
PjnsRjsxhmpfssxnjbnxxjs,
pjnsOfjljwjwxhmnjßjs
jxgqjngjyifgjn:
injLjifspjsxnsikwjn.

Wenn beim Chiffrieren der Nachricht lediglich das Alphabet ohne Sonderzeichen und Zahlen verwendet wurde, kommen nur 26 mögliche Schlüssel in Frage. Sie brauchen den Schlüssel daher gar nicht zu kennen, ein derartig codierter Geheimtext kann durch einfaches Durchprobieren der einzelnen Schlüssel in realistischer Zeit von Hand geknackt werden. Voraussetzung hierfür ist lediglich, dass Eve weiß, dass Alice und Bob eine Verschiebechiffre zum Codieren ihrer Nachrichten verwenden.

Das aufwendige Durchprobieren der einzelnen Schlüssel ist in der Regel nicht einmal notwendig: Am einfachsten ist es, beim Knacken des Codes von kurzen Wörtern auszugehen, die wahrscheinlich häufig im Geheimtext auftauchen.

Schauen Sie sich den folgenden mit einer Verschiebechiffre verschlüsselten Text an:

Jre ervgrg bf bfcnrg qhepu Anpug haq Jvaq?
Rf vfg qre Ingre zvg frvarz Xvaq.
Re ung qra Xanora jbuy va qrz Nez,
Re snßg vua fvpure, re uäyg vua jnez.

Es fällt auf, dass sich am Anfang der Zeilen zwei bis vier jeweils ein Wort befindet, das nur aus zwei Buchstaben besteht. Wenn Eve weiß (oder vermutet), dass der Ursprungstext in deutscher Sprache verfasst wurde, kommen hierfür nur wenige Wörter der deutschen Sprache in Frage, zum Beispiel:

1. *Im + In*
2. *Er + Es*
3. *An + Ab*

Da die beiden letzten Buchstaben »f« und »e« der verschlüsselten Wörter im Alphabet nebeneinander stehen, scheidet das dritte Wortpaar *An* und *Ab* von vornherein aus, weil »n« und »b« nun mal nicht direkt aufeinanderfolgen. Eve muss jetzt also nur noch die beiden anderen Möglichkeiten ausprobieren und stellt fest, dass sich beim ersten Wortpaar *Im* und *In* kein eindeutiger Wert für die Verschiebung bestimmen lässt, da der Abstand zwischen »r« und »i« 9, der Abstand zwischen »m« und »e« bzw. »n« und »f« jedoch 18 ist. Beim zweiten Wortpaar *Er* und *Es* ist die Verschiebung hingegen in allen Fällen 13, sodass das der richtige Schlüssel ist.

Mit wenigen Tricks kann ein Angreifer also die Anzahl der Schlüssel, die er ausprobieren, und damit die Zeit, die er dafür aufwenden muss, um das 13-Fache reduzieren. Diese Tatsache spricht nicht gerade für die Sicherheit der hier verwendeten Chiffre.

Die im Beispiel verwendete Verschiebung nennt sich übrigens *rot13* (siehe nächster Kasten). Der Klartext lautet also:

Wer reitet so spät durch Nacht und Wind?
Es ist der Vater mit seinem Kind.
Er hat den Knaben wohl in dem Arm,
Er fasst ihn sicher, er hält ihn warm.

Die Anzahl der Versuche, die ein Angreifer unternehmen muss, um einen Geheimtext zu entschlüsseln, entscheidet also darüber, wie sicher oder unsicher der verwendete Code ist. Dabei gilt: Je mehr Anläufe nötig sind, um den richtigen Schlüssel zu erraten, desto sicherer ist

die verwendete Verschlüsselungsmethode. Die Anzahl der nötigen Versuche hängt unter anderem mit der *Länge* des verwendeten Schlüssels zusammen.

Um Alices und Bobs Kommunikation besser vor Eve zu schützen, muss also ein längerer Schlüssel her. Um das zu erreichen, könnte man beispielsweise die Buchstaben des zu verschlüsselnden Textes abwechselnd um 2, 5 und 9 Zeichen verschieben.

Aus dem Wort »Alice« würde dann:

A → C (2 Zeichen)
l → q (5 Zeichen)
i → r (9 Zeichen)
c → e (2 Zeichen)
e → j (5 Zeichen)

Der Geheimtext zu »Alice« ist also »Cqrej«.

Exkurs

Die Caesar-Chiffre mit dem Schlüssel 13 wird auch als rot13 bezeichnet, »rot« steht hier für Rotation. Sie können sich dazu zwei Rädchen vorstellen, wie bei einem Zahlenschloss, nur mit Buchstaben statt Zahlen. Wenn die Rädchen zuerst den gleichen Stand haben (z. B. beide auf »A« stehen) und Sie dann eines um 13 Stellen rotieren, zeigt das zweite Rädchen die rot13-Verschlüsselung des ersten Rädchens.

rot13 hat gegenüber anderen Caesar-Chiffren die Besonderheit, dass eine zweite Verschlüsselung des Geheimtextes wieder zum Klartext führt, da das Alphabet 26 Zeichen lang ist und man bei einer Rotation von 26 wieder im Ausgangszustand ankommt. Wenn Sie dagegen einen Text, der mit rot7 verschlüsselt ist, nochmal mit rot7 verschlüsseln, landen Sie bei rot14 und keineswegs beim Ausgangstext (zum Entschlüsseln hätten Sie die Rotation rückgängig machen müssen).

Scherzhaft wird in der Informatikerszene auch manchmal von der Verschlüsselungsmethode rot26 gesprochen. Die Pointe ist ungefähr die gleiche, als wenn man von jemandem spricht, der eine »360°-Wendung« gemacht hat. (Auch den letzten Satz hätten wir übrigens mit rot13 verschlüsseln können, falls Sie zu den Leuten gehören, die es schrecklich finden, wenn man Witze erklärt.)

Im Internet wird rot13 manchmal verwendet, um Dinge zu verschlüsseln, die nicht geheim sind, aber nicht aus Versehen gelesen werden sollen. Beispielsweise könnte in einem Diskussionsforum über eine bestimmte Fernsehserie das Ende der Staffel bereits von Leuten verraten werden, die die Serie im amerikanischen Original gesehen haben. Wenn diese den Leuten, die auf die deutsche Ausstrahlung warten, den Spaß nicht verderben wollen, könnten sie alle Informationen, die das Ende verraten würden, in rot13 posten – für Leute, die diese dann bewusst lesen wollen, ist das leicht zu entschlüsseln.

Der auf diesem Wege erstellte Geheimtext zum vorherigen Textbeispiel sähe dann so aus:

Yja tjrvjc ut bräy mwwlj Sjemc wsm Ynwf?
Jb kxc fja Xfcgw vky bgnwgr Tksm.
Gw qcy mgs Tpfkgs fqmu ks mgr Jtr,
Nt kjßv nqp xremnt, ja jäqc kmw yfao.

Wie die einfache Verschiebechiffre ist auch diese Abwandlung ein *symmetrisches Verschlüsselungsverfahren*, die Schlüssel zum Codieren und Decodieren der Nachricht sind also identisch – in diesem Falle 2-5-9.

Um sich das Ganze zu verdeutlichen, können Sie sich die Chiffre als einen Tresor (oder verschlossenen Briefumschlag, wie in unserem Schema zur symmetrischen Verschlüsselung, Abbildung 2.1) vorstellen, in dem Alice ihre Nachricht deponiert und ihn mit einem Schlüssel abschließt. Der Schlüssel muss dann in irgendeiner Weise zu Bob gelangen, der mit seiner Hilfe den Tresor wieder öffnen und die Nachricht entnehmen kann.

An einer Verschiebechiffre mit drei verschiedenen Zahlenwerten hat die nur mit Bleistift und Papier ausgestattete Eve schon wesentlich länger zu knacken als an der einfachen Caesar-Chiffre.

Wenn sie alle 26 × 26 × 26 (also 17.576) Kombinationen durchgeht, kostet sie das, bei einem optimistisch geschätzten Tempo von einer Minute pro Kombination, über 292 Stunden. Schlaf, Essen und Toilettenpausen nicht mitgerechnet, entspricht das etwa zwölf Tagen. Dies scheint für eine sehr motivierte Eve (die für die nächsten zwei Wochen sonst nichts Wichtiges vorhat) noch machbar – aber was, wenn wir die Schlüssellänge noch weiter erhöhen?

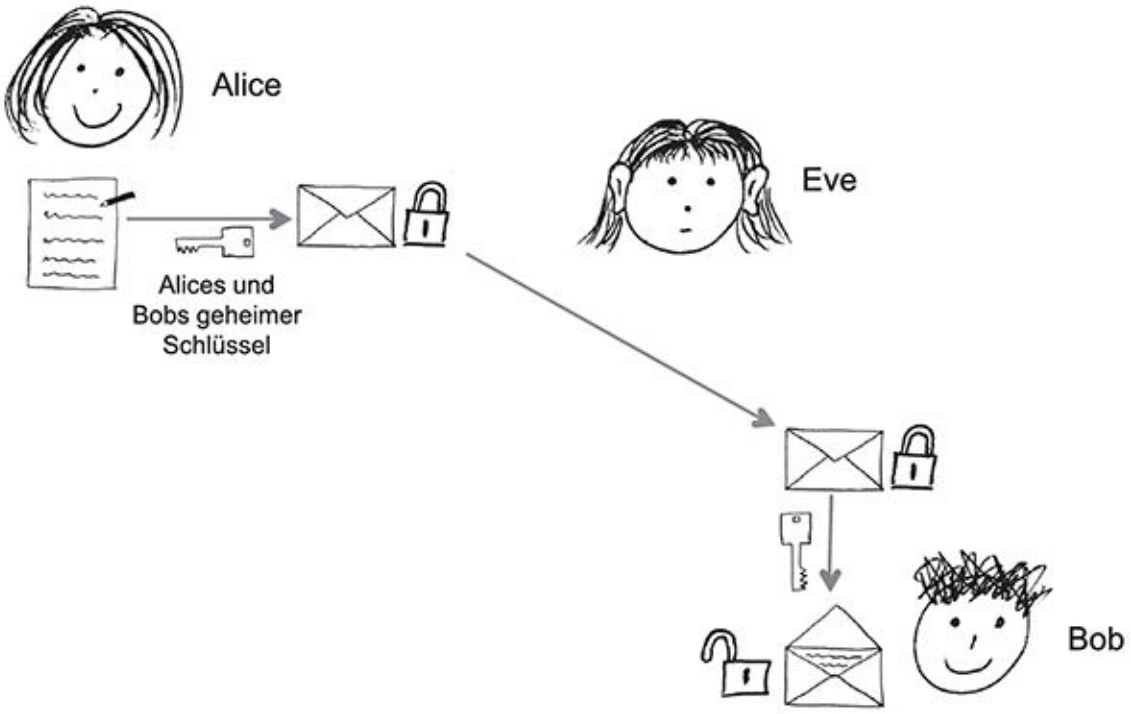


Abb. 2.1 Schema der symmetrischen Verschlüsselung

Denkt man weiter über den Grundsatz »je länger der Schlüssel, desto sicherer die Verschlüsselung« nach, kommt man zu dem Schluss, dass die sicherste Verschlüsselungsmethode die sein muss, bei der der Schlüssel mindestens so lang wie die zu codierende Nachricht ist. Das ist richtig und technisch gesehen auch die einzig sichere, wirklich unknackbare Verschlüsselung (wenn nur der verschlüsselte Text ohne weitere Informationen vorliegt). Allerdings stellt dies Alice und Bob vor ein neues Problem, das der *Schlüsselübergabe*: Zu sicherer Kommunikation gehört nämlich leider nicht nur eine sichere Verschlüsselungsmethode – Botschaft und Schlüssel müssen auch in einer geeigneten Form an den Empfänger übermittelt werden. Je länger also der geheime Schlüssel ist, desto schwieriger wird es für Alice, ihn auf sichere Weise an Bob zu übermitteln. Bob jedoch kann ohne den Schlüssel ihre Nachricht nicht dechiffrieren. Den Schlüssel im Klartext über denselben Kanal wie die Nachricht zu übermitteln (zum Beispiel per E-Mail), wäre nicht sehr sinnvoll, da Eve Alices Nachrichten wahrscheinlich abfängt. Eve müsste in diesem Falle also nur den Stapel der abgefangenen Nachrichten durchgehen, um den Schlüssel zu finden, mit dem sie den Geheimtext entschlüsseln kann.

Perfect Forward Secrecy (PFS)

Sowohl bei der symmetrischen als auch bei der asymmetrischen Verschlüsselung wird die Sicherheit der Kommunikation gefährdet, wenn es einem Angreifer gelingt, den geheimen Sitzungsschlüssel (bei symmetrischer Verschlüsselung) beziehungsweise den privaten Schlüssel (bei asymmetrischer Verschlüsselung) zu stehlen. Wenn dies gelingt, sind alle zurückliegenden Nachrichten, für die dieser Schlüssel verwendet wurde, für den Angreifer lesbar. Wenn Alice und Bob nicht wissen, dass ein Schlüssel entwendet wurde, und deswegen die Schlüssel wie bisher weiterverwenden, sind sogar auch die in der Zukunft liegenden Nachrichten für den Angreifer lesbar.

Wenn bei einem Verschlüsselungsverfahren diese Gefahr gebannt wird, spricht man auch von Perfect Forward Secrecy (PFS), also perfekte in die Zukunft gerichtete Geheimhaltung. PFS kann beispielsweise erreicht werden, indem für jedes Gespräch ein eigener Sitzungsschlüssel erstellt und nach dem Gespräch vernichtet wird. Wie das konkret aussieht, darauf werden wir in späteren Abschnitten noch eingehen – PFS ist beispielsweise ein Bestandteil von »Off the record«-Instant-Messaging (OTR), das Sie im Kapitel über Chatten und Instant Messaging kennenlernen werden.

Es ist übrigens gar nicht so unwahrscheinlich, dass Gespräche, die heute noch sicher verschlüsselt sind, im Nachhinein lesbar werden, wenn keine PFS besteht. Der technische Fortschritt führt nämlich dazu, dass sichere Schlüssel immer länger werden müssen, um Brute-Force-Angriffen standzuhalten. Das Verschlüsselungsverfahren *Data Encryption Standard* (DES), das 1976 als Standard für die US-amerikanische Verwaltung und 1981 auch für den privaten Sektor anerkannt wurde, gilt beispielsweise heute in seiner einfachen Form nicht mehr als sicher, weil die Schlüssellänge damals auf 56 bit begrenzt wurde – eine Länge, die für unsere heutigen Computer kein unüberwindliches Problem mehr darstellt.

Eventuell kommt Ihnen nun der Gedanke, dass man den entsprechenden Schlüssel ebenfalls codiert übermitteln könnte – hier beißt sich die Katze allerdings in den Schwanz, denn dazu müsste dann erneut ein Geheimschlüssel im Klartext zu Bob übertragen werden.

Bei diesem kniffeligen Problem hilft uns die *asymmetrische Verschlüsselung* weiter.

2.1.3. Asymmetrische Verschlüsselung – der Tresor mit Schnappschloss

Der Grund, warum bei symmetrischen Verschlüsselungsmethoden überhaupt ein Schlüsseltausch zwischen Alice und Bob notwendig ist, liegt darin, dass beide eine bestimmte Information benötigen, um die Nachricht zu ver- und zu entschlüsseln. Beide müssen über das gleiche *Geheimwissen* verfügen.

Es geht jedoch auch anders: Bei asymmetrischen Verschlüsselungsverfahren sind die Schlüssel zum Chiffrieren und Dechiffrieren der Nachricht immer unterschiedlich.

Der Schlüssel zum Decodieren des Geheimtextes bleibt stets bei Bob, dem Empfänger der Nachricht, und wird von ihm sorgsam geheim gehalten. Dieser wird daher auch *privater Schlüssel* oder *private key* genannt. Alice hat einen anderen Schlüssel, mit dem sie Nachrichten an Bob nur codieren, aber nicht decodieren kann. Aus diesem Grund bringt es Bob auch nicht in Schwierigkeiten, wenn jemand anderes als Alice diesen Schlüssel besitzt. Sogar Eve, die die Kommunikation der beiden belauschen will, darf ihn in die Finger bekommen – sie kann mit diesem schließlich nur eigene Nachrichten an Bob verschlüsseln, aber die Kommunikation zwischen Alice und Bob nicht entziffern. Diesen Schlüssel bezeichnet man daher als *öffentlichen Schlüssel* oder *public key*. Die Verfahren der asymmetrischen Verschlüsselung werden daher auch als *Public-Key-Verfahren*, asymmetrisch bezeichnet.

Wenn Alice eine Nachricht an Bob schreiben möchte, beschafft sie sich also seinen öffentlichen Schlüssel, verschlüsselt mit diesem die Nachricht und schickt sie an Bob. Bob entschlüsselt sie mit seinem privaten Schlüssel, der während der ganzen Kommunikation in Bobs Besitz verbleibt (siehe unser Schema zur asymmetrischen Verschlüsselung, Abbildung 2.2). Beim Tresor-Beispiel bedeutet das: Alice legt sozusagen ihre Nachricht in einen offenen Tresor mit einem Schnappschloss und klappt diesen zu. Nur Bob kann ihn dann mit seinem privaten Schlüssel wieder öffnen und die Nachricht entnehmen.

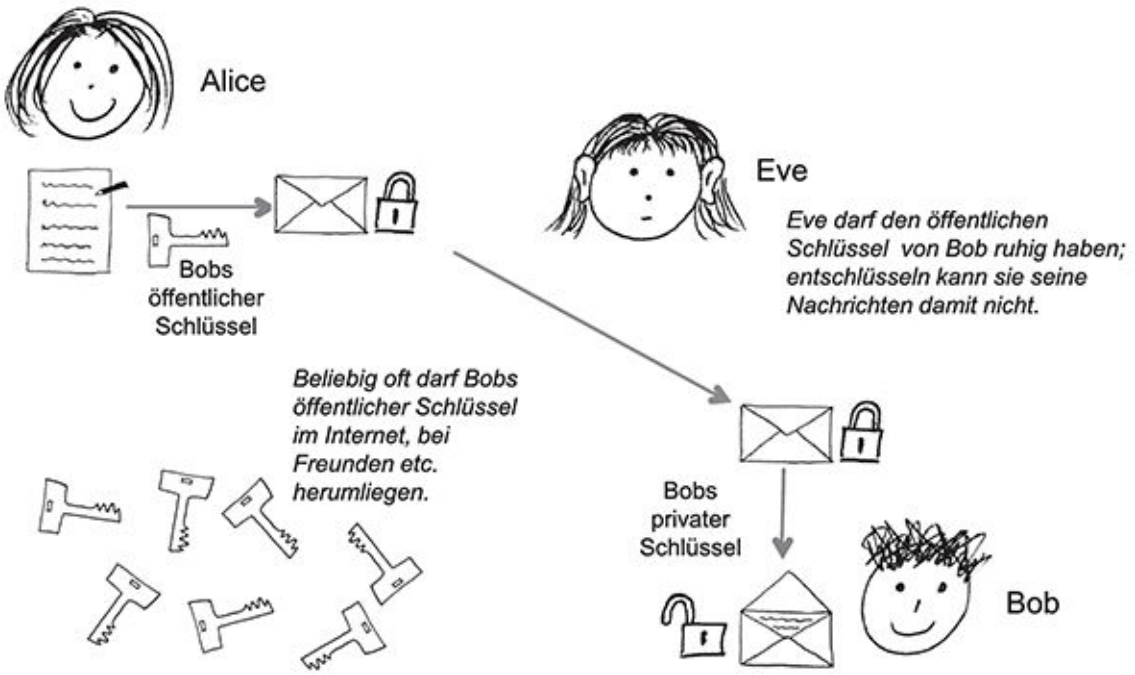


Abb. 2.2 Schema der asymmetrischen Verschlüsselung

Der öffentliche Schlüssel kann bei den meisten Verfahren mithilfe des privaten Schlüssels rekonstruiert werden. Das ist, wie Sie weiter oben gesehen haben, aber auch nicht weiter schlimm, da der öffentliche Schlüssel ohnehin für jeden zugänglich sein soll. Diese Möglichkeit ist glücklicherweise eine Einbahnstraße – der private Schlüssel kann nicht aus seinem öffentlichen Pendant rekonstruiert werden. Dieser Umstand beruht auf folgendem Prinzip:

Der private Schlüssel entspricht zwei großen Primzahlen. Primzahlen sind Zahlen, die nur durch 1 und sich selbst teilbar sind, ohne dass ein Rest übrig bleibt – also *1*, *2*, *3*, *5*, *7*, *11* und so weiter. Die großen Primzahlen, die in der asymmetrischen Verschlüsselung benutzt werden, haben mehrere hundert Stellen. Trotzdem ist es mithilfe eines Computers recht simpel, diese großen Primzahlen zu identifizieren. Einfach ist es außerdem, diese beiden Zahlen miteinander zu multiplizieren – so erhält man (Achtung – stark vereinfacht!) den öffentlichen Schlüssel. Auch mit den schnellsten Computern ist es bisher nicht möglich herauszufinden, welche der großen Primzahlen miteinander multipliziert wurden, wenn man nur das Endergebnis der Multiplikation kennt. Aus diesem Grund kann der private Schlüssel nicht aus dem öffentlichen berechnet werden – ein geniales mathematisches Prinzip, das wir für die Verschlüsselung praktisch anwenden können!

Das Verfahren ist allerdings nur sicher, wenn die Primzahlen auch wirklich groß genug sind. Welche Primzahlen miteinander multipliziert wurden, um zum Beispiel das Ergebnis 323 zu erhalten, kann nämlich auch ein Mensch mit Bleistift, Papier und ein wenig freier Zeit herausfinden. Mit steigender Rechenleistung der Computer müssen auch die Primzahlen, die für eine sichere Verschlüsselung geeignet sind, immer größer werden. Codes, die vor 20 Jahren noch nicht zu knacken waren, lassen sich heute mit modernen Rechnern brechen. Aus diesem Grund befürchten Fachleute, dass die Entwicklung von *Quantencomputern*, die für bestimmte Aufgaben um ein Vielfaches leistungsfähiger sein werden als heutige Computer, unsere heutigen Verschlüsselungsverfahren im Handumdrehen nutzlos machen könnte.

Diffie-Hellman-Schlüsselaustausch

Das Problem der Schlüsselübergabe lässt sich nicht nur lösen, indem man den Schlüssel »sicher« übermittelt, sondern auch damit, dass der Schlüssel gar nicht übermittelt werden muss. Es gibt nämlich ein Verfahren, mit dem zwei Gesprächspartner über eine Distanz hinweg ein gemeinsames Geheimnis vereinbaren können, ohne dass sie dazu (über potenziell unsichere Kommunikationswege) irgendwelche geheimen Informationen austauschen müssen: den Diffie-Hellman-Schlüsselaustausch. (Die Bezeichnung Schlüsselaustausch hat sich eingebürgert, aber der Schlüssel wird nicht ausgetauscht, sondern vielmehr vereinbart.)
Das Diffie-Hellman-Verfahren beruht darauf, dass die beiden Gesprächspartner nicht geheime Informationen austauschen, aus denen dann mit einem mathematischen Verfahren ein geheimer Schlüssel berechnet wird, der zur Verschlüsselung der Sitzung genutzt und nach Ende der Sitzung zerstört wird.
Die asymmetrische Verschlüsselung, wie wir sie bisher beschrieben haben, nimmt insgesamt wegen der komplizierten mathematischen Verfahren viel mehr Rechenleistung in Anspruch als die symmetrische Verschlüsselung. Wenn von asymmetrischer oder Public-Key-Verschlüsselung die Rede ist, wird daher in Wahrheit oft eine Kombination aus symmetrischer und asymmetrischer Verschlüsselung eingesetzt – eine sogenannte *hybride Verschlüsselung*.

2.1.4. Hybride Verschlüsselung

Nehmen Sie einmal an, Alice und Bob kommunizieren über ein Computernetzwerk miteinander und möchten nicht nur sporadisch einfache Textnachrichten austauschen, sondern ein Videotelefonat führen.

Hinweis

Im Grunde unterscheidet sich ein Videochat aus technischer Sicht nicht sehr von einer Textnachricht. Alices und Bobs Computer »zerhacken« dabei (stark vereinfacht) Video- und Audioinformationen in unzählige kleine Datenpakete (also Nachrichten) und tauschen diese in hoher Frequenz miteinander aus. Auf Empfängerseite werden diese Datenpakete dann wieder zu Bildern und Tönen zusammengesetzt. Wie Sie sich sicher vorstellen können, fallen hierbei wesentlich größere Datenmengen an als bei einer einfachen E-Mail. Zusätzlich spielt gerade bei menschlicher Sprache die Geschwindigkeit, in der Daten verarbeitet und übertragen werden können, eine große Rolle. Jeder, der während eines Telefonats mit seinem Handy schon mal in ein Funkloch geraten ist, hat erlebt, wie sich dies auf das akustische Verstehen von Sprache auswirken kann. Die Telefonverbindung ist vielleicht noch nicht zusammengebrochen, aber die Wortfetzen, die bei Ihnen ankommen, ergeben kaum noch einen Sinn.

Alice und Bob wollen ihr Gespräch gegen Eves Schnüffeleien absichern, stehen dabei allerdings vor einem Dilemma:

Asymmetrische Verschlüsselung ist zwar sicherer, aber auch rechenintensiver als ihr symmetrisches Pendant. Um die Datenmengen, die bei einem Videotelefonat anfallen, so schnell zu ver- und entschlüsseln, dass weder Sprach- noch Bildqualität merklich leiden, reicht die Leistung ihrer Computer schlichtweg nicht aus. Eine synchrone Verschlüsselung wäre hingegen schnell, aber nicht sicher genug.

Genau dieses Problem löst die hybride Verschlüsselung. Hierbei erzeugt Alices Computer beim Aufbau der Verbindung zu Bob einen neuen zufälligen Schlüssel hinreichender Länge. Dieser neue Schlüssel wird mit Bobs öffentlichem Schlüssel asymmetrisch chiffriert und an Bobs Computer übertragen (siehe Abbildung 2.3 in diesem Kapitel), wo er mithilfe von Bobs privatem Schlüssel wieder decodiert wird. Der Datenstrom des eigentlichen Telefonats wird dann mit diesem nun auf beiden Seiten zur Verfügung stehenden zufälligen Schlüssel symmetrisch ver- beziehungsweise entschlüsselt (Abbildung 2.4). Das Problem des Schlüsselaustausches bei der symmetrischen Chiffrierung wird also durch den zusätzlichen Einsatz einer asymmetrischen Verschlüsselung umgangen.

Falls Sie nun die Übersicht verloren haben, hier noch einmal das Tresor-Beispiel: Alice legt ihre Nachricht in einen zufällig ausgewählten Tresor und schließt diesen mit einem von zwei dazugehörenden Schlüsseln ab. Einen der Schlüssel packt sie in eine Schatulle mit einem

Schnappschloss, die sie für diesen Zweck von Bob bekommen hat und für die nur er einen passenden Schlüssel besitzt. Beides schickt sie dann mit einer Spedition[1] an Bob. Dieser kann mit seinem Schlüssel die Schatulle öffnen und den Schlüssel entnehmen. Mit seiner Hilfe ist er nun in der Lage, den Tresor aufzuschließen und die für ihn bestimmte Nachricht zu entnehmen. Bob legt dann seine Antwort wieder in den Tresor und verschließt diesen mit dem dafür vorgesehenen Schlüssel. Die Spedition transportiert ab diesem Zeitpunkt nur noch den Tresor zwischen Alice und Bob hin und her, die nun beide die passenden Schlüssel besitzen.

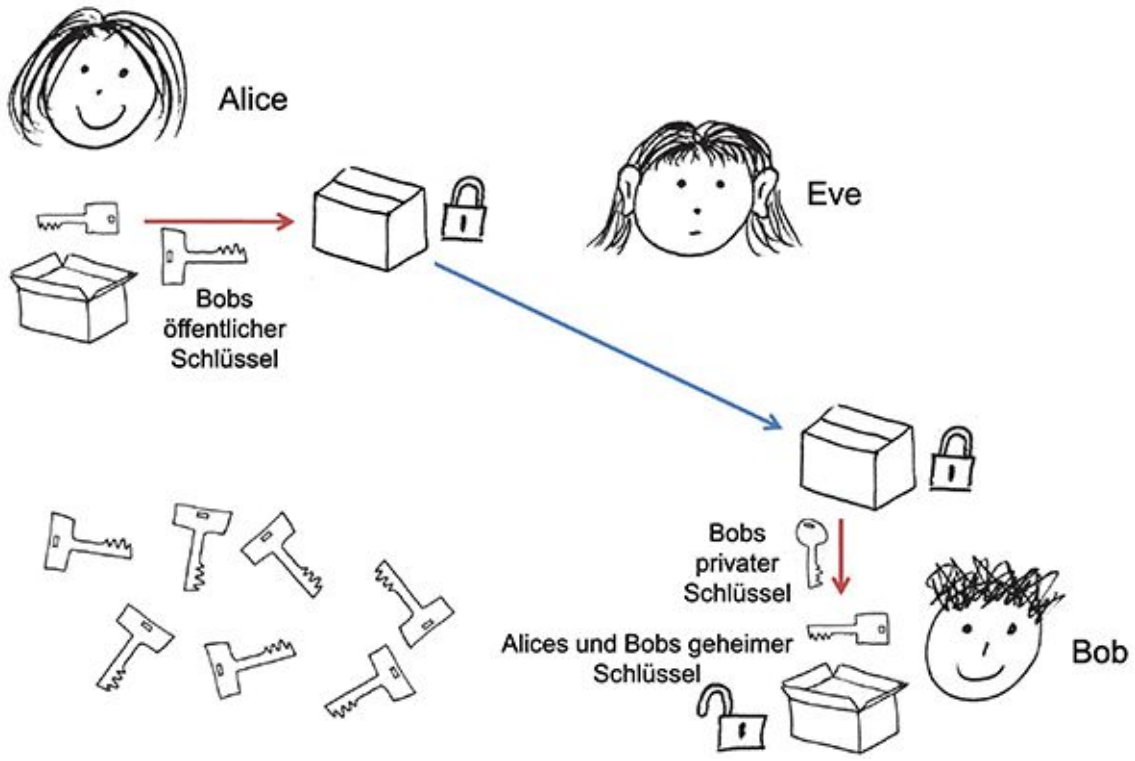


Abb. 2.3 Hybride Verschlüsselung, erster Schritt: Übermittlung des geheimen Schlüssels per asymmetrischer Verschlüsselung

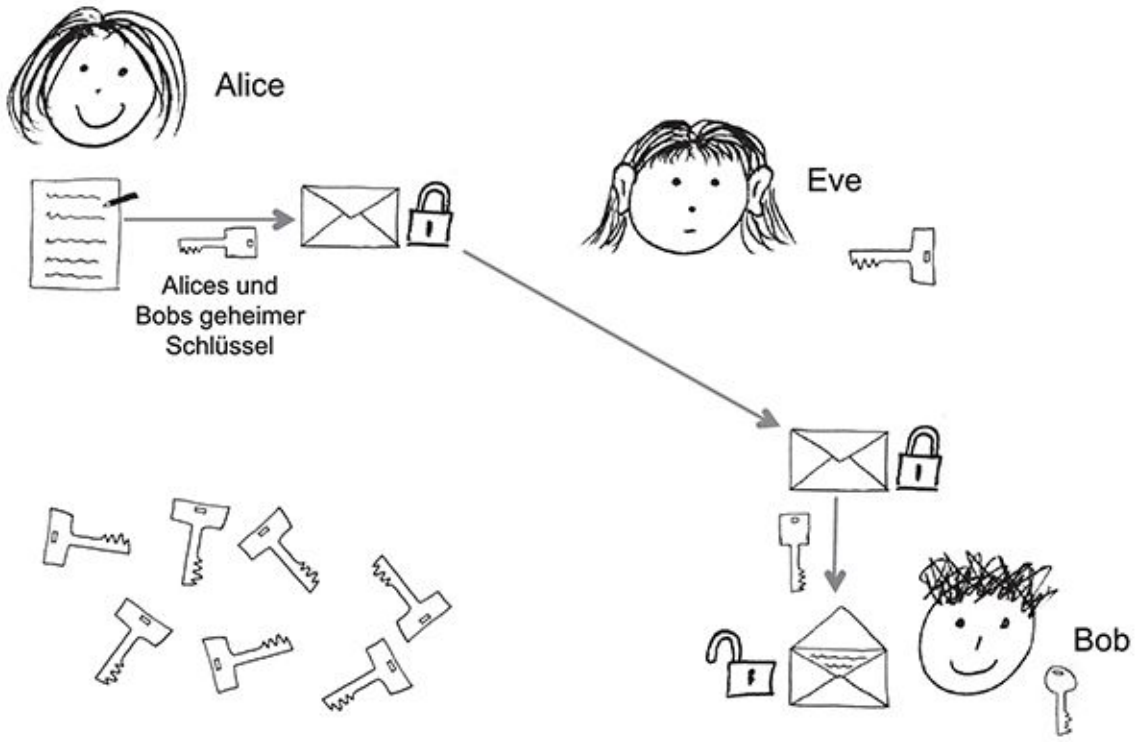


Abb. 2.4 Hybride Verschlüsselung, zweiter Schritt: Kommunikation per symmetrischer Verschlüsselung

In der Praxis hat Bob den privaten Schlüssel für seine Nachrichten wahrscheinlich in Form einer Datei irgendwo auf der Festplatte seines Computers oder auf einem USB-Stick abgelegt. Seine stets neugierige Kollegin Eve sitzt leider nur eine Schreibtischlänge entfernt an ihrem Arbeitsplatz. Um zu verhindern, dass sie Bobs privaten Schlüssel in einem unbeobachteten Moment einfach kopieren kann, hat Bob ihn zusätzlich mit einem Passwort geschützt. Dies bedeutet, dass der private Schlüssel mit einem symmetrischen Verfahren codiert und erst dann auf der Festplatte gespeichert wird. Der Schlüssel dazu wird aus dem Passwort, das man in diesem Zusammenhang auch als *passphrase* (»Pass-Satz«) bezeichnet, berechnet.

Da Passwörter Ihnen im Zusammenhang mit dem Schutz Ihrer Daten immer wieder begegnen werden, möchten wir sie im Folgenden ein wenig genauer unter die Lupe nehmen.

2.2 Gute und schlechte Passwörter – hundename123

Welche Möglichkeiten hätte Eve, Bobs richtiges Passwort herauszufinden?

1. Sie kann das Passwort erraten.
2. Sie kann alle möglichen Zeichenkombinationen durchprobieren, bis sie das Passwort gefunden hat.

Nur ein menschlicher Angreifer kann ein Passwort mit dem ersten Verfahren knacken. Es ist dazu entweder Hintergrundwissen oder die Anwesenheit des Angreifers vor Ort notwendig. Erfolgreich könnte ein solcher Angriff zum Beispiel sein, wenn Eve weiß, wie Bobs Hund heißt und in welchem Jahr er ihn bekommen hat. Noch einfacher wird es, wenn Eve weiß oder herausfindet, dass Bob stets einen Schmierzettel mit seinen Passwörtern unter seiner Tastatur aufbewahrt.

Der zweite Ansatz kann auch von einem Computer durchgeführt werden. Außer bei sehr kurzen Passwörtern ist ein Computer hier sogar notwendig, da das Durchprobieren aller möglichen Kombinationen einen menschlichen Angreifer viel zu viel Zeit kosten würde. Diese Vorgehensweise wird auch als *brute force* (englisch für »rohe Gewalt«) bezeichnet, da im

Gegensatz zum ersten Verfahren nicht Nachdenken zum Ziel führt, sondern die Fähigkeit, möglichst viele Passwörter in einer bestimmten Zeit auszuprobieren.

Es gibt eine Reihe von Herangehensweisen, die diese beiden Prinzipien kombinieren, also menschliches Vorwissen mit der Rechenleistung eines Computers, zum Beispiel indem alle Wörter eines Wörterbuchs ausprobiert werden.

2.3 Tipps für gute Passwörter

Was macht also ein gutes Passwort aus, das robust gegenüber beiden Arten von Angriffen ist? Gegen das einfache Erraten Ihres Passwortes können Sie sich schon durch wenige einfache Maßnahmen schützen.

- Verwenden Sie *niemals persönliche Informationen* als Passwort (Geburtstage, Namen von Partnern, Kindern, Haustieren, Adressbestandteile usw.)
- Notieren Sie Ihre Passwörter *nicht auf Zettelchen* (die z. B. am Bildschirm kleben, unter der Tastatur, der Schreibtischauflage oder in der obersten Schublade liegen – dort wird jede Eve zuerst suchen).
- Geben Sie Ihr Passwort *niemals an andere Personen* weiter.

Welche Passwörter sind widerstandsfähig gegenüber Brute-Force-Angriffen? Vorteilhaft sind zunächst einmal lange Passwörter (»longer is stronger«) – Sie können sich vorstellen, dass es länger dauert, ein Passwort mit 20 Stellen durch Ausprobieren herauszufinden, als eines mit zwei Stellen.

Da aber kaum eine Eve ein reines Brute-Force-Verfahren anwenden würde, sondern sich viel eher aus einschlägigen Quellen im Internet Wörterbücher mit vielen Passwort-Kandidaten herunterladen würde, reicht die Länge als alleiniger Faktor nicht aus. Ein langes Passwort ist beispielsweise völlig nutzlos, wenn es sich um ein Wort handelt, das in einem gewöhnlichen Wörterbuch steht. Es existieren auch Wörterbücher mit Worten, in denen zum Beispiel »i« durch »1« oder »!« ersetzt wurde. Wenn Sie also »f1ff1« statt »fiffi« schreiben, macht das Ihr Passwort nicht wirklich sicherer. Zudem gibt es Algorithmen, die Bestandteile von Wörtern in Wörterbüchern neu miteinander kombinieren (siehe auch Kasten zum Passwort-Cracking weiter unten). Gegenüber vielen Angriffen ist Ihr Passwort umso sicherer, je zufälliger es ist. Informatiker reden davon, dass unter anderem die *Entropie* eines Passworts, also seine Unordnung, ein Maß für seine Stärke ist.

Natürlich könnten Sie nun stets 30 Zeichen lange Passwörter verwenden, die aus rein zufälligen Zeichenfolgen (inklusive Sonderzeichen und Zahlen) bestehen. Aber wie viele davon können Sie sich merken – ein halbes? Und ein sicheres Passwort, das auf einem Zettel unter Ihrer Tastatur liegt, ist, wie eingangs erwähnt, kein sicheres Passwort.

Um Ihr Passwort sicherer gegen Brute-Force-Angriffe zu machen, haben Sie also folgende Möglichkeiten:

- Sie überlegen sich Passwörter, deren Zeichenfolge annähernd zufällig erscheint, aber die trotzdem für Sie gut zu merken sind. Eine Idee ist, sich einen Satz zu merken und die Anfangsbuchstaben der Wörter als Passwort zu verwenden. Beispiel: »Der Dackel sieht aus wie eine Wurst mit Beinen!« Daraus können Sie das Passwort »DDsaw1WmB!« ableiten. Sicher keine ganz zufällige Zeichenfolge (weil zum Beispiel deutsche Wörter häufiger mit bestimmten Buchstaben anfangen), aber besser als »fiffi15«.
- Sie verwenden lange Passwörter aus zufälligen Zeichenfolgen und verwalten sie mit einem geeigneten Passwort-Manager. Auf diese werden wir später in Kapitel 6 (»Für Vergessliche und solche, die es werden wollen«) noch ausführlicher eingehen.

2.3.1. Hashfunktionen

Was hat aber nun das Passwort eigentlich mit der Verschlüsselung zu tun? Wenn Sie einen privaten Schlüssel oder irgendeine andere Information mit einer symmetrischen Chiffre codieren, wird der Schlüssel für diese Codierung aus einem Passwort berechnet. Das passiert mittels einer sogenannten *Hashfunktion*, die wir im Rest dieses Kapitels erklären werden.

Ein Passwort wird natürlich auch für andere Zwecke verwendet, zum Beispiel zur Zugangskontrolle. Für diese Passwörter gelten die gleichen Sicherheitsregeln, die Sie bisher gelernt haben. Auch und besonders für Passwörter zur Zugangskontrolle (zum Beispiel zu Ihrem E-Mail-Account oder Ihrem Onlinebanking-Zugang) ist es sinnvoll, dass Sie zumindest einmal von der Hashfunktion gehört haben. Das Hashverfahren läuft nämlich, wie Sie sehen werden, darauf hinaus, dass Ihr Passwort nirgendwo, also auch nicht auf einem Server des E-Mail-Anbieters oder der Bank, im Klartext gespeichert werden muss (oder soll!). Wenn Ihre Bank und alle anderen Anbieter von zugangskontrollierten Services sich an diese Regel halten,

verringert sich enorm das Risiko, dass bösartige Eindringlinge Ihr Passwort und die Passwörter der anderen Kunden erbeuten können – es gehört daher zum guten Standard für Anbieter, die Passwörter ihrer Kunden niemals im Klartext zu speichern.

An dieser Stelle kommen die Hashwerte von Passwörtern ins Spiel: Durch Berechnung des Hashwerts weiß Ihr Gegenüber, also zum Beispiel Ihre Bank, dass Sie das richtige Passwort eingegeben haben. Dazu füttert man eine Hashfunktion mit einem Text, und diese berechnet daraus eine Buchstaben- und Zahlenkombination, einen *Hashwert*, der spezifisch für seinen Ursprungstext ist. Das bedeutet, dass auch eine nur gering veränderte Eingabe zu einer völlig anderen Ausgabe führt. Nur zwei exakt gleiche Passwörter haben den gleichen Hashwert, deshalb kann man genauso gut zwei Hashwerte statt der ursprünglichen Passwörter vergleichen. Beim »Hashen« eines Passworts geht Information verloren – man kann daher aus einem Passwort einen Hashwert berechnen, aber aus einem Hashwert nicht das zugehörige Passwort (ähnlich wie bei den privaten und öffentlichen Schlüsseln im vorangegangenen Abschnitt). Wenn also statt eines Passworts dessen Hashwert gespeichert wird, hat das folgende Vorteile:

1. Es wird *weniger Speicherplatz* gebraucht, da der Hashwert oft kürzer als das ursprüngliche Passwort ist.
2. Es ist *sicherer*, da wie schon erwähnt bei einem Diebstahl der Hashwerte die Passwörter nicht rekonstruiert[2] werden können (anders als bei einer Datei, die die Passwörter im Klartext enthält).

Dass nur zwei genau gleiche Passwörter den gleichen Hashwert haben, stimmt nicht ganz. Hashwerte sind oft kürzer als ihr Ursprung, daher kann es verschiedene Eingaben geben, die zum gleichen Ergebnis führen. Eine gute Hashfunktion sollte zu möglichst keiner dieser sogenannten *Kollisionen* führen.

Eine ganz einfache Hashfunktion ist zum Beispiel die Quersumme einer Zahl (die in dieser Form natürlich nur auf Zahlen anwendbar ist). Bei einer Eingabe von 23 ist der Hashwert 5, denn 2 + 3 = 5. Aus der Eingabe von 10439 ergibt sich ein Hashwert von 1 + 0 + 4 + 3 + 9 = 17.

Nehmen wir an, dass Sie bei einer Verschlüsselung das Passwort 10439 gewählt haben und daher der Hashwert von 17 auf Ihrer Festplatte gespeichert wurde. An dieser Stelle sehen Sie auch, dass 17 weniger Speicherplatz als 10439 einnimmt. Die Angreiferin Eve möchte nun Ihre Daten lesen und versucht es mit dem Passwort 10438. Der Computer berechnet daraus den

Hashwert, der 16 beträgt, und vergleicht ihn mit dem gespeicherten Hashwert von 17. Die beiden stimmen nicht überein, also können auch das eingegebene Passwort und das korrekte Passwort nicht gleich sein. Die Eingabe 10438 wird also abgelehnt.

Wenn Eve nun 40193 anstatt 10439 eingibt, passiert allerdings Folgendes:

Der Hashwert von 40193 beträgt ebenfalls 17 – der Computer würde 40193 demnach ebenfalls als korrektes Passwort akzeptieren, und Eve erhielte Zugriff auf Bobs verschlüsselten Daten. Es ist also eine Kollision aufgetreten, was beim Bilden von einfachen Quersummen natürlich sehr häufig passiert. Dies ist ein Grund, warum die Quersumme hier früh aus dem Kreise geeigneter Hashfunktionen für den täglichen Gebrauch ausscheidet.

Das Handwerkszeug eines Passwort-Crackers

Wenn wir mal von dem Fall absehen, dass jemand, der Sie gut kennt, aus irgendeinem Grund zum Beispiel in Ihr Postfach einbrechen will und dazu Ihr Passwort errät – wie gelangen Passwörter normalerweise in die Hände eines Angreifers?

Der erste Schritt ist meistens, dass eine Tabelle mit »gehashten« Passwörtern von einem Server gestohlen wird oder sonstwie das Licht der Öffentlichkeit erblickt – beispielsweise durch einen Angestellten oder Exangestellten, der dem Unternehmen böse gesonnen ist. So eine Tabelle ist eine sehr große Textdatei, die die Hashwerte von zahlreichen Passwörtern enthält.

Der »Passwort-Cracker«, also der Angreifer, der die Passwörter entschlüsseln möchte, benötigt neben dieser Textdatei noch ein Programm, das sehr schnell die Hashes verschiedener Buchstabenfolgen berechnen und mit den Einträgen in der Hashtabelle vergleichen kann. Außerdem benutzt er, um seinen Job einfacher zu machen, noch eine oder mehrere Wörterbuchdateien. Diese können nicht nur echte Wörter verschiedener Sprachen enthalten, sondern auch häufige echte Passwörter (beispielsweise aus einer 14,5 Millionen Einträge langen Liste mit echten Passwörtern, die 2012 dem Unternehmen RockYou gestohlen wurde).

Da der Klartext nicht aus dem Hashwert berechnet werden kann, sondern nur umgekehrt, wie wir oben gesehen haben, tut das Programm nun Folgendes: Es nimmt immer wieder eine Klartext-Zeichenkette, berechnet daraus den Hashwert (beispielsweise mit dem Hashing-Algorithmus MD5) und schaut dann nach, ob der Hashwert in der Hashtabelle vorkommt. Wenn ja, ist ein Passwort geknackt worden: Es entspricht der Zeichenkette, aus der dieser Hashwert berechnet wurde.

Das Programm kann, grob gesagt, drei Methoden anwenden, um die Zeichenketten zu finden, mit denen es startet.

1. Brute Force: Es geht alle möglichen Zeichenkombinationen einer bestimmten Länge durch (vereinfacht gesagt von aaaaaa, aaaaab, .. über zzzzzz bis 999999). Das ist sehr rechenintensiv und ist unter anderem ein Grund dafür, warum lange Passwörter sicher sind.

2. Wörterbuchattacke: Es geht alle Wörter in den Wörterbüchern durch, die der Benutzer ihm zur Verfügung gestellt hat.

3. Regelbasierte Attacke: Es stellt die Zeichenketten nach bestimmten Regeln zusammen, beispielsweise Wörter aus dem Wörterbuch plus eine Zahl zwischen 0 und 99, Wörter aus dem Wörterbuch plus spiegelverkehrtes Wort bis hin zu ganz verfeinerten Algorithmen, die davon ausgehen, mit welcher Wahrscheinlichkeit in einer Sprache ein bestimmter Buchstabe auf einen bestimmten anderen Buchstaben folgt.

Insbesondere die regelbasierten Attacken werden stetig weiterentwickelt und führen dazu, dass auch auf den ersten Blick schwer zu knackende Passwörter mit Sonderzeichen und Zahlen dem Passwort-Cracker zum Opfer fallen können.

2.4 Web of Trust und Zertifizierungsstellen – Vertrauen im Netz

Weiter oben haben Sie erfahren, wie das Prinzip asymmetrischer Verschlüsselung funktioniert: Wenn Alice Bob eine verschlüsselte Nachricht zukommen lassen möchte, benötigt sie seinen öffentlichen Schlüssel. Bob selbst kann den erhaltenen Text dann mit seinem privaten Schlüssel dechiffrieren und lesen.

Bobs öffentlicher Schlüssel darf dabei der Öffentlichkeit jederzeit zugänglich sein. Ist er es nicht, können nur diejenigen sicher mit ihm kommunizieren, denen er zuvor seinen öffentlichen Schlüssel zur Verfügung gestellt hat. Wenn Bob nur mit Freunden verschlüsselte Nachrichten austauschen will, reicht das auch vollkommen aus. Denkbar ist allerdings auch, dass Bob nicht immer nur mit Alice kommunizieren möchte, sondern aus irgendeinem Grund verschlüsselte E-Mails von Leuten empfangen will, die er nicht persönlich kennt:

- von Kunden, falls Bob die E-Mail-Adresse für geschäftliche Zwecke nutzt

- von Kollegen aus dem In- und Ausland, mit denen er sich fachlich austauschen möchte
- oder einfach von Fremden aus dem Internet, die auf seine persönliche Webseite über Guerilla Gardening[3] gestoßen sind und Erfahrungen über die günstigsten Lichtverhältnisse für den Grünkohlanbau austauschen wollen

Wenn Bob diesen Menschen, mit denen er zuvor nie persönlichen Kontakt hatte, Zugriff auf seinen öffentlichen Schlüssel gewähren möchte, kann er ihn, je nach verwendeter Verschlüsselungstechnologie, auf einen sogenannten *Key Server* hochladen. Ein Key Server ist ein über das Internet erreichbarer Dienst, auf dem wie in einem Telefonbuch Tausende von öffentlichen Schlüsseln und zugehörige Informationen (zum Beispiel E-Mail-Adressen) gespeichert sind.

Beispielsweise ist Angela aus der Uckermark, die neben ihrem stressigen Job als Politikerin begnadete Hobbygärtnerin ist, Bobs öffentlicher Schlüssel bisher nicht bekannt. Dennoch möchte sie ihm eine verschlüsselte E-Mail schreiben. Sie kann in diesem Fall besagten Server nutzen, um mithilfe von Bobs E-Mail-Adresse den passenden Public Key zu identifizieren und herunterzuladen. Aber – Sie haben es vielleicht schon befürchtet – bei der Nutzung eines solchen Key Servers ergibt sich für Angela ein gravierendes Sicherheitsproblem: Jeder kann ohne Prüfung einen beliebigen öffentlichen Schlüssel, in Verbindung mit einem Kommentar und einer E-Mail-Adresse, auf einem solchen Server hinterlegen. Angela kann sich also nicht wirklich sicher sein, dass der Schlüssel, den sie heruntergeladen hat, nicht in Wahrheit von Eve stammt, die ihn unter falschem Namen dort abgelegt hat. Wenn das so wäre, würde Angela nichts ahnend ihre privaten Nachrichten an Bob mit Eves öffentlichem Schlüssel, nicht mit Bobs Schlüssel, chiffrieren. Eve könnte dann die Nachrichten abfangen, mit ihrem privaten Schlüssel entschlüsseln und lesen. Und nicht nur das: sie könnte die Nachricht daraufhin mit Bobs öffentlichem Schlüssel verschlüsseln und an ihn weiterleiten, sodass weder Angela noch Bob wüssten, dass die geheimen Nachrichten von Eve mitgelesen werden! (Dies wäre ein Beispiel für eine sogenannte »Man in the Middle«-Attacke.)

Für dieses Dilemma existieren zwei Lösungen: Die erste Lösung ist die persönliche Schlüsselverifikation. Angela und Bob treffen sich im Vorfeld persönlich und tauschen miteinander die öffentlichen Schlüssel aus. Dies geschieht beispielsweise mit der Hilfe von

USB-Sticks oder anderen mobilen Datenträgern. Da Angela allerdings in der Uckermark und Bob auf Jamaika lebt, ist dieses Vorgehen unrealistisch.

Wenn die persönliche Verifizierung nicht möglich ist, hilft einem die Verifizierung des Schlüssels durch einen vertrauenswürdigen Dritten weiter. Hier gibt es wiederum zwei Möglichkeiten:

1. Bob lässt seinen öffentlichen Schlüssel dabei durch eine unabhängige, allgemein anerkannte Autorität, der auch Angela vertraut, »beglaubigen«. Eine solche Instanz wird auch als *Certificate Authority* (Zertifizierungsstelle oder kurz: CA) bezeichnet. Sie ist grob mit der Personalausweisstelle Ihrer Stadt vergleichbar. Hier wird festgestellt, ob Bob wirklich derjenige ist, der er vorgibt zu sein. Bei der Stadt erhält er einen neuen Personalausweis, bei einer CA wird sein Schlüssel einfach mithilfe einer *digitalen Signatur* verifiziert. Die Bestätigung von öffentlichen Schlüsseln erfolgt bei dieser Herangehensweise also *zentralisiert*, durch eine einzige oder wenige übergeordnete Instanzen.

2. Bobs öffentlicher Schlüssel wird durch eine oder mehrere Personen verifiziert, denen Angela persönlich vertraut. In diesem Fall entsteht durch die persönlichen Vertrauensbeziehungen der Benutzer untereinander ein Netzwerk, das als *Web of Trust* (WoT) bezeichnet wird. Die Schlüsselbestätigung im Web of Trust erfolgt *dezentral*, also durch viele verteilte, gleichgestellte Instanzen.

Wir stellen Ihnen die Vor- und Nachteile beider Zertifizierungssysteme weiter unten vor. Vorher erfahren Sie zum besseren Verständnis noch ein bisschen mehr über die digitale Signatur, ohne die beide Verfahren nicht funktionieren würden.

2.4.1. Digitale Signatur

Vereinfacht gesehen funktioniert die Verifizierung eines öffentlichen Schlüssels durch einen vertrauenswürdigen Dritten folgendermaßen: Es wird ein Textdokument erzeugt, in dem Name, E-Mail-Adresse und gegebenenfalls weitere Informationen dem öffentlichen Schlüssel zugeordnet werden. Dieses Dokument wird nun durch den vertrauenswürdigen Dritten *digital signiert*, um zu bezeugen, dass er die enthaltenen Angaben überprüft und für korrekt befunden hat. Aber was ist eine *digitale Signatur*?

Weiter oben haben Sie gelernt, dass bei der asymmetrischen Verschlüsselung eine mit dem öffentlichen Schlüssel chiffrierte Nachricht nur mit dem zugehörigen privaten Schlüssel

decodiert werden kann. Dies ist aber auch umgekehrt möglich – eine mit dem privaten Schlüssel codierte Nachricht kann demnach nur mit ihrem öffentlichen Pendant dechiffriert werden.

Sie fragen sich jetzt wahrscheinlich, wieso Bob beispielsweise eine Nachricht mit seinem privaten Schlüssel verschlüsseln sollte, wenn diese dann doch vom Rest der Welt mithilfe ihres öffentlichen Schlüssels gelesen werden kann. Die Antwort ist simpel – wenn die Nachricht mit Bobs öffentlichem Schlüssel wieder lesbar gemacht werden kann, beweist dies zweierlei Dinge:

1. Die Nachricht wurde tatsächlich von Bob geschrieben.
2. Niemand hat die Nachricht auf ihrem Weg verändert, da niemand in Besitz von Bobs privatem Schlüssel ist außer ihm selbst.

Bob hat also eine »digitale Unterschrift«, eine *digitale Signatur*, geleistet.

Der Einfachheit halber hängt Bob zusätzlich noch seinen öffentlichen Schlüssel direkt an die so signierte Nachricht an, damit die Empfängerin sich von deren Authentizität und Integrität überzeugen kann. Hierbei entsteht allerdings wieder ein kleines Problem: Um sowohl verschlüsselte als auch signierte Nachrichten zu versenden, müsste Bob diese jedes Mal zunächst mithilfe seines privaten Schlüssels und anschließend mit dem öffentlichem Schlüssel der Empfängerin chiffrieren. Und das wäre für beide Seiten ein erheblicher Aufwand.

Um das mehrfache Ver- und Entschlüsseln zu vermeiden, bedient sich Bob eines Tricks. Statt beim Signieren die ganze Nachricht zu verschlüsseln, bildet er einfach deren spezifischen Hash (siehe oben). Diesen chiffriert er mit seinem privaten Schlüssel und schreibt das Ergebnis unter seine eigentliche Nachricht. Die Empfängerin kann nun nach Erhalt der Nachricht seinerseits deren Hashwert berechnen. Sind sein errechneter Hashwert und der mithilfe von Bobs Public Key dechiffrierte Hashwert identisch, ist die Integrität der Nachricht bewiesen. Unterscheiden sich die beiden Werte, ist es wahrscheinlich, dass die Nachricht unterwegs verändert wurde. Zusätzlich ist die Empfängerin weiterhin in der Lage festzustellen, ob wirklich Bob der Urheber des Textes ist, da nur er im Besitz des zur Signierung verwendeten privaten Schlüssels sein kann. Die digitale Signatur kann übrigens sowohl getrennt als auch zusätzlich zur asymmetrischen Verschlüsselung einer Nachricht eingesetzt werden.

Der Mechanismus der digitalen Signatur ist, wie eingangs erwähnt, das zentrale Element bei der »Beglaubigung« öffentlicher Schlüssel und damit bei der Vertrauensbildung im Internet.

2.4.2. Die Zertifizierungsstelle (CA)

Zurück zur Bestätigung eines öffentlichen Schlüssels durch eine Zertifizierungsstelle. Diese erstellt also vereinfacht gesehen ein Dokument, in dem ein öffentlicher Schlüssel einer E-Mail-Adresse und einem Namen zugeordnet wird. Nun erstellt diese mithilfe ihres privaten Schlüssels eine Signatur und schreibt diese zusätzlich in diese Datei. So entsteht ein digital beglaubigtes Dokument, also ein (digitales) Zertifikat (siehe Abbildung 2.5). Mit ihm kann bewiesen werden, dass die Zertifikatsstelle (und kein anderer!) bescheinigt, dass Name, Adresse und Schlüssel zusammengehören.

Ein öffentlicher Schlüssel wird immer anhand seines *Fingerabdrucks* (englisch »fingerprint«) identifiziert. Dieser wird meistens als ein hexadezimaler Code, also eine Folge von Zahlen aus dem Hexadezimalsystem (z. B. 8A 24 D6 13) dargestellt und fungiert als einzigartiger »Name« für einen individuellen Schlüssel.

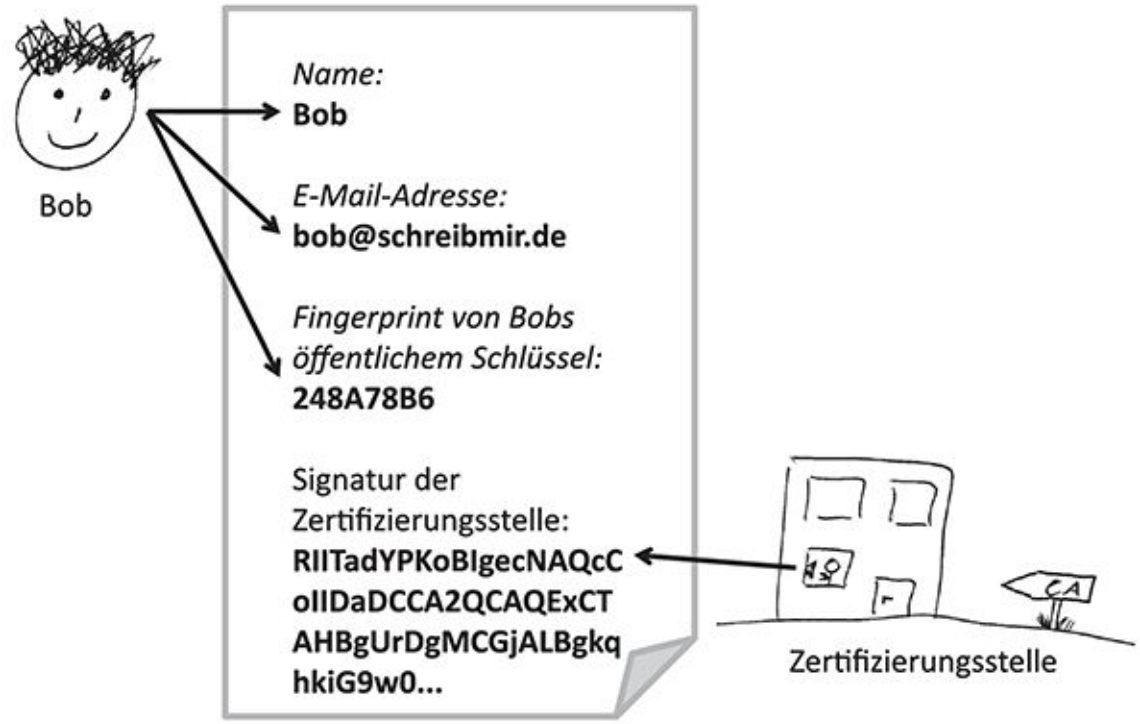


Abb. 2.5 Zertifikat für einen öffentlichen Schlüssel (Dokument mit Fingerprint, Mailadresse, Namen und Signatur)

Wenn Angela Bob nun eine vertrauliche Nachricht schicken möchte, kann sie also seinen öffentlichen Schlüssel herunterladen und sich von der Zertifizierungsstelle (CA) bestätigen lassen, dass dieser öffentliche Schlüssel tatsächlich zu Bob gehört.

Existiert bisher kein entsprechendes Zertifikat, könnte Angela ihn bitten, sich mit seinem Personalausweis bei der CA vorzustellen. Nehmen wir nun einmal an, er kommt dieser Bitte nach und seine Ausweisdokumente sind tadellos in Ordnung:

Die CA stellt nun ein Zertifikat für Bobs öffentlichen Schlüssel aus und signiert ihn. Sie verwendet dazu wiederum ihren eigenen privaten Schlüssel. Die »Echtheit« des Zertifikates kann danach von allen anderen mithilfe des öffentlichen Schlüssels der CA überprüft werden.

Nun werden Sie sich zu Recht fragen, wer dann den öffentlichen Schlüssel der Zertifizierungsstelle beglaubigt. Dies kann eine übergeordnete Zertifizierungsstelle tun. Eine Zertifizierungsstelle, der keine weitere Stelle übergeordnet ist, wird als *Root CA* (Wurzelzertifizierungsstelle) bezeichnet. Dies könnte zum Beispiel die Bundesnetzagentur sein. Diese Struktur, die eine mögliche Form der *Public-Key-Infrastruktur* (PKI) darstellt, ist also streng hierarchisch aufgebaut (siehe Abbildung 2.6). Ein Beispiel für einen hierarchisch aufgebauten Standard zum Verschlüsseln und Signieren von E-Mails ist *S/MIME*, über den Sie im nächsten Kapitel mehr erfahren werden.

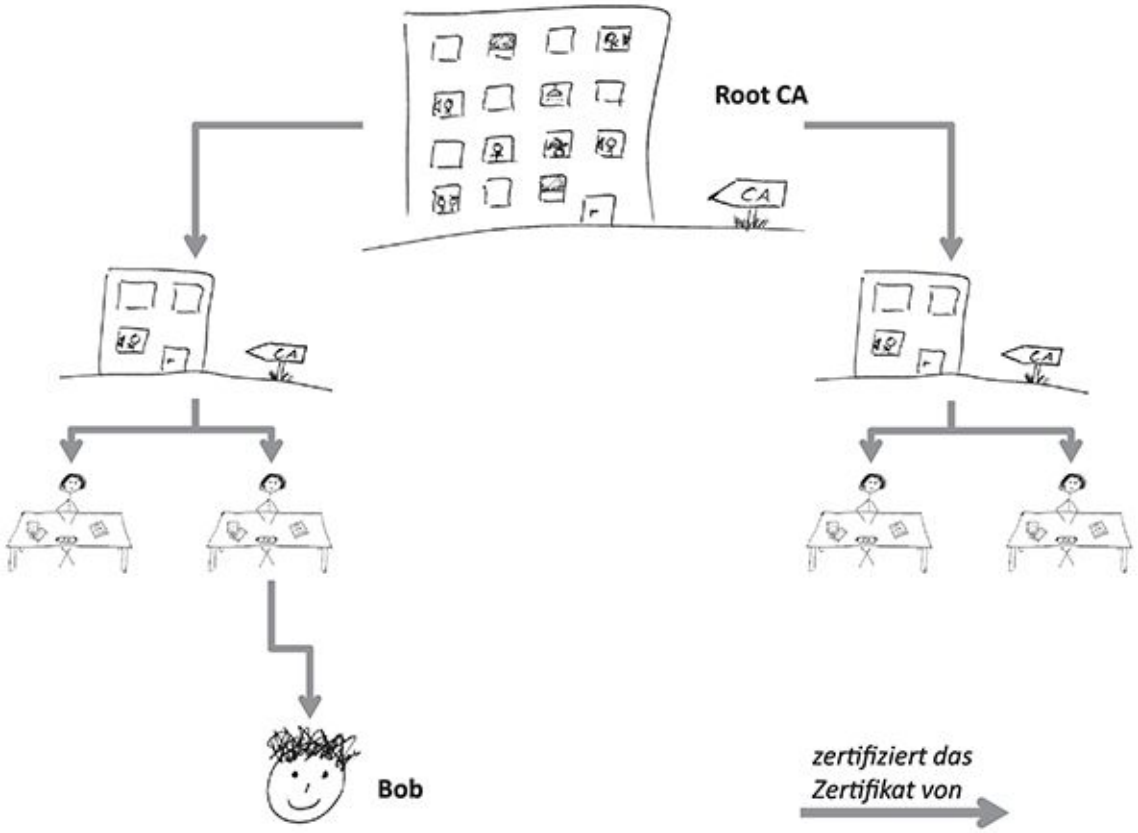


Abb. 2.6 Schema der Public-Key-Infrastruktur (PKI)

Der hierarchische und sehr zentralisierte Aufbau der PKI hat einen gravierenden Nachteil. Ein Angreifer, der in die Computersysteme einer CA eindringt und ihren privaten Schlüssel in seinen Besitz bringt, kann plötzlich gültige Zertifikate für Schlüssel erzeugen, die eigentlich gar nicht vertrauenswürdig sind. Das versetzt ihn in die Lage, sich fälschlicherweise als ein real existierender Kunde der CA auszugeben (beispielsweise eine Bank), indem er ein scheinbar gültiges Zertifikat vorweist. Als wäre das nicht schon schlimm genug, kompromittiert er damit auch die Sicherheit aller untergeordneten CAs. Begünstigt durch den hierarchischen Aufbau der PKI kann der Angreifer sich also auch als einer ihrer Kunden ausgeben.

2.4.3. Zertifizierung im Web of Trust (WoT)

Im Gegensatz zur streng hierarchischen PKI gibt es eine alternative Struktur, um öffentliche Schlüssel zu bestätigen: das oben schon angesprochene *Web of Trust* (Netz des Vertrauens, siehe Abbildung 2.7).

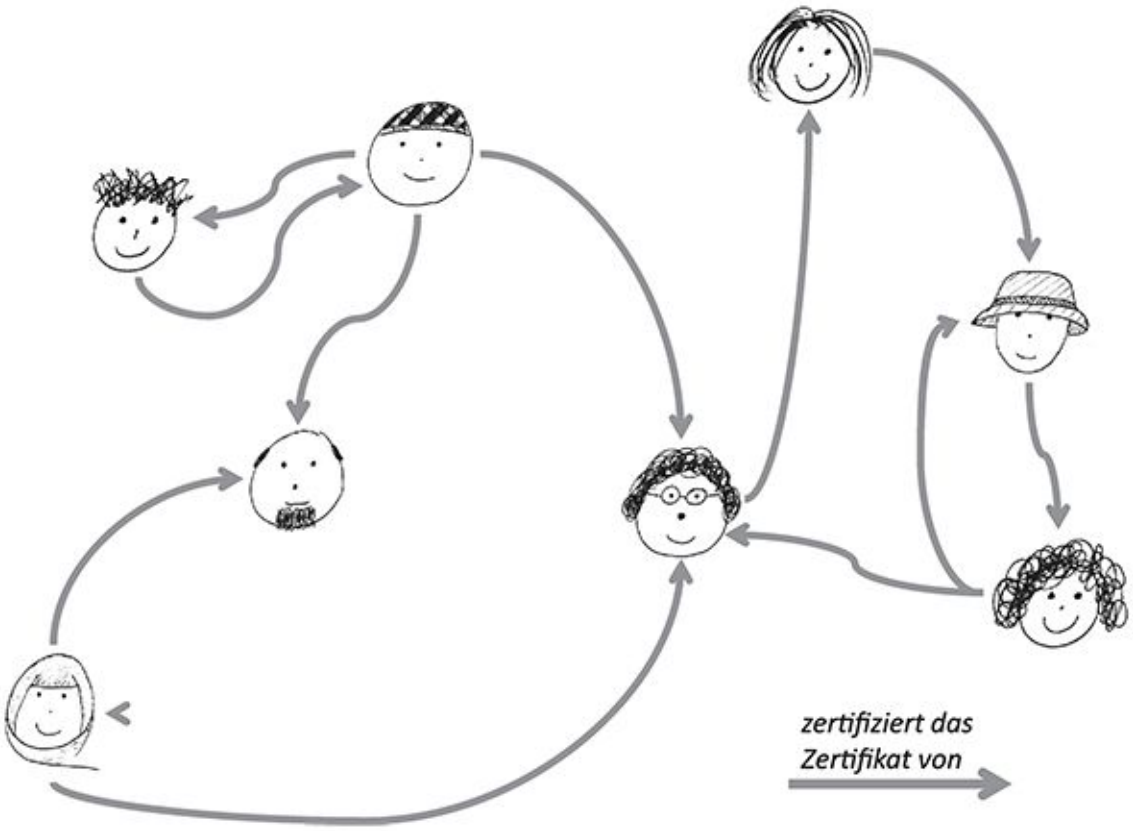


Abb. 2.7 Schema eines Web of Trust

Die hierarchische PKI und das Web of Trust haben die Gemeinsamkeit, dass bei beiden Verfahren die Authentizität eines öffentlichen Schlüssels durch einen vertrauenswürdigen Dritten bestätigt wird. Während diese Aufgabe im ersten Fall durch eine offizielle Zertifizierungsstelle übernommen wird, kann in einem Web of Trust jeder Dritte als eine derartige Instanz fungieren. Voraussetzung dafür ist, dass derjenige, der verschlüsselt kommunizieren möchte, diesem Dritten auch tatsächlich vertraut.

Nehmen wir also einmal mehr an, dass Angela eine verschlüsselte Nachricht aus der Uckermark an Bob in Jamaika schicken will, den sie nie zuvor getroffen hat. Bob hat seinen öffentlichen Schlüssel nicht von einer Zertifizierungsstelle bestätigen lassen, aber dafür von seinem alten Schulfreund Trent. Trent hat also ein Dokument, auf dem der Fingerprint von Bobs Schlüssel, Bobs Name und seine E-Mail-Adresse stehen, mit seinem privaten Schlüssel signiert und damit ein entsprechendes Zertifikat erzeugt.

Glücklicherweise kennen Trent und Angela sich ebenfalls (die beiden haben sich auf einer Konferenz in Miami kennengelernt, als sie im Shuttle-Bus nebeneinander saßen). Angela

vertraut Trent und somit auch seinem Zertifikat, mit dem er bestätigt, dass Bobs öffentlicher Key tatsächlich Bob gehört. Auf diese Art kommt also eine sogenannte *Chain of Trust* (Kette des Vertrauens) zwischen Angela und Bob zustande, ohne dass diese beiden sich persönlich kennen.

Unser Beispiel war allerdings nicht sehr realistisch – dass Angela in der Uckermark und Bob auf Jamaika zufällig einen gemeinsamen Freund haben, ist doch recht unwahrscheinlich. Ein klein wenig wahrscheinlicher ist es, dass sie gemeinsame flüchtige Bekannte haben, denen sie etwas vertrauen, aber nicht so sehr wie einem engen Freund wie Trent. Noch wahrscheinlicher ist es, dass sie keine direkten gemeinsamen Bekannten haben, sondern Angela einen Freund hat, dessen Cousine mal mit der Frau von einem Arbeitskollegen von Bob auf einem Seminar war.

Six degrees of separation – oder: Wie klein die Welt (manchmal) ist

Glauben Sie nicht? Der Sozialwissenschaftler Stanley Milgram hat 1967 sogar vermutet, dass zwei beliebige Personen auf der Welt durch nicht mehr als sechs Bekanntschaften miteinander verbunden sind. Zu diesem Schluss kam er nach einem Experiment, in dem Versuchspersonen Postpakete an ihnen unbekannte Adressaten weiterleiten sollten. Erlaubt war nur, die Pakete an persönliche Bekannte zu schicken, die diese dann wiederum an Bekannte schicken sollten. Dies wurde als das *Kleine-Welt-Phänomen* oder »Six degrees of separation« (wörtlich übersetzt »sechs Trennungsgrade«) bekannt. Sicher ist dieses Konzept eine ziemlich grobe Verallgemeinerung der tatsächlichen Verhältnisse, zum Beispiel erreichte nur ein kleiner Teil der Pakete sein Ziel. Seitdem wurden aber ähnliche Experimente per Telefon, E-Mail und in elektronischen sozialen Netzwerken durchgeführt, sodass die ursprüngliche (doch recht umstrittene) Theorie weiter ergänzt werden konnte.

Mittlerweile weiß man, dass Personen mit vielen sozialen Beziehungen und Personen mit einzelnen geografisch weitreichenden Beziehungen, die sozusagen mehrere Unternetzwerke miteinander verbinden, eine wichtige Rolle spielen, damit Kommunikationspfade nicht zu lang werden. In diesem Beispiel sind es nicht mehr zwei Trennungsgrade zwischen Angela und Bob (wie im Beispiel mit Trent), sondern schon fünf:

1. Angela zu ihrem Freund

2. Freund zu Cousine

3. Cousine zur Frau des Arbeitskollegen

4. Frau des Arbeitskollegen zu Arbeitskollegen

5. Arbeitskollege zu Bob

Die Chain of Trust zwischen Angela und Bob hätte also in diesem Beispiel eine Länge von 5.

Natürlich ist die Zertifizierung von Bobs Schlüssel auf diesem Weg für Angela sehr viel unsicherer als über Trent. Auf dem Weg zwischen ihr und Bob liegen schließlich vier Personen, die sie nicht persönlich kennt. Eine oder mehrere davon könnten unzuverlässig sein. Man könnte also sagen, dass eine Chain of Trust mit zunehmender Länge immer unzuverlässiger wird.

Eine einzelne Chain of Trust, insbesondere eine lange, ist also nicht ausreichend, wenn man wirklich Sicherheit über die Identität eines Schlüsselinhabers haben möchte. Hier kommt das Web of Trust ins Spiel: Wenn Angela nicht nur einen Freund hat, der seine E-Mails verschlüsselt und öffentliche Schlüssel anderer Leute signiert, sondern zwanzig Freunde, von denen jeder wieder viele Menschen kennt, die öffentliche Schlüssel zertifizieren, dann führt vielleicht nicht nur eine Kette von Angela zu Bob, sondern fünf oder zehn.

Die Wahrscheinlichkeit, dass sich in jeder Kette eine unzuverlässige Person befindet, nimmt mit der Anzahl der Ketten ab. Je dichter das Web of Trust ist und je mehr Signaturen das Zertifikat von Bobs Schlüssel hat, desto sicherer kann Angela sich über Bobs Identität sein. Auf dem Web of Trust beruht beispielsweise der PGP/GnuPG-Standard, auf den wir ebenfalls später noch genauer eingehen werden.

Diese Struktur ist also nicht hierarchisch und somit auch nicht durch einen erfolgreichen Angriff auf eine einzige wichtige Zertifizierungsstelle zu kompromittieren. Angenommen, Eve wollte Angela ihren eigenen öffentlichen Schlüssel anstelle von Bobs unterschieben, damit sie Angelas Nachrichten lesen kann: Eve könnte zwar beliebig viele Personen erfinden, die diesen gefälschten Schlüssel signieren, aber da Angelas Bekannte keine dieser erfundenen Personen kennen, bringt Eve das gar nichts. Vielleicht gibt es einen unzuverlässigen Bekannten von Bob, der unachtsam, desinteressiert oder bestechlich ist. Eventuell lässt er sich deswegen sogar von Eve dazu bringen, ihren gefälschten Schlüssel in Zusammenhang mit Bobs Namen zu zertifizieren. Auf diesem Weg könnte Eve eine einzige Vertrauenskette fälschen. Wenn allerdings ein dichtes Web of Trust existiert, fällt dies jedoch nicht weiter ins Gewicht.

Nur wenn das Netzwerk so spärlich ist, dass Angela sich auf eine einzige Kette verlassen muss, wird die Sicherheit von Angelas Kommunikation in Gefahr gebracht. Anders als im Fall der hierarchischen PKI bezieht sich dieses Risiko aber wirklich nur auf Angelas Kommunikation und nicht auf die aller anderen, die sich auf dieselbe Zertifizierungsstelle im hierarchischen Modell verlassen. Andererseits ist ein Angriff auf eine Einzelperson möglicherweise einfacher zu bewerkstelligen als der Angriff auf eine professionelle Zertifizierungsstelle.

Sie sehen also, dass beide Ansätze ihre Vor- und Nachteile haben. Eine wesentliche Stärke des Web of Trust ist seine Robustheit gegenüber dem Ausfall einzelner Knoten, also einzelnen unzuverlässigen Personen oder einzelnen Schlüsseln, deren Sicherheit kompromittiert wurde. Diesen Vorzug teilt es mit dem Internet selbst, das auch dezentral konstruiert wurde, um beim Ausfall einzelner Server (beispielsweise im Falle eines militärischen Angriffs) immer noch eine Kommunikation zwischen den verbleibenden Servern zu ermöglichen.

Das Web of Trust ist dem hierarchischen Modell dann überlegen, wenn es sich tatsächlich um ein dichtes Netz handelt. In diesem Fall kann es seine Vorteile ausspielen. Für eine Angela, die nur wenige direkte Kontakte hat, ist es schwer, ihr unbekannte Personen über eine oder gar mehrere Chains of Trust zu erreichen. Andererseits kann sie die Dichte und Reichweite ihres Netzes selbst verbessern, indem sie mehr persönliche Kontakte zu Leuten knüpft, die viele öffentliche Schlüssel signieren. Hierzu bietet sich zum Beispiel der Besuch von Key-Signing-Parties an, die häufig auf IT-Fachkonferenzen oder auch im Rahmen von sogenannten Cryptoparties stattfinden. Eine Übersicht über geplante Veranstaltungen in Ihrer Region finden Sie auf https://www.cryptoparty.in. Oder Sie veranstalten einfach Ihre eigene Key-Signing-Party!

2.5 Vertrauen ist gut, Open Source ist besser

Wie wir weiter oben schon kurz erwähnt haben, arbeitet ein Computer mit binären Zahlen, also Zahlen, die nur durch Abfolgen von 0 und 1 dargestellt werden. Das ist deshalb so, weil unsere heutigen Computer mit elektrischem Strom betrieben werden. Dieser kennt im Grunde nur zwei definierte Zustände: an und aus, also 1 und 0. Um einen Rechner in den Pioniertagen der Informatik mit Informationen und vor allem mit Instruktionen zu füttern, musste man sie vorher von Hand in diese Maschinensprache übersetzen. Eine solche Herangehensweise ist bei der heutigen Komplexität der Rechner und der an sie gestellten Anforderungen weitestgehend

unmöglich. Stattdessen existieren für nahezu jeden Anwendungszweck unzählige hoch entwickelte Programmiersprachen, mit deren Hilfe nahezu alles vom einfachen Tic-Tac-Toe-Spiel über Webdienste wie Facebook und Twitter bis hin zu selbstlernenden neuralen Netzen realisiert werden kann. Damit ein Computer allerdings die Anweisungen eines Menschen versteht, müssen diese von der jeweiligen Programmiersprache in die Maschinensprache übersetzt werden. Ein Programm, das menschenlesbaren Programmcode hin zu einem computerverständlichen Binärcode (also Abfolgen von 1 und 0) umwandelt, nennt man Compiler. Den eigentlichen Vorgang der Übersetzung bezeichnet man als Kompilieren.

2.5.1. Closed Source

Die allermeisten Menschen (auch Informatiker) können Maschinencode nicht schnell genug lesen und verstehen, um zu begreifen, was er tut, und ihn dann womöglich auch noch zu verändern. Für die Hersteller von Computerprogrammen aller Art ist das praktisch, da Konkurrenten sich beispielsweise nicht einfach anschauen können, warum die Software des Wettbewerbers so viel besser funktioniert als die eigene. Des Weiteren lassen sich Software-Updates und Erweiterungen viel einfacher verkaufen, wenn die Nutzer diese nicht selbst entwerfen können. Daher belassen es Softwarehersteller oft dabei und liefern nur die fertigen, kompilierten Programme ohne den ursprünglichen Programmcode aus, der auch als Source Code oder Quellcode bezeichnet wird. Software, deren Quellcode nicht frei verfügbar ist, wird als *Closed Source* (englisch für »geschlossene Quelle«) oder auch als *proprietär* bezeichnet.

2.5.2. Open Source

Es gibt allerdings auch Software, deren Quellen ungehindert für die Allgemeinheit einsehbar sind. Diese wird auch als *quelloffen* oder *Open Source* bezeichnet. Meistens wird dabei der Quellcode über Webseiten oder spezielle Plattformen wie beispielsweise *GitHub*[4] verbreitet. Dort darf sich jeder Interessierte die Quelltexte herunterladen und selbst in Maschinencode übersetzen, den er auf seinem Rechner ausführen und testen kann. Eines der bekanntesten Programme dieser Art kennen Sie vielleicht: Es ist der Linux-Kernel, der Kern aller Linux-Betriebssysteme, welcher beispielsweise auch in Android-Mobiltelefonen steckt. Aber auch der Browser Mozilla Firefox, das E-Mail-Programm Thunderbird und die meisten Webserver, die für die Übertragung von Webseiten auf Ihren Browser zuständig sind, sind Open-Source-Software. Viele dieser Anwendungen werden von passionierten Programmierern freiwillig in

ihrer Freizeit betreut und weiterentwickelt. Allerdings bezahlen oft auch Unternehmen professionelle Softwareentwickler dafür, dass sie gemeinsam mit den Freiwilligen an quelloffener Software arbeiten. Das ist vor allem dann der Fall, wenn das Unternehmen Dienstleistungen und Produkte auf Basis von Open-Source-Programmen anbietet.

2.5.3. Vertrauen ist gut, Kontrolle ist besser

Sie werden sich nun vielleicht fragen, welchen Unterschied es für Sie persönlich macht, ob die von Ihnen verwendete Software nun quelloffen ist oder nicht.

Oft führen Hersteller proprietärer Software an, dass ihre Produkte angeblich wesentlich sicherer seien. Angreifer könnten eben aufgrund des unter Verschluss gehaltenen Programmcodes Sicherheitslücken nicht so einfach aufspüren. Außerdem könne dann bei Abschluss entsprechender Verträge viel umfassendere Unterstützung in Problemfällen geleistet werden.

Tatsächlich aber ist Open Source vor allem aufgrund des für jeden verfügbaren Programmcodes oft wesentlich sicherer als Closed Source. Da sich bei großen Projekten viele verschiedene Menschen mit dem Quellcode der jeweiligen Programme beschäftigen, fallen Sicherheitsprobleme oder Fehler einfach schneller auf und werden in der Regel auch entsprechend schnell durch die Gemeinschaft behoben. Hersteller von Closed-Source-Software haben in vielen Fällen gar nicht die personellen Kapazitäten, um schnell genug zu reagieren. Auch ist die Verlockung oft groß, sicherheitsrelevante Aspekte dem Unternehmensgewinn unterzuordnen: Dann werden Sicherheitsprobleme gerne mal verschwiegen, zumindest, bis man selbst eine Lösung anbieten kann.

Mittlerweile haben viele große und kleine Unternehmen die Stärken von Open-Source-Software erkannt und unterstützen entsprechende Projekte monetär und auch personell. Andere haben neue Geschäftsmodelle auf Basis von Open Source entwickelt und sind damit sehr erfolgreich.

2.6 Sicherheit offline – Schultersurfen & Co.

Bisher haben Sie in diesem Kapitel viel über Computersicherheit gelernt – symmetrische und asymmetrische Verschlüsselung, Passwörter, Hashes, Signaturen, Public-Key-Infrastruktur und andere wichtige Konzepte. Alle diese technischen Dinge sind dazu gedacht, Sie gegen Angreifer

zu schützen, die Ihnen online begegnen. Ihre digitale Privatsphäre kann jedoch auch durch Angriffe gefährdet sein, die offline und ohne »High-Tech« erfolgen. Das heißt im Wesentlichen, dass ein Angreifer sich verschiedenster zwischenmenschlicher Tricks bedient, um zu seinem Vorteil an Ihre persönlichen Daten zu gelangen. Das können Zugangsdaten zu Onlineplattformen sein, die TAN-Listen für Ihr Onlinebanking und vieles mehr. Obwohl diese Vorgehensweisen nicht im eigentlichen Fokus dieses Buches liegen, möchten wir trotzdem an dieser Stelle kurz auf sie eingehen.

Wie in der digitalen Welt beruhen auch diese Angriffe darauf, Schwachstellen auszunutzen – allerdings nicht die Schwachstellen einer Software, sondern die von Menschen und Organisationen. Das Ausnutzen dieser Schwächen wird daher auch als *Social Engineering* bezeichnet, was man in diesem Zusammenhang mit »soziale Manipulation« übersetzen kann. In der Fachliteratur haben sich englische Bezeichnungen für verschiedene Arten des Social Engineerings durchgesetzt.

Bei den meisten dieser Angriffe handelt es sich um simple zwischenmenschliche Kniffe und Täuschungen. Vielleicht sind sie sogar so offensichtlich, dass Sie während des Lesens der folgenden Abschnitte anzweifeln werden, dass Sie selbst jemals auf einen so dreisten Trick hereinfallen würden. Denken Sie aber daran, dass Sie im Moment allein schon deswegen sensibilisiert sind, weil Sie dieses Buch lesen. Außerdem sind Sie im Moment (hoffentlich) nicht in Eile oder abgelenkt. Wenn Sie das nächste Mal am Bahnhof kurz Ihre E-Mails auf dem Laptop checken wollen oder an Ihrem Arbeitsplatz von einer offiziell klingenden Person angerufen werden, während Sie in Gedanken eigentlich schon in der Kantine sind, könnte Ihre Reaktion schon ganz anders aussehen. Und glauben Sie uns, schon gestandene Informatiker und andere Experten sind auf simple Tricks hereingefallen.

Im Folgenden also zu einigen verbreiteten Angriffstechniken, mit denen Eve versuchen könnte, Bobs Daten offline auszuspähen.

2.6.1. Impersonating

Eine der einfachsten Arten, wie Eve sich unberechtigt Informationen verschaffen kann, ist es, sich als jemand auszugeben (englisch »impersonate«), dem Bob vertraut. Das kann in der Regel kein Freund oder Bekannter von Bob sein, da es im persönlichen Kontakt viel schwerer ist, eine bestimmte andere Identität anzunehmen; schließlich identifizieren wir unsere Freunde nicht

anhand ihres Namens, sondern ihres Gesichts, der Stimme, des Gangs und anderer schwer zu fälschender Merkmale.

Viel einfacher ist es für Eve, sich in jemanden zu verwandeln, dem Bob von Berufs wegen vertraut, beispielsweise eine Mitarbeiterin von Bobs Telefonanbieter oder Internetprovider. Wenn sie daran interessiert ist, Bobs E-Mail-Passwort zu erfahren, könnte sie beispielsweise erfragen, mit welchem Benutzernamen und Passwort er sich im Kundenportal des Telefonanbieters anmeldet. Da Menschen gern das gleiche Passwort (oder leichte Abwandlungen davon) für verschiedene Zwecke benutzen, hätte sie anhand dieser Daten gute Chancen, sich Zugang zu Bobs E-Mail-Postfach zu verschaffen. Ein beliebter Vorwand, um Bobs Anmeldedaten zu erfragen, ist beispielsweise das Angebot, Bobs Telefonvertrag auf einen günstigeren Tarif umzustellen. Vermutlich noch beliebter ist ironischerweise das Märchen, dass Bobs Anmeldedaten gehackt wurden; Eve fordert ihn dann auf, zur Wiederherstellung der Datensicherheit sein altes Passwort mitzuteilen und ein neues zu wählen. Das neue kommt natürlich nie zur Anwendung, während Eve mithilfe von Bobs altem Passwort nun Zugriff auf sein Postfach hat.

Um einer Eve solche Angriffe zu erschweren, sollten Sie Folgendes beachten: Geben Sie unter keinen Umständen Ihr Passwort am Telefon oder persönlich heraus! Egal, wie offiziell die fragende Person wirkt. Kein echter Mitarbeiter eines Providers oder irgendeines anderen Unternehmens, das zumindest ein grundlegendes Verständnis von Datensicherheit hat, wird jemals nach Ihrem Passwort im Klartext fragen.

Sollten Sie daran zweifeln, dass ein Anrufer der ist, der er vorgibt zu sein, lassen Sie sich einfach seinen Namen, Abteilung und Telefonnummer geben. Rufen Sie ihn dann zurück oder fragen Sie in der Zentrale der Firma nach, ob besagter Mitarbeiter unter dieser Telefonnummer dort bekannt ist.

2.6.2. Phishing

Beim Phishing (abgeleitet von »Fishing«, also Fischen) handelt es sich gewissermaßen um die unpersönliche Form des Impersonating: Eve gibt sich nicht persönlich oder am Telefon als jemand anderes aus, sondern mittels einer gefälschten E-Mail. Diese verleitet Bob entweder dazu, persönliche Informationen seinerseits mitzuteilen, oder sie enthält einen Link auf eine ebenfalls gefälschte Webseite. Dies kann beispielsweise ein optischer Klon einer bekannten

Firmenseite wie Paypal oder Amazon sein, auf der Bob dann aufgefordert wird, seine Anmeldedaten einzugeben, die auf diese Art direkt bei Eve landen.

Um solche Angriffe zu erkennen, sollten Sie bei offiziell aussehenden E-Mails mit Tippfehlern, komplizierten Absenderadressen oder ungewohnt aussehenden Log-in-Seiten bekannter Firmen misstrauisch werden. Überprüfen Sie die Adresszeile Ihres Browsers und achten Sie auf das Symbol für eine verschlüsselte Verbindung (siehe auch Kapitel 3) – gehört die aufgerufene Webseite wirklich zum erwarteten Unternehmen?

Des Weiteren würde Ihre Hausbank Sie beispielsweise niemals zur Eingabe gleich mehrerer TAN-Nummern auf einmal auffordern. Hierbei gilt: Wenn eine Bank, oder Behörde etwas Wichtiges von Ihnen möchte, schickt Sie Ihnen auch im digitalen Zeitalter immer noch einen guten alten Brief nach Hause. Im Zweifel genügt hier sogar oft ein einfacher Anruf beim vermeintlichen Urheber der Nachricht, um für Klarheit zu sorgen.

2.6.3. Shoulder Surfing

Beim Shoulder Surfing (Schultersurfen) versucht ein Angreifer, persönliche Informationen von Ihrem Bildschirm oder Ihrer Tastatur mitzulesen. Das können die Ihres Laptops sein, aber auch die Tasten des Bankautomaten, auf der Sie Ihre PIN eingeben. Auf Bankautomaten sind mittlerweile fast überall Aufkleber angebracht, die Sie daran erinnern, Ihre Eingabe mit der Hand gegen Schultersurfer abzuschirmen. Denken Sie aber auch daran, dass Ihr Nachbar im Zug (auch der in der Sitzreihe hinter Ihnen) leicht mitlesen kann, was Sie mit der Tastatur schreiben oder auf Ihrem Bildschirm anzeigen. Machen Sie es sich daher zur Gewohnheit, keine Passwörter im Blickfeld unbekannter Personen einzugeben. Ein verwandter Fallstrick ist die Eingabe von Passwörtern bei Bildschirmpräsentationen (insbesondere auf Tablet-Computern, auf denen jeder Buchstabe des Passwortes kurz angezeigt wird) oder bei Telekonferenzen.

Auch Smartphones sind beliebte Ziele für das Shoulder Surfing. Bedenken Sie auch bei der Eingabe Ihres Entsperrcodes, dass sich Muster und Zahleneingaben mit fettigen Fingern auf Touch-Displays ganz besonders gut nachvollziehen lassen! Auch können beispielsweise die Fingerabdrücke auf Ihrem Smartphone verwendet werden, um (mit einigen Hilfsmitteln und etwas Geduld und Geschick) den Fingerabdrucksensor von iPhones der neueren Generation zu umgehen. Es kann also nicht schaden, dem Smartphone gelegentlich mal eine liebevolle

Reinigung mit einem fettlöslichen Mittel, beispielsweise einem Brillenputztuch, zukommen zu lassen.

Der Bildschirm eines Laptops ist etwas schwerer zu schützen. Zu diesem Zweck gibt es allerdings sogenannte Blickschutzfilter. Das sind flache Scheiben oder Folien, die auf dem Bildschirm platziert werden und bewirken, wie Sie in Abbildung 2.8 sehen, dass der Bildschirminhalt nur noch aus einem Winkel von annähernd 90 Grad erkennbar ist. Sie selbst können den Text auf Ihrem Bildschirm also lesen, Ihr Sitznachbar im Zug aber nicht. Einen derartigen Filter können Sie natürlich nur anbringen, wenn Sie Ihren eigenen Laptop benutzen. Wenn Sie unterwegs fremde Computer verwenden, beispielsweise in einem Internetcafé, sollten Sie prinzipiell davon ausgehen, dass alle eingegebenen oder angezeigten Daten in falsche Hände geraten könnten.

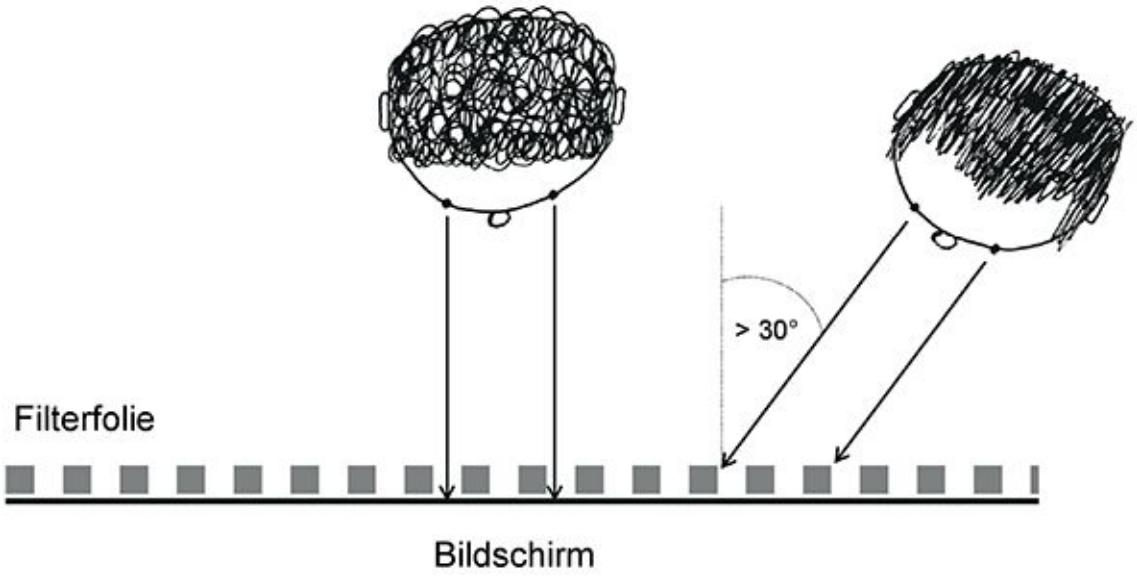


Abb. 2.8 Funktionsweise Blickschutzfilter

2.6.4. Dumpster Diving

Beim Dumpster Diving, wörtlich »Mülleimertauchen«, sucht Eve nach verwertbaren Informationen in Bobs Müll. Sie kann hierbei nicht nur auf vertrauliche Briefe und Rechnungen stoßen, sondern auch auf Kreditkarten, Festplatten und andere noch lesbare Datenträger.

Wenn der Angriff nachts erfolgt, geht Eve nur ein geringes Risiko ein, entdeckt zu werden. Tagsüber ist ihr Risiko höher. Allerdings spekuliert sie eventuell darauf, dass nur wenige Leute

genug Interesse für ihre Umwelt aufbringen, um sie nach dem Grund ihrer Wühlerei in Bobs Müll zu fragen.

Um solche Angriffe auf Ihre Daten zu verhindern, denken Sie daran, niemals einen noch lesbaren Datenträger in den Müll zu werfen! Bank-, Kreditkarten können Sie zerschneiden, CDs zerbrechen. Bei *Festplatten* reicht allerdings die einfache Löschung der Dateien nicht aus. Hierbei werden nämlich nicht die Daten selbst, sondern nur ihre Indexierung im Inhaltsverzeichnis der Festplatte aufgehoben. Wenn Sie die Festplatte danach weiter verwenden, hören die eigentlichen Daten erst nach und nach auf, physikalisch zu existieren, da Sie sie mit neuen Daten überschreiben. Es gibt spezielle Programme, um den Inhalt von Festplatten so zu entfernen, dass dieser im Nachhinein nicht mehr rekonstruierbar ist. Dazu wird der gesamte Datenträger zunächst mehrfach mit Zufallsdaten (Datenmüll) überschrieben und dann noch neu formatiert. Kostenlose Programme, die dies können, sind beispielsweise *Darik's Boot and Nuke (DBAN)* und *Parted Magic*. Wie Ihnen bestimmt einleuchtet, ist es sinnvoll, diese Programme beispielsweise von einem bootfähigen USB-Stick oder einer DVD aus zu starten und nicht von der Festplatte, da ja die ganze Festplatte gelöscht werden soll.

Falls beim sicheren Löschen ein Fehler auftritt, hilft nur noch die physikalische Zerstörung der Festplatte. Hier dürfen Sie sich beispielsweise eines Hammers bedienen (je nach Leidensfähigkeit Ihrer Nachbarn besser nicht nach zehn Uhr abends). Auch ein starker Magnet zerstört die Festplatte – wenn Sie allerdings wie die meisten keinen Zugang zu einem wirklich starken Magneten wie einem MRT haben, ist es schwierig herauszufinden, wann eine Festplatte durch einen Magneten oder einen Induktionsherd wirklich ausreichend gelöscht ist.

[1] Das wird ganz schön teuer. Alice und Bob sollten besser auf E-Mail umsteigen.

[2] Dies ist etwas vereinfacht – mithilfe sogenannter »Rainbow Tables« können letztendlich doch Passwörter rekonstruiert werden, aber nur bei einem ungeeigneten Hash-Verfahren und zu kurzen Passwörtern.

[3] http://guerrillagardening.org

[4] http://www.github.com

Kapitel 3 Sicher surfen im Web

In den letzten beiden Kapiteln haben wir als Beispiele für sichere (und unsichere) Kommunikation vor allem E-Mail herangezogen. Klar geraten beim E-Mailen Ihre Daten in Gefahr – Sie schicken Sie ja in die ganze Welt hinaus. Anders dagegen beim Surfen – da sind Sie ja vor allem ein passiver Leser, der kaum etwas über sich verrät. Richtig? Falsch!

Schon in den Frühzeiten der Technologie war das World Wide Web kein Read-only-Medium, und im Laufe der Zeit ist die Interaktivität des Webs immer wichtiger geworden. Marketingmenschen haben eine Zeit lang gern vom Web 2.0 gesprochen, wenn sie diesen Sachverhalt meinten. Eigentlich ist die Interaktivität aber immer schon inbegriffen, wenn man vom Web spricht. Das soll sich auch gar nicht ändern, denn sonst könnten Sie ja genauso gut wieder anfangen, Videotext zu lesen.

Wie sonst im Leben bringt auch im Web die Vielfalt der Möglichkeiten einiges an Stolperfallen mit sich. Damit Sie diesen aus dem Weg gehen können, erklären wir Ihnen zuerst kurz, wie das WWW eigentlich funktioniert.

3.1 Das Internet in der Nussschale

Wenn vom Internet die Rede ist, denken die meisten Leute an das *World Wide Web (WWW)*, obwohl es streng genommen nur ein Teil des Internets ist. Im WWW »wohnen« die Webseiten, von Amazon und Ebay über das Fahrkartenportal der Deutschen Bahn bis hin zum privaten Blog, auf dem der Student von nebenan die Fotos von seinem Abendessen postet.

Aus technischer Sicht besteht das Web aus den Daten, die über das sogenannte *Hypertext Transfer Protocol (HTTP)* von einem Computer zum anderen übertragen werden. Aus gesellschaftlicher Sicht ist es allerdings weit mehr: ein universeller Dienst, über den die Menschheit so ziemlich alles abwickelt, was sich in irgendeiner Art und Weise auf elektronischem Wege erledigen lässt. Genau dieser Umstand macht es so attraktiv für das Abfischen und Manipulieren von Daten.

3.1.1. Kurze Geschichte des WWW

Das World Wide Web entstand 1989 im europäischen Kernforschungszentrum CERN. Es wurde von dem englischen Physiker und Informatiker Tim Berners-Lee und dem (heute weniger bekannten) belgischen Informatiker Robert Cailliau entworfen – ursprünglich als einfache Möglichkeit, wissenschaftliche Artikel zu veröffentlichen und miteinander zu verknüpfen.

Einer der zwei grundlegenden Bausteine war das schon erwähnte Hypertext Transfer Protocol[1]. In den Anfangszeiten des Web gab es noch ein paar ähnliche Protokolle – im Gegensatz zu diesen war HTTP jedoch frei und kostenlos verfügbar, sodass es sich innerhalb weniger Jahre durchsetzen konnte.

Der zweite wichtige Baustein war die Auszeichnungssprache *Hypertext Markup Language (HTML)*. Mit ihr ließen sich Texte ohne großen Aufwand strukturieren, formatieren und durch sogenannte *Hyperlinks* (kurz »Links« genannt) miteinander verknüpfen.

1993 wurde dann auch schon der erste massentaugliche *Browser*namens »Mosaic« veröffentlicht – massentauglich, weil er erstmals die Möglichkeit bot, Webseiten auch grafisch darzustellen. Zuvor hatten Browser, also Programme zum Darstellen der Inhalte des WWW, nur Schrift angezeigt. Mosaics Vater war der erst 22 Jahre alte Informatiker Marc Andreessen, der damals am National Center for Supercomputing Applications der University of Illinois arbeitete. Mosaic bescherte dem jungen World Wide Web ein explosionsartiges Wachstum. Andreessen gründete später die Firma Netscape Communications und benannte Mosaic in Netscape Navigator um – die langjährigen Internetnutzer unter Ihnen können sich an den Netscape-Browser vielleicht noch erinnern. Netscape wurde dann später von AOL aufgekauft, die Netscape noch bis 2008 halbherzig weiterführten. Außerdem ging aus Netscape das Mozilla-Projekt hervor, dessen Produkte Firefoxund Thunderbird heute ein weit verbreiteter Browser beziehungsweise E-Mail-Client sind.

Der ursprüngliche Zweck des WWW, das Anzeigen und Verlinken wissenschaftlicher Texte, macht heute nur noch einen Bruchteil der Aktivität im WWW aus. Stattdessen lesen wir Blogs, schauen Serien und lustige Katzenvideos, spielen Spiele, tätigen Banküberweisungen, kaufen online ein und vieles mehr. Um all das leisten zu können, sind heutzutage im WWW noch einige andere Technologien neben HTTP und HTML notwendig, die Sie im Weiteren ein bisschen kennenlernen werden. (Aber keine Angst, wir wollen Sie hier nicht zum Netzwerkspezialisten oder zur Webentwicklerin ausbilden – wir fassen uns kurz.)

Die Konzepte, auf denen das WWW basiert, stammen wie schon besprochen aus der Steinzeit des Internets – aus einer Zeit, in der ein Internetanschluss nur wenigen Menschen auf der Welt zur Verfügung stand. Sicherheit spielte daher bei der Entstehung des WWW erst einmal eine untergeordnete Rolle. Außerdem wurde sie im weiteren Verlauf der Geschichte allzu oft einer Fülle von Funktionen geopfert, mit der die großen Browser-Hersteller um Nutzer buhlten. Als mit zunehmender Verbreitung des WWW auch die Fälle von Betrug und Datendiebstahl nicht mehr zu ignorieren waren, gewann endlich auch das Thema Sicherheit an Bedeutung. Aus diesem Grund wurden und werden nachträglich immer wieder Sicherheitsmechanismen auf vorhandene Technologien aufgestöpselt, um die Nutzer (manchmal auch vor sich selbst) zu schützen. Der folgende Abschnitt soll Ihnen dabei helfen, die nötigen technischen Grundlagen zu verstehen, um Risiken abzuschätzen und angemessen auf Gefahren reagieren zu können.

3.1.2. Das Hypertext Transfer Protocol (HTTP)

HTTP bildet, wie bereits zu Beginn dieses Kapitels erwähnt, die eigentliche Grundlage des World Wide Web. Aus diesem Grund lohnt es sich, die dahinterliegenden Abläufe einmal genauer unter die Lupe zu nehmen.

Die Anfrage – Request

Die Kommunikation über HTTP erfolgt immer zwischen einem Client (zum Beispiel Ihrem Webbrowser) und einem Webserver. Der Webserver ist ein spezielles Dienstprogramm auf dem Computer, der eine Website bereitstellen soll. Der Client stellt einen sogenannten Request (Anfrage) an den Server, der wiederum mit einer Response (Antwort) antwortet. Sowohl Request als auch Response bestehen aus jeweils zwei Teilen: dem Header, der aus Steuerungsinformationen besteht, und dem Body (auch Payload genannt), der die eigentlichen Nutzdaten enthält. Nutzdaten sind beispielsweise der HTML-Code einer Webseite oder die Binärdaten eines Bildes, das Sie hoch- oder herunterladen. Nach dem Erhalt einer Antwort wird der Kommunikationskanal zwischen Client und Server geschlossen[2], weshalb man im Falle von HTTP auch von einem *verbindungslosen* Protokoll spricht. Diese Eigenschaft wird vor allem dann interessant, wenn es um Authentifizierung gegenüber Webdiensten oder um Werbetracking geht – dazu später mehr.

```
GET /gut-geruestet/http-test.html HTTP/1.1
Host: www.cryptocheck.de
```

Im obigen Beispiel sehen Sie die Anfrage, die Ihr Browser an einen Webserver stellt, wenn Sie die URL http://www.cryptocheck.de/gut-geruestet/http-test.html in die Adresszeile eingeben oder einen entsprechenden Hyperlink auf einer Webseite angeklickt haben. Der *Uniform Resource Locator (URL)* ist eine Adresse, die angibt, über welchen Dienst (hier: HTTP) von welchem Server (hier: www.cryptocheck.de) welche Ressource (hier die Seite: /gut-geruestet/http-test.html) abgerufen werden soll. Der Browser zerlegt diese Angaben nun so, dass der Webserver sie verstehen kann, und stellt einen entsprechenden Request an den Server. Das Wort GET kennzeichnet, dass der Browser nur lesend auf die Ressource zugreifen möchte. Diese Kennzeichnung der Zugriffsart wird HTTP-Methode genannt. Auf GET folgt der Name der Ressource und die Protokollversion, die der Browser für die Kommunikation erwartet – in diesem Falle wäre das also HTTP/1.1. Zu guter Letzt wird dem Webserver durch die Angabe des Header-Attributes Host mitgeteilt, unter welcher *Domain* die angefragte Ressource zu finden sein soll. Dies ist erforderlich, da ein einzelner Webserver für viele verschiedene Seiten zuständig sein kann, die aber alle über dieselbe IP-Adresse erreicht werden. Durch den Inhalt des Host-Feldes kann der Webserver bestimmen, welcher Webseite die Anfrage konkret gilt. Für einen sogenannten GET-Request sind keine Nutzdaten erforderlich, daher ist in diesem Beispiel nur der Request-Header zu sehen.
Im Gegensatz dazu beinhaltet ein sogenannter POST-Request in jedem Falle Nutzdaten.

```
POST /gut-geruestet/upload.html HTTP/1.1

Host: www.cryptocheck.de

Content-Type: application/x-www-form-urlencoded
Content-Length: 256

[Daten]
```

Analog zum GET-Request zeigt der Browser dem Webserver mittels des Wortes POST an, dass er im weitesten Sinne schreibend auf die Ressource /gut-geruestet/upload.html zugreifen möchte – beispielsweise, um ein Bild hochzuladen. Die Header-Felder Content-Type und Content-Length zeigen dem Server Art und Größe der Daten an, die dann im Request-Body übertragen werden.

Für HTTP stehen noch eine Vielzahl anderer Zugriffsmethoden zur Verfügung, die alle eine bestimmte Aufgabe haben. Für das tägliche Surfen im Web und ein grundlegendes Verständnis des Protokolls spielen diese allerdings keine Rolle.

Die Antwort – Response

Wie eingangs erwähnt, folgt auf eine Anfrage des Clients immer eine Antwort des Servers. Diese enthält ebenfalls stets einen Header mit Steuerungs- sowie Metainformationen und in den meisten Fällen auch Daten (Body), welche an den Client ausgeliefert werden sollen.

HTTP/1.1 200 OK

Server: nginx/1.6.2

Date: Sun, 29 Mar 2015 10:13:02 GMT

Content-Type: text/html

Content-Length: 8592

Last-Modified: Fri, 27 Mar 2015 17:16:26 GMT

[Daten]

Besagte Daten können so ziemlich alles sein – eine Webseite (also HTML-Code), ein Bild, Videodaten, Audiodaten und so weiter. Das Header-Attribut Content-Type ist die Empfehlung an den Client, wie die Daten zu verarbeiten sind.

3.1.3. Hypertext Markup Language (HTML)

Wenn Sie also eine Webseite (beispielsweise http://www.cryptocheck.de/gut-geruestet/http-test.html) aufrufen, wird zunächst HTML-Code zurückgegeben und von Ihrem Browser eingelesen. HTML ist eine sogenannte Auszeichnungssprache, sie beschreibt sowohl den Aufbau als auch den Inhalt einer Webseite. Ihr Browser interpretiert die enthaltenen Anweisungen und errechnet eine entsprechende Anzeige. Dieser Vorgang wird auch *Rendering* genannt.

Hinweis

In Ihrem Browser können Sie den Quellcode einer Seite anschauen, indem Sie mit Ihrer rechten Maustaste in einen freien Bereich der Website klicken und im dargestellten Kontextmenü »Seitenquelltext anzeigen« auswählen.

Das empfangene HTML-Dokument enthält meistens zusätzliche Anweisungen, die den Browser dazu veranlassen, weitere Inhalte (zum Beispiel Bilder oder Videos) vom Webserver abzurufen und in die Darstellung der Seite einzubetten. Für jedes nachgeladene Element wird wiederum ein HTTP-Request gesendet, die darauf folgende Response abgewartet und verarbeitet. Sie können sich vorstellen, dass dieser Umstand HTTP nicht gerade zu einem Inbegriff von Geschwindigkeit macht. Zwar können moderne Browser bis zu acht HTTP-Anfragen gleichzeitig an eine einzelne Domain stellen, allerdings erlaubt der HTTP/1.1-Standard, wenn man ihn denn genau nimmt, nur zwei gleichzeitige Verbindungen. Es ist dem Betreiber des Webservers überlassen, ob er sich an diesen Standard hält. Es muss also nicht unbedingt an Ihrem Internetanschluss liegen, wenn eine Seite sich merklich zäh aufbaut.

3.1.4. Sicheres HTTP: HTTPS

Nacktes HTTP ist alles andere als ein sicheres Protokoll: Alle zwischen Bob und Alice per HTTP übertragenen Daten, und dazu zählen natürlich auch Informationen aus Log-in-Masken oder webbasierte Chats, können von einer mäßig begabten Eve ohne Mühe ausgelesen und sogar unterwegs verändert werden, ohne dass Bob oder Alice es mitkriegen. Mit HTTP allein können Sie also weder die *Vertraulichkeit* noch die *Authentizität* einer Webseite sicherstellen. Um dieses Problem zu umgehen, führte Netscape 1994 das *Hypertext Transfer Protocol Secure*, kurz *HTTPS*, ein. Eine HTTPS-Verbindung wird durch eine Transportverschlüsselung mittels TLS geschützt.

Hinweis

Transport Layer Security

Transport Layer Security, kurz TLS, ist ein Netzwerkprotokoll, durch das eine verschlüsselte Datenverbindung durch ein nicht vertrauenswürdiges Netzwerk hergestellt wird. Dazu wird ein sogenanntes hybrides Verfahren verwendet, das heißt, die Kombination einer asymmetrischen und symmetrischen Verschlüsselung, wie in Kapitel 2 beschrieben.

Die alten Versionen von TLS waren unter dem Namen SSL (Secure Sockets Layer) bekannt. HTTPS-Verbindungen werden zum Beispiel beim Onlinebanking eingesetzt. Angenommen, Alice möchte Überweisungen bei ihrer Bank, der BobCredit, tätigen, die ihr dazu ein Onlinebanking-Portal anbietet: Damit Alice sich versichern kann, dass sie tatsächlich mit BobCredit kommuniziert und nicht mit Eve oder Mallory, ist zunächst ein sogenannter *Handshake* erforderlich. Beim Handshake präsentiert BobCredit Alice ein Zertifikat, anhand dessen sie sichergehen kann, dass sie tatsächlich mit dem Server von BobCredit kommuniziert. Umgekehrt kann auch Alices Computer dem BobCredit-Server mit einem Zertifikat ihre Identität beweisen. Nachdem sich beide Partner von der Identität des Gegenübers überzeugt haben, wird eine HTTPS-Verbindung aufgebaut, und Alice kann ihre Überweisung an BobCredit verschlüsselt kommunizieren, ohne die Gefahr, dass beispielsweise Mallory davon erfährt oder Eve den Betrag auf ihr Konto umleitet.

Die zur Verschlüsselung verwendete Chiffre ist bei einer TLS-Verbindung übrigens Verhandlungssache. Der Server der Bank zeigt beim Handshake an, welche Codierungsverfahren er unterstützt. Alices Computer versucht, daraus das Verfahren auszuwählen, das ihm am geeignetsten erscheint. Auch eine Neuverhandlung der verwendeten Chiffre während einer laufenden TLS-Verbindung ist möglich, wenn einer der beiden Teilnehmer diese anfordert. Die Sicherheit einer TLS-Verbindung steht und fällt mit den verwendeten Verschlüsselungsalgorithmen. Ein schlecht konfigurierter Server kann Alices Computer beispielsweise dazu bringen, eine gebrochene (also bereits entschlüsselte) Chiffre für die Kommunikation auszuwählen. Unter Umständen ermöglicht das wiederum Eve, den gesamten Datenverkehr simultan oder im Nachhinein zu entschlüsseln. Dies ist einer der Gründe dafür, warum Sie Ihre Software, insbesondere den Browser beziehungsweise Ihre Bankingsoftware, stets aktuell halten sollten: Verantwortungsvolle Hersteller entfernen unsichere Chiffren aus ihren Programmen oder setzen Sie zumindest davon in Kenntnis, dass diese Verbindung unsicher sein könnte. Wenn ein Dienst nun ausschließlich unsichere Verschlüsselungsverfahren zur TLS-geschützten Kommunikation anbietet, können Sie im Einzelfall entscheiden, ob Sie das Risiko eingehen möchten oder nicht.

Hinweis

HTTP/2

Am 18. Februar 2015 wurden die Arbeiten an *HTTP/2* als Nachfolger des in die Jahre gekommenen HTTP von der IETF erfolgreich abgeschlossen. In weiten Teilen wird das neue Webprotokoll auf einem Entwurf von Google beruhen. Es erlaubt beispielsweise das Zusammenfassen von einzelnen Anfragen und wird damit um ein Vielfaches schneller sein als sein Vorgänger. Anders als ursprünglich geplant wird die Kommunikation über HTTP/2 allerdings nicht standardmäßig verschlüsselt erfolgen. Mozilla und Google haben jedoch angekündigt, dass HTTP/2 sich in Firefox und Chrome nur in Verbindung mit einer TLS-Verschlüsselung nutzen lassen wird.

Verschlüsselte Verbindungen erkennen

Ob eine HTTPS-Verbindung besteht und ob die aufgerufene Seite auch die ist, die sie zu sein scheint, zeigen Ihnen aktuelle Browser in der Regel durch ein Schloss-Symbol in der Adresszeile an.

Bei entsprechendem Bedarf können sich große Betreiber von Webseiten zusätzlichen Sicherheitsüberprüfungen durch eine Zertifizierungsstelle unterziehen (Näheres siehe unten). Diese erweiterten Überprüfungen sollen ein höheres Maß an Vertrauenswürdigkeit sicherstellen und spiegeln sich in sogenannten Extended-Validation-Zertifikatenwider.

Webseiten mit Extended-Validation-Zertifikaten werden in vielen Browsern noch einmal gesondert gekennzeichnet:

- *Firefox* (Abbildung 3.1 und 3.2)

Abb. 3.1 Firefox, verschlüsselte Verbindung

Abb. 3.2 Firefox, verschlüsselte Verbindung, erweitert

- *Chrome* (Abbildung 3.3 und 3.4)

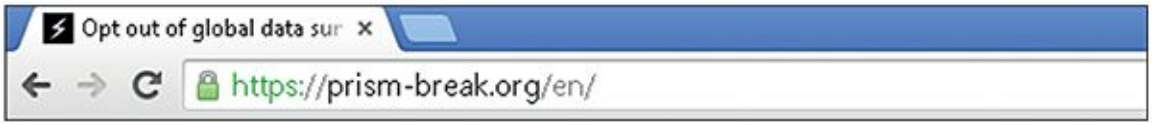


Abb. 3.3 Chrome, verschlüsselte Verbindung

Abb. 3.4 Chrome, verschlüsselte Verbindung, erweitert

- *Opera* (Abbildung 3.5 und 3.6)

Abb. 3.5 Opera, verschlüsselte Verbindung

Abb. 3.6 Opera, verschlüsselte Verbindung, erweitert

- *Internet Explorer 11* (Abbildung 3.7 und 3.8)

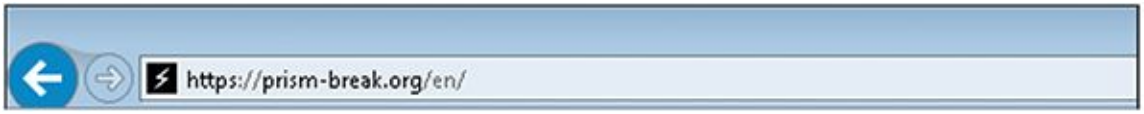


Abb. 3.7 Internet Explorer 11, verschlüsselte Verbindung

Abb. 3.8 Internet Explorer 11, verschlüsselte Verbindung, erweitert

HTTPS Everywhere

Die *Electronic Frontier Foundation*[3] (EFF) ist eine amerikanische Nichtregierungsorganisation, die sich für die Wahrung der Bürgerrechte im digitalen Zeitalter einsetzt. Aus ihrem Umfeld stammt die Browser-Erweiterung *HTTPS Everywhere*. Dieser kleine Helfer erkennt, ob Sie gerade versuchen, eine Webseite über eine unverschlüsselte HTTP-Verbindung abzurufen, und

testet, ob diese nicht stattdessen auch über HTTPS zu erreichen ist. Ist das der Fall, werden Sie automatisch auf die verschlüsselte Verbindung umgeleitet, ohne dass Sie etwas dafür tun müssen. Sie können außerdem selbst weitere Webseiten definieren (siehe Abbildung 3.9), die das Add-on noch nicht kennt, auf denen Sie auf HTTPS umgeleitet werden möchten, und auch Ausnahmen, bei denen Sie eine unverschlüsselte Verbindung wünschen. Das Add-on ist Open Source und bisher für Chrome, Firefox (einschließlich Firefox for Android) und Opera verfügbar.

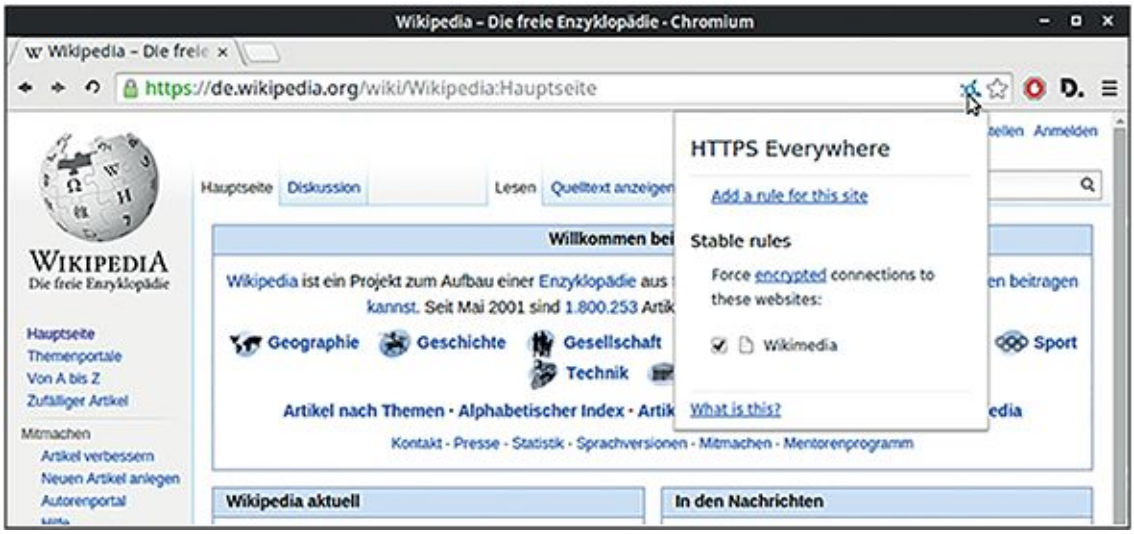


Abb. 3.9 HTTPS Everywhere

Weitere Informationen und Download: https://prism-break.org/de/projects/https-everywhere https://www.eff.org/https-everywhere

3.2 Ihr Browser und Sie

Während sich das World Wide Web im Laufe der 90er-Jahre und darüber hinaus zu einem universellen Informationsdienst entwickelte, wurden auch die Aufgaben eines Browsers immer vielfältiger und komplexer. Auf den hohen Innovationsdruck reagierten die Hersteller teilweise sehr unterschiedlich. Einige Browser verschwanden auch ganz von der Bildfläche. Moderne Browser sind mittlerweile zu Programmen herangereift, die (mithilfe von Zusatzprogrammen, sogenannten Plug-ins) fast jeden beliebigen Typ von Daten darstellen oder abspielen können. Die heute am häufigsten verwendeten Browser für stationäre Geräte (also Desktop-PCs und Notebooks) sind Google Chrome, Mozilla Firefox, Microsoft Internet Explorer, Apple Safari und

Opera. Je nachdem, welche Statistik man sich anschaut, liegt hier mal der eine und mal der andere vorn (wobei Opera am wenigsten verbreitet ist). Darüber hinaus gibt es noch viele »kleine« Browser – wir wollen uns in diesem Buch aber auf diese fünf beschränken.

Jeder der genannten Browser kann kostenlos heruntergeladen und installiert werden. Die Mehrzahl davon wird Ihnen von Unternehmen zur Verfügung gestellt, die Spezialisten bezahlen, um Fehler an der jeweiligen Software zu beheben und diese weiterzuentwickeln. Open Source, also mit einem für jeden Menschen kostenlos einsehbaren Quellcode, sind nur Chromium und Mozilla Firefox. Auf Chromium basieren Google Chrome und Opera.

Wo aber kommt das Geld her, von dem die Entwickler der kostenlosen Browser bezahlt werden? *Firefox* ist ein Sonderfall, da er von der gemeinnützigen Mozilla Foundation entwickelt wird, bei der unter anderem freiwillige Programmierer mitarbeiten und die von Spenden und Stiftungsvermögen lebt. Diese Spenden kommen von Privatleuten und Firmen, die Open-Source-Software unterstützen und langfristig selbst davon profitieren wollen. Allerdings stammte ein Großteil der Einnahmen der Mozilla Foundation von Google, deren Suchmaschine vertraglich als Standardsuche von Firefox festgelegt wurde. Es werden Zahlen von bis zu 90 Prozent der Einnahmen genannt; laut einem Beitrag von Stefan Mey auf Heise Online beispielsweise 280 Millionen Dollar im Jahr 2012. Seit 2014 (dem Jahr, in dem der Vertrag mit Google auslief) gibt es einen Fünfjahresvertrag mit Yahoo. Die Bedingungen dieses Vertrages werden allerdings erst im November 2016 veröffentlicht.

Microsoft und Apple (die Entwickler von Internet Explorer beziehungsweise Safari) liefern eigene Betriebssysteme und Hardware, mit der sie (in den unterschiedlichsten Kombinationen) Geld verdienen. Die Entwicklung der Browser wird somit durch die übrigen Geschäftsfelder der Konzerne querfinanziert. Sie sollen die bestehende Produktlandschaft ergänzen und die Wahrscheinlichkeit erhöhen, dass Sie den Produkten dieser Hersteller treu bleiben.

Googles Chrome und der Opera-Browser basieren, wie gesagt, auf dem quelloffenen Chromium. Google finanziert die Weiterentwicklung seiner Software, um die Google-Suche und andere Produkte (beispielsweise Google-Drive) noch stärker mit dem Browser zu verzahnen und damit noch näher an den Nutzer, also Sie, heranzutragen. Wenn Sie zum Beispiel Dienste von Google nutzen, insbesondere, wenn Sie dabei einen persönlichen Account verwenden, mit dem Sie auch E-Mails empfangen oder Termine verwalten, gewinnt Google Daten, mit denen Ihnen noch präziser auf Ihre Bedürfnisse zugeschnittene Werbung angezeigt werden kann. Ähnlich

geht auch Opera Software vor, das Unternehmen hinter dem gleichnamigen Webbrowser: Opera Software besitzt wie Google ein Werbenetzwerk für mobile Endgeräte namens »Opera Mediaworks«. Dieses verspricht, Werbung kontextbasiert[4], aufgrund demografischer Einordnung[5] oder auf Basis des Nutzerverhaltens[6] einspielen zu können. Woher die Daten stammen, auf deren Basis dieser Dienst angeboten wird, können Sie sich sicher denken. Anpassungen und Fehlerbehebungen beider Unternehmen fließen übrigens wieder zurück in den Quellcode von Chromium und helfen dabei, die Software robuster zu machen und weiterzuentwickeln. Egal, ob Sie nun ein Freund von Google oder Opera und den damit verbundenen Werbe- und Trackingpraktiken sind, eins muss man ihnen lassen: Auch sie helfen dabei, offene (Open Source) Software und Standards zu entwickeln und weiter zu verbessern, wenngleich sie das nicht ohne Eigeninteresse tun.

Weil Browser mittlerweile so universelle Werkzeuge sind, haben sie auch einen erheblichen Einblick in das, was Sie den ganzen Tag über im Web treiben. Aus diesem Grund ist es für werbetreibende Unternehmen generell interessant, einen wie auch immer gearteten Browser anzubieten, um mehr über Sie zu erfahren und Ihnen auf dieser Basis passende Werbung anzeigen zu können. Deshalb sollten Sie sich gut überlegen, welchen Browser Sie auf welchem Ihrer Geräte installieren und wie Sie ihn einsetzen möchten. Fragen Sie sich, wer die Arbeit bezahlt, die in einer solchen Software oder einem Onlinedienst steckt, welche Interessen dahinter stehen und welche Gegenleistung zum Beispiel in Form von Informationen über Ihr Nutzerverhalten und personalisierte Werbung erwartet wird. Fragen Sie sich generell bei allen kostenlosen Diensten im Internet, was der Preis für den Dienst ist und ob Sie bereit sind, diesen zu bezahlen.

3.2.1. Welcher Browser für welchen Nutzer?

Die oben genannten fünf weit verbreiteten Browser können Sie auf Ihrem Laptop- oder Desktop-Computer in den meisten Fällen unabhängig vom verwendeten Betriebssystem installieren. Ausnahmen sind allerdings Apples Safari und der Internet Explorer von Microsoft. Trotz früherer »Ausflüge« auf das Betriebssystem des jeweiligen Konkurrenten sind die aktuellen Versionen nur noch für das eigene Betriebssystem und dessen jeweilige Smartphone-Variante OS X/iOS bzw. Windows/Windows Phone erhältlich. Tabelle 3.1 zeigt eine Übersicht der häufigsten Browser und ihrer Verfügbarkeit auf den jeweiligen Betriebssystemen.

Tabelle 3.1

Windows	OS X	Linux	iOS	Android	Windows Phone
Internet Explorer	[[richtig]]	[[falsch]]	[[falsch]]	[[falsch]]	[[falsch]]	[[richtig]]
Safari	[[falsch]]	[[richtig]]	[[falsch]]	[[richtig]]	[[falsch]]	[[falsch]]
Firefox	[[richtig]]	[[richtig]]	[[richtig]]	[[falsch]]	[[richtig]]	[[falsch]]
Chrome	[[richtig]]	[[richtig]]	[[richtig]]	[[richtig]]	[[richtig]]	[[falsch]]
Opera	[[richtig]]	[[richtig]]	[[richtig]]	[[richtig]]	[[richtig]]	[[richtig]]

Unter Linux existieren noch weitere quelloffene Browser wie beispielsweise Konqueror, Iceweasel, Web (Epiphany) oder Midori. Letzterer ist übrigens auch unter Windows nutzbar.

Chromium – das quelloffene System, das Google Chrome und Opera zugrunde liegt – kann übrigens auch als eigenständiger Browser installiert werden. Die Installation ist abhängig vom Betriebssystem leider nicht ganz trivial und dementsprechend mit Vorsicht zu genießen.

Wie Sie Tabelle 3.1 entnehmen können, gibt es für Smartphones weniger Auswahl: Die drei gängigsten mobilen Betriebssysteme Android, iOS und Windows/Windows Phone sind von den Herstellern in der Regel so abgeriegelt, dass sich auf dem Gerät keine Software, die nicht aus dem App-Store des jeweiligen Herstellers kommt, ohne größeren Aufwand installieren lässt. Das heißt, auch die Browser, die nicht aus dem jeweiligen Haus stammen, müssen über diesen App-Store installiert werden. Dabei geht Apple bisher am restriktivsten vor, weshalb der Firefox-Browser bis zur Veröffentlichung dieses Buches noch nicht für iOS erschienen ist. Opera ist derzeit der einzige Browser, der für alle drei mobilen Betriebssysteme zur Verfügung steht.

Viele mobile Varianten gängiger Browser unterscheiden sich je nach Endgerät stark von ihren Desktop-Pendants. Opera Software bietet hier alleine vier unterschiedliche Versionen für die verschiedensten Geräte und Betriebssysteme an. Einige dieser Varianten sollen die Datenmenge einer aufgerufenen Website durch die Nutzung eines von Opera bereitgestellten Internetdienstes verkleinern und dadurch Bandbreite einsparen, wodurch Webseiten auf den mobilen Geräten schneller geladen und das gebuchte Datenvolumen geschont werden soll[7]. Zusätzlich ermöglicht es Opera, die abgerufenen Webseiten inhaltlich vollständig zu analysieren und die so gewonnenen Informationen für die Verbesserung ihres bereits erwähnten Werbenetzwerks zu verwenden.

Falls Sie auf Ihrem Android-, iOS- oder Windows-Smartphone (oder -Tablet) einen alternativen Browser suchen, sollten Sie übrigens doppelt vorsichtig sein. Bei der Recherche zu diesem Buch sind wir unter anderem im Windows Phone Store mehrfach auf Programme gestoßen, die wie eine Version von Firefox oder Chrome aussehen sollten, aber keine waren. Achten Sie besonders auf Ihrem mobilen Gerät darauf, dass Sie nur Software installieren, von der Sie zweifelsfrei wissen, woher sie stammt und was sie bezweckt. Ein hilfreicher Indikator für die Vertrauenswürdigkeit einer App aus einem der App-Stores sind die Berechtigungen, die diese bei der Installation anfordert. Warum sollte ein Webbrowser beispielsweise auf Ihr Adressbuch oder Ihre SMS zugreifen wollen? Im Zweifel heißt es an dieser Stelle – Finger weg!

Wie wählen Sie also den richtigen Browser für Ihre Bedürfnisse aus?

Nahezu alle modernen Browser sind heute als Plattformen konzipiert – das heißt, der Funktionsumfang lässt sich fast beliebig durch sogenannte *Add-ons* erweitern. Auf diese Add-Ons gehen wir später noch einmal ein. Zudem ist der Browser-Markt einem stetigen Wandel unterworfen und ordnet sich ständig neu – kurz nach Erscheinen dieses Buches gibt es vielleicht schon einen neuen, der um Nutzer wirbt. Im Folgenden wollen wir einige allgemeine Kriterien besprechen, anhand derer Sie beurteilen können, welcher Browser für Ihre Bedürfnisse am besten geeignet ist.

3.2.1.1 Geschwindigkeit

Auch wenn die Geschwindigkeit eines Browsers für das Thema dieses Buches – nämlich Ihre Sicherheit – eigentlich keine Rolle spielt, so ist sie doch für die meisten Anwender eines der wichtigsten Kriterien bei der Auswahl eines Browsers. Ist die gefühlte Zeitspanne vom Aufruf einer Webseite bis zur Anzeige zu lang, wird man zu Recht ungeduldig. Die technischen Gründe, warum unterschiedliche Browser zur Darstellung desselben Inhalts verschieden lange benötigen, sind vielfältig. Wenn Sie Schwankungen außer Acht lassen, auf die die jeweilige Software keinen Einfluss hat, zum Beispiel die zur Verfügung stehende Internetbandbreite oder die Verbindungsqualität Ihres WLANs, dann bleibt davon aber nur noch eine überschaubare Anzahl übrig.

Die sogenannte *Browser- oder HTML-Engine* (von englisch »engine« = Maschine oder Motor) ist der Teil Ihres Browsers, der den HTML-Code einer Webseite interpretiert und daraus ein für Sie sichtbares Bild erzeugt. Wie lange eine Engine für das Einlesen und Verarbeiten besagter

Anweisungen benötigt, ist ein entscheidender Faktor dafür, wie schnell sich Ihr Browser anfühlt. Webkit (Apple), Gecko (Mozilla), Trident (Microsoft), Blink (Google) oder Presto (Opera) sind einige der am weitesten verbreiteten Engines. Vom zugrunde liegenden Quellcode her sind sie sogar teilweise miteinander verwandt, weil sie aus den gleichen Vorläufern entstanden sind. Grundsätzlich unterscheiden sich moderne Browser-Engines heute kaum noch durch ihre Leistungsfähigkeit, wohl aber über die damit verbundene Beanspruchung der Ressourcen Ihres Computers oder Smartphones. Welches Programm nun für Sie persönlich das optimale Verhältnis von Geschwindigkeit zu Ressourcenhunger bietet, können Sie am besten durch Ausprobieren herausfinden.

Ein weiterer Faktor, der noch größeren Einfluss auf die Ladegeschwindigkeit von Webseiten haben kann, ist die Fähigkeit Ihres Browsers, *JavaScript* zügig auszuführen. JavaScript ist eine Programmiersprache, und kleine JavaScript-Programme werden häufig in Webseiten eingebettet, um zusätzliche Funktionen anzubieten. Wenn ein Formular auf einer Webseite auf Ihre Eingaben reagiert, bevor Sie das Formular abgeschickt haben – wenn es Ihnen zum Beispiel anzeigt, wie stark ein Passwort ist, das Sie eingegeben haben – dann wird das in der Regel mithilfe von JavaScript realisiert. Der Einsatz von JavaScript kann auch unerwünschte Nebeneffekte haben, wie wir später noch sehen werden. Die Interpretation und das Ausführen von JavaScript-Anweisungen übernimmt die sogenannte *JavaScript-Engine* Ihres Browsers. Auch hier existiert fast für jeden Browser eine gesonderte Lösung. Allerdings haben sich auch hier wie bei den HTML-Engines die modernen Webbrowser einander stark angenähert.

Auch die Hersteller haben natürlich erkannt, wie wichtig den Nutzern Geschwindigkeit ist. Webseiten werden allerdings auch immer anspruchsvoller und damit ressourcenhungriger. Daher lassen sich die Hersteller von Browsern immer neue Kniffe einfallen, um ihre Software zu beschleunigen. Google hat beispielsweise Chrome und seinen Open-Source-Vetter Chromium so erweitert, dass jeder Tab in einen eigenen abgeschlossenen Programmteil ausgelagert wird. Dieser Programmteil, auch Prozess oder Thread genannt, wird von Ihrem Betriebssystem wie ein eigenständiges Programm behandelt, dem entsprechende Ressourcen zugewiesen werden. Auf modernen Computersystemen und Smartphones, die heute in der Regel mehr als nur einen Prozessorkern besitzen, können die einzelnen Prozesse auf verschiedene Kerne verteilt und so parallel verarbeitet werden, was das mobile Surfen merkbar schneller werden lässt. Auf der anderen Seite hat dies auch einen Vorteil für die

Sicherheit beim mobilen Surfen: Einer Website, auf der schädlicher Programmcode ausgeführt wird, wird es dadurch schwerer gemacht, auf die übrigen Teile des Browsers und eventuell andere geöffnete Webseiten zuzugreifen. Der Nachteil der Strategie ist jedoch, dass Ressourcen, die zur Anzeige einer Website benötigt werden, nicht zwischen den verschiedenen geöffneten Seiten geteilt werden können und so mehrfach aktiv sein müssen und dann mehr Speicher benötigen. Derzeit wird die Strategie, in der jeder Tab ein eigener Prozess ist, in Google Chrome sehr erfolgreich einsetzt. Die Mozilla Foundation hat ebenfalls angekündigt, ihren Webbrowser Firefox in diese Richtung weiterzuentwickeln.

3.2.1.2 Komfort

Ganz wichtig ist für Sie und uns als Nutzer eines Browsers auch der Komfort der Benutzeroberfläche. Wie sind Bedienelemente eingeordnet? Sind häufig genutzte Funktionen schnell oder eher kompliziert zu erreichen? Wie aufgeräumt und strukturiert wirkt die Oberfläche auf Sie? All das sind Fragen, die Sie sich zumindest unbewusst stellen. Oft folgt daraus, dass man ein Programm lieber nutzt, das weniger Funktionen hat als ein anderes, wenn es ein übersichtlicheres »Gesicht« hat. Dabei spielt es oft auch eine Rolle, wie eng die Software mit Ihrem Betriebssystem verzahnt ist. Wirkt alles wie aus einem Guss und sind Ihnen die Bedienkonzepte aus Ihrem Alltag vertraut, das heißt, finden Sie intuitiv und schnell die Einstellungen des Browsers, kennen Sie die Symbole der Menüleiste schon von anderen Programmen? Dann fällt Ihnen die Benutzung sicher spürbar leichter. Diese Art der Benutzerfreundlichkeit gilt als eine Spezialität von Apple, hat aber inzwischen auch die anderen Plattformen erreicht.

3.2.1.3 Sicherheit

Wie Sie wissen, besitzt Ihr Browser die maximale Übersicht über Ihre Aktivitäten im WWW. Als Hauptschnittstelle zwischen Ihnen und dem Web hat die Software zudem auch den größtmöglichen Einfluss darauf, welche Daten Sie ins Netz übertragen und welche Informationen Ihnen angezeigt werden. Kontrolliert jemand anderes außer Ihnen selbst Ihren Browser, ist dieser Jemand auch in der Lage, tief in Ihre Onlineaktivitäten einzugreifen und Ihnen möglicherweise zu schaden. Genau das macht Browser zu einem der beliebtesten Angriffsziele im Internet.

Ein Angreifer, der keinen physikalischen Zugang zu Ihrem System hat, muss sich (wenn er es nicht mit Social Engineering versucht, siehe Kapitel 2) vorhandener Sicherheitslücken bedienen. Sicherheitslücken basieren in den meisten Fällen auf Softwarefehlern. Jede Software, egal ob nun das Navigationsprogramm einer Ariane-5-Rakete, ein Indie-Game auf Ihrem Tablet oder eben Ihr Webbrowser, beinhaltet solche Fehler, die auch als Bugs (siehe Kasten) bezeichnet werden.

Hinweis

Bugs

Die Verwendung des Wortes »Bug« in einem technischen Kontext findet sich schon im 19. Jahrhundert. Schon damals bezeichneten die Menschen kleinere mechanische oder elektrische Fehlfunktionen an Maschinen so. Der Begriff wurde sogar vom Erfinder Thomas Edison 1878 in einem Brief an seinen Freund Tivadar Puskás verwendet:

»Der erste Schritt [bei all meinen Erfindungen] ist eine Eingebung, sie kommt wie ein Ausbruch, dann tauchen Schwierigkeiten auf – dieses Ding funktioniert einfach nicht mehr und [es geschieht] dann, dass >Bugs< – wie solche kleinen Fehler und Schwierigkeiten genannt werden – sich zeigen.«

Wahrscheinlich war es die Informatikpionierin Grace Hopper, die dann im 20. Jahrhundert das Wort Bug mit Fehlern in der damals noch jungen Computertechnik verknüpfte. Sie erzählte gerne eine Anekdote darüber, wie eine Motte am 9. September 1947 in einem Relais des Computers Mark II Aiken Relay Calculator zu einer Fehlfunktion führte. Die Techniker, die das Problem damals entdeckten und das Insekt aus dem Relais entfernten, hielten den Vorfall im Logbuch mit dem folgenden Kommentar fest:

»First actual case of bug being found.«(Der erste Fall eines tatsächlich gefundenen »Bugs«.)

Egal, wie aufwendig die Tests sind, die man an beliebiger Soft- oder Hardware durchführt – es bleiben stets Fehler übrig, die nicht von den Tests erfasst werden. Oft genug führen Bugs dazu, dass Verschlüsselung geschwächt oder Sicherheitsmechanismen ausgehebelt werden können. Im schlimmsten Fall ist ein Angreifer sogar mittels eines sogenannten *Buffer Overflows* (siehe Kasten) oder anderer Tricks in der Lage, eigene Anweisungen in die Software einzuschleusen. Das Ausnutzen einer solchen Sicherheitslücke wird auch als Exploit (englisch für »Nutzung«, »ausnutzen«) bezeichnet.

Achten Sie daher bei der Wahl Ihres Webbrowsers immer darauf, dass dieser regelmäßige Updates erhält. Plötzlich bekannt werdende Sicherheitslücken sollten vom Hersteller zeitnah durch einen entsprechenden *Patch* (einen »Flicken«, der das Programm repariert) geschlossen werden. Erfahrungsgemäß reagieren die entsprechenden Entwicklergemeinschaften im Open-Source-Bereich oft schneller auf Sicherheitsprobleme als die Teams kommerzieller Unternehmen wie Apple oder Microsoft. Außerdem fallen aufgrund der Vielzahl der freiwilligen Helfer Softwarefehler in Open-Source-Projekten tendenziell schneller auf. Wenn Sie Ihren Browser also stets aktuell halten, verringern Sie das Risiko, Opfer eines Angriffs auf Ihre Privatsphäre oder gar auf Ihr Eigentum zu werden. Zudem können Webseiten, die auf die neuere Webtechnologien setzen, nur mit den entsprechenden Programm-Updates weitgehend fehlerfrei dargestellt werden.

Hinweis
Buffer Overflows (Pufferüberläufe)

Daten eines Computers werden auf der Festplatte oder auf internen oder externen Laufwerken (zum Beispiel CD-Laufwerken oder USB-Sticks) gespeichert. Darüber hinaus gibt es aber noch den Arbeitsspeicher (Random Access Memory, RAM); dort werden Daten vorgehalten, die für den Prozessor eines Computersystems für einen schnellen Zugriff verfügbar sein sollen.

Der Platz in einem derartigen Speicher ist nicht fest aufgeteilt, sondern muss sorgfältig verwaltet werden. Bildlich gesprochen ist der Arbeitsspeicher wie ein langes Regal, das zunächst leer ist, aber durch eine beliebige Anzahl von Aktenordnern unterschiedlichster Größe gefüllt werden kann. Damit Sie Informationen zu einem bestimmten Thema wiederfinden, beschriften Sie Ihre Aktenordner sorgfältig. So ähnlich macht das auch Ihr Computer – er klebt allerdings keine Etiketten auf die Rückseite der Ordner, sondern vergibt für jede Dateneinheit eine Adresse, mit deren Hilfe sich die Daten wiederfinden lassen. Diese Adresse beschreibt sozusagen den Abstand des Ordners vom Rand Ihres Regals: Der Ordner der Steuererklärung liegt 142 cm, der nächste Ordner mit den Versicherungsunterlagen 150 cm vom linken Regalrand entfernt. In einem Computer geschieht diese Adressvergabe laufend, in rasender Geschwindigkeit und im Falle mehrerer Prozessoren (CPUs) auch nahezu gleichzeitig an verschiedenen Stellen des Speichers. Das Ganze kann also ziemlich kompliziert und fehleranfällig werden. Ändert sich nämlich die Breite des Ordners mit der Steuererklärung, wenn er zum Beispiel am Ende des Jahres 1 cm dicker wird, würde sich die Adresse des nachfolgenden Ordners mit den Versicherungsunterlagen auf 151 cm ändern.

Computerprogramme müssen daher dem System mitteilen, wie viel Speicher sie für welche Informationen reservieren möchten. Dieser Vorgang wird auch als Allokation bezeichnet. Wird mehr Speicher benötigt als ursprünglich gedacht, reagieren die meisten Programme darauf, indem sie versuchen, mehr Speicher vom System zu erhalten, oder indem sie eine Fehlermeldung ausgeben. Manchmal kommt es jedoch durch Softwarefehler oder andere Umstände dazu, dass ein Programm die zu speichernde Datenmenge gar nicht oder nur unzureichend prüft. In diesem Falle kann es also geschehen, dass die Größe einer Zeichenkette ursprünglich mit 100 Zeichen angegeben war, aber tatsächlich 1000 Zeichen gespeichert werden sollen. Dies kann zur Folge haben, dass 900 Zeichen in einen Teil des Speichers geschrieben werden, der gar nicht mehr zum eigentlichen Programm gehört. Im Regal-Beispiel wäre das in etwa so, als würden Sie ungewollt Ihre Steuererklärungen mit den Bildern des letzten Familienfestes überkleben, weil das Fotoalbum links vom Ordner »Steuern« stand und zu klein für die vielen Fotos war. Dieses Phänomen wird auch als Buffer Overflow oder Pufferüberlauf bezeichnet. In der Regel führen Buffer Overflows zum Programm- oder sogar Systemabsturz. Sie können aber unter Umständen auch von Angreifern genutzt werden, um schädliche Programme in den Arbeitsspeicher zu schieben und auszuführen. Im Regal-Beispiel ist das so, als würde ein Unbekannter das besagte Fotoalbum mit Katzenbildchen füllen und sich damit den Zugriff auf Ihren Steuer-Ordner erschleichen, um Ihnen eine falsche Steuererklärung unterzuschieben, die Sie dann nichts ahnend in die Post geben.

Die Desktop-Varianten von Chrome, Opera, Firefox und dem Internet Explorer verfügen alle über eine automatische Update-Funktion. Für Apples Safari sowie die Linux-Versionen der genannten Browser, falls diese existieren, ist diese Funktion nicht direkt in die Software integriert, sondern entsprechende Aktualisierungen werden über den zentralen Update-Mechanismus des Betriebssystems abgewickelt. Dieser lässt sich aber sowohl unter Linux als auch unter OS X so konfigurieren, dass alle sicherheitsrelevanten Aktualisierungen automatisch im Hintergrund ablaufen. Auch die gängigen Mobilbetriebssysteme erlauben über ihre Einstellungen automatische Updates. Sie können hierbei angeben, dass automatische Updates nur bei vorhandener WLAN-Verbindung heruntergeladen werden sollen und so das gebuchte mobile Datenvolumen schonen.

3.2.1.4 Integrierte Suche und Auswahl einer Suchmaschine

Integrierte Suche bedeutet, dass Sie Suchbegriffe für eine Suchmaschine direkt in der Adresszeile Ihres Browser eingeben können. Das heißt, Sie müssen nicht erst eine Suchmaschine, beispielsweise über http://www.google.de oder http://www.ecosia.de, aufrufen, um dann Ihren Suchbegriff, zum Beispiel »asymmetrische Verschlüsselung«, auf der Webseite der Suchmaschine einzugeben. Stattdessen erkennt der Browser die Eingabe als Suchbegriff und gibt sie an die hinterlegte Standardsuchmaschine weiter. Wichtig ist, dass Sie die Standardsuchmaschine und deren Verhalten selbst festlegen können. Zudem sollten Sie auch einstellen können, ob eine Suche auch bei einem Navigationsfehler (wenn Sie sich zum Beispiel bei der Eingabe der URL vertippt haben) ausgelöst werden soll oder nicht. Viele Browser bieten auch die Möglichkeit, mehrere Suchmaschinen gleichzeitig zu integrieren und diese dann kontextbezogen zu nutzen: Indem Sie dem Suchbegriff ein »g« voranstellen, wird beispielsweise »asymmetrische Verschlüsselung« in der Google-Suchmaschine gesucht, durch ein »i« in der Bildsuche und so weiter.

Ein Problem der Standardsuchmaschinen ist die sogenannte *Filterbubble*: Je länger Sie eine Suchmaschine verwenden, desto mehr Daten sind über Sie gespeichert. Dies geschieht zum Beispiel im Browserverlauf, den Sie vielleicht lange nicht gelöscht haben, in Cookies oder dadurch, dass Sie mit einem persönlichen Account angemeldet sind und dadurch eine Suche Ihrem Profil zugeordnet werden kann. Aber auch, wenn Sie dies alles nicht tun (und wir zeigen Ihnen weiter unten, wie Sie Cookies und Verläufe regelmäßig löschen), sind Sie an Ihren Browser-Einstellungen und -Erweiterungen durch sogenanntes *Browser-Fingerprinting* (siehe unten) zu identifizieren. Der Begriff *Filterbubble* besagt nun, dass Ihnen im Laufe der Zeit vermehrt Suchergebnisse angezeigt werden, die Ihren Bedürfnissen, Interessen oder früheren Suchen entsprechen. Das mag auf der einen Seite komfortabel sein, wenn Sie zum Beispiel Geschäfte in Ihrer Umgebung angezeigt bekommen oder als Wissenschaftler viele wissenschaftliche Suchergebnisse und weniger populärwissenschaftliche Ergebnisse – es kann aber Ihre Sicht auf die Dinge einschränken und Sie für bestimmte Webseiten oder Inhalte regelrecht erblinden lassen.

Überlegen Sie daher doch, ob Sie Google oder Bing als voreingestellte Suchmaschine nicht durch eine alternative Suchmaschine ersetzen wollen. Einige der zahlreichen Alternativen, die meist auch als Add-on und damit als Standardsuchmaschine für den Browser erhältlich sind:

- *DuckDuckGo*: Diese amerikanische Suchmaschine verzichtet nach eigenen Angaben darauf, Ihre Daten zu sammeln. Nachteil ist, dass viele englischsprachige Ergebnisse angezeigt werden.
- *Startpage* reicht Ihre Suchanfrage anonymisiert an Google weiter und ist als App für iOS und Android verfügbar. Das gleiche (niederländische) Unternehmen, das Startpage betreibt, bietet mit *Ixquick* auch eine Metasuchmaschine an.
- *Ecosia* ist eine Suchmaschine aus Berlin, die mindestens 80 Prozent ihrer Einnahmen für das Pflanzen von Bäumen ausgibt und ebenfalls als Add-on für Firefox erhältlich ist.
- Auch die Suchmaschine *benefind* spendet einen Teil ihrer Einnahmen (Werbeeinnahmen aus Suchanfragen und Provisionen aus Onlineshopping) an gemeinnützige Organisationen.
- *Wegtam* ist eine deutsche Metasuchmaschine, die neben Google und Yahoo auch zahlreiche spezielle Datenbanken durchsucht (beispielsweise für Rezepte, wissenschaftliche Publikationen oder Blogs) und ebenfalls angibt, keine Nutzerdaten zu speichern.
- *YaCy* ist Open Source und läuft nicht auf einem zentralen Server wie andere Suchmaschinen, sondern auf den Rechnern der Benutzer – ein sogenanntes Peer-to-Peer-Projekt. Der Nutzer muss hierzu ein kleines Programm auf seinem Computer installieren und kann dann nicht nur Suchanfragen starten, sondern auch selbst das Web crawlen (also Seiten indexieren). YaCy gibt es für Windows, Linux und MacOS, und es gibt eine (eingeschränkt funktionsfähige) Bildersuche. YaCy wird vom Institute of Technology aus Karlsrufe und SUMA e.V., einem Verein für freien Wissenszugang, unterstützt.

3.2.1.5 Synchronisation von Einstellungen über mehrere Geräte hinweg

Wenn Sie viele unterschiedliche Geräte verwenden, kann es hilfreich sein, Einstellungen des Browsers über alle Geräte hinweg synchronisieren zu können. Hierzu bieten die meisten Hersteller entsprechende Onlinedienste an – allen voran Google Chrome, mittlerweile aber auch Mozilla Firefox und andere. Diese Funktion stellt natürlich eine potenzielle Gefahr für Ihre

Privatsphäre dar, weil die Daten nicht mehr nur lokal gespeichert werden – daher sollten Sie den persönlichen Nutzen und eventuelle Risiken gründlich gegeneinander abwägen.

3.2.1.6 Lesezeichen

Das Anlegen eines *Lesezeichens* (auch als *Bookmark* oder *Favorit* bezeichnet), erzeugt im Lesezeichen-Untermenü Ihres Browsers einen Link auf die Webseite, die Sie markiert haben. Im Dschungel des Internets, in dem man oft nur durch Zufall über interessante Seiten stolpert, sind Lesezeichen ein Hilfsmittel, das kaum zu ersetzen ist. Wie die im vorigen Punkt besprochenen Einstellungen können auch Lesezeichen über mehrere Geräte hinweg synchronisiert werden – auch hier ist zu beachten, dass Ihre Informationen damit in die Cloud des Anbieters wandern und dort möglicherweise schlecht geschützt werden. Sie können sich vorstellen, dass Ihre Lesezeichen-Sammlung überaus viel über Sie aussagt und damit zu den sensiblen persönlichen Daten gezählt und entsprechend geschützt werden sollte. Im Zweifelsfall sollte man also auf den Bequemlichkeitsgewinn durch Synchronisation von Lesezeichen eher verzichten.

3.2.1.7 Privates Fenster/Inkognito-Modus

Ein guter Browser sollte es Ihnen ermöglichen, ein sogenanntes *privates Fenster* zu öffnen, das isoliert zu anderen Fenstern ausgeführt wird. Ein solches Fenster »vergisst« alle in seinem Kontext gespeicherten Informationen, wenn es geschlossen wird: Es werden also beispielsweise keine Cookies gespeichert oder Seiten in die Chronik übernommen.

3.2.1.8 Passwort-Manager

In viele moderne Browser ist schon ein *Passwort-Manager* integriert. Wenn Sie einen solchen nutzen möchten (mehr dazu in Kapitel 6), sollte er Log-in-Informationen zu verschiedenen Webseiten sicher verschlüsselt ablegen und gegebenenfalls automatisiert in die Log-in-Masken der jeweiligen Webseiten einfügen.

3.2.1.9 Verschiedene Browser-Profile (Identitäten)

Viele Browser bieten Ihnen die Möglichkeit, verschiedene sogenannte *Profile* oder Identitäten anzulegen, in denen dann Einstellungen und Browsing-Daten gekapselt vorgehalten werden.

Sie können für sich selbst eins oder mehrere Profile anlegen, in denen Sie zum Beispiel die Lebensdauer von Cookies, aktivierte Add-ons und Einstellungen für die Standardsuchmaschine festlegen können. Zumindest unter Mozilla Firefox können Sie sogar mehrere Profile in mehreren Browser-Fenstern gleichzeitig aktivieren. So können Sie beispielsweise verhindern, dass ein Fenster auf Cookies eines anderen Fensters zugreift, was im Umgang mit Facebook-Cookies sehr hilfreich sein kann – wenn Sie eine separate Facebook-Identität anlegen, die Sie für Facebook (und nur für Facebook) verwenden, kann das durch den Like-Button veranlasste Tracking keinen Bezug mehr zu Ihrem Namen herstellen. Siehe hierzu auch den Abschnitt »Cookies« weiter hinten in diesem Kapitel.

3.2.1.10 Add-ons

Add-ons sind Unterprogramme, die sich in Ihren Browser integrieren und diesem so neue Funktionen hinzufügen. Sie können dadurch beispielsweise den Komfort oder auch die Sicherheit des mobilen Surfens erhöhen. Add-ons sollten für Ihren Browser in ausreichender Zahl und Qualität zur Verfügung stehen und möglichst einfach zu installieren und zu verwalten sein. Ihre Qualität sollte über ein aussagekräftiges Bewertungssystem zu beurteilen sein. Außerdem sollten Sie überprüfen, ob Ihr Browser von sich aus einen brauchbaren Ad-Blocker zur Blockade unerwünschter Werbung mitbringt oder ob ein entsprechendes Add-on existiert.

Der Begriff »Add-on« wird häufig synonym mit »Plug-in« verwendet. Streng genommen handelt es sich aber um zwei verschiedene Konzepte. *Plug-ins* sind im Gegensatz zu Add-ons weitgehend eigenständige Programme, die lediglich in den Kontext des Browsers integriert werden und mit diesem ebenfalls über spezielle APIs kommunizieren. Plug-ins werden zum Beispiel dazu eingesetzt, Dateiformate zu dekodieren (entschlüsseln), die der HTML-Browser nicht selbst lesen kann. Ein Beispiel hierfür ist der bekannte Flash-Player von Adobe oder andere Plug-ins zum Abspielen von Audio- und Videoformaten. Über den Umgang mit Plug-ins erfahren Sie mehr weiter unten in diesem Kapitel.

3.2.2. Die Chronik – eine Einstellungssache

Die Chronik, auch Browser-Historie oder Verlauf genannt, ist eine Aufstellung darüber, welche Webseiten Sie in welcher Reihenfolge und zu welchen Zeitpunkten abgerufen haben. Falls Sie

eine Seite wieder besuchen wollen, auf der Sie irgendwann schon einmal gewesen sind, können Sie sie so ganz einfach wiederfinden.

Ihr Browser-Verlauf kann Sie, wie Sie vielleicht schon wissen, aber auch in Schwierigkeiten bringen: Wenn Sie sich beispielsweise mit Ihrem Partner einen Computer teilen und dort nach einem Geburtstagsgeschenk gesucht haben, könnte es sein, dass es am Stichtag schon keine Überraschung mehr ist. Zugegebenermaßen ist das kein weltbewegendes Beispiel, allerdings können Sie sich auch leicht ausmalen, dass es weitreichendere Folgen haben kann, wenn jemand anderes (beispielsweise Ihr Arbeitgeber) Ihren Browser-Verlauf inspiziert.

Neben anderen Menschen sind auch Computerprogramme unter bestimmten Voraussetzungen dazu in der Lage, auf Ihre Browser-Historie zuzugreifen. Add-ons für Browser, auf die wir später noch einmal genauer eingehen, können beispielsweise die in Ihrem Verlauf gespeicherten Daten nutzen und für automatische Vervollständigung von Eingaben in Formularen verwenden. Für unseriöse Anbieter von Add-ons bedeutet das, dass diese die komplette Chronik auslesen und gegen Ihren ausdrücklichen Willen beispielsweise für Werbezwecke verwenden können. In der Vergangenheit gab es zudem immer wieder Probleme mit in Webseiten eingebettetem JavaScript, das unter Umgehung verschiedener Sicherheitsmaßnahmen in der Lage war, zumindest Teile der Browser-Historie auszulesen und für unseriöse Zwecke zu verwenden.

Für den Schutz Ihrer Privatsphäre kann es also wichtig sein zu bestimmen, wann der Aufruf einer Seite protokolliert wird und wann nicht.

Um Browser-Hygiene zu betreiben, können Sie im Nachhinein alle oder bestimmte Einträge aus der Chronik entfernen oder Einträge von Vornherein mit einem Verfallsdatum versehen (siehe Tabelle).

Tabelle 3.2Mögliche Chronik-Einstellungen in gebräuchlichen Browsern

Google Chrome	Verlaufsübersicht
Einzelne Elemente entfernen	
Gesamten Verlauf löschen	
Mozilla Firefox	Verlaufsübersicht
Einzelne Elemente entfernen	
Gesamten Verlauf löschen	
Elemente älter als x automatisch löschen	

Microsoft Internet Explorer	Verlaufsübersicht
Einzelne Elemente entfernen	
Gesamten Verlauf löschen	
Elemente älter als x automatisch löschen	
Verlauf nach Beenden des Browsers automatisch leeren	
Apple Safari	Verlaufsübersicht
Einzelne Elemente entfernen	
Gesamten Verlauf löschen	
Elemente älter als x automatisch löschen	
Verlauf nach Beenden des Browsers automatisch leeren	
Opera	Verlaufsübersicht
Einzelne Elemente entfernen	
Gesamten Verlauf löschen	
Elemente älter als x automatisch löschen	
Verlauf beim Beenden des Browsers automatisch löschen	

Tipp: Im Privaten oder Inkognito-Modus (siehe Abschnitt »Inkognito-Modus«) verwirft ein Browser alle innerhalb dieses Fensters entstandenen Chronik- und Cache-Einträge. Wenn Sie also nach einem Überraschungsgeschenk für Ihren Partner suchen, nutzen Sie dazu einfach den Inkognito-Modus.

3.2.3. Der Cache – des Browsers Kurzzeitgedächtnis

Der *Browser-Cache* ist ein Zwischenspeicher, der dazu verwendet wird, sich wiederholende Inhalte auf Ihrem Computer vorzuhalten. Damit wird vermieden, dass sie bei jedem Aufruf einer Webseite erneut über das Internet heruntergeladen werden müssen. Dies spart zum einen Bandbreite und Zeit bei der Anzeige der ursprünglichen Webseite, zum anderen beschleunigt es auch die Anzeige von Unterseiten einer Webseite, da hierfür im Idealfall nur noch die Inhalte vom Webserver heruntergeladen werden müssen, die sich auch wirklich geändert haben. Das Ablegen von Daten im Browser-Cache wird auch als *Caching* bezeichnet. Der Betreiber einer Website kann festlegen, welche Inhalte der Seite wie lange im Cache verbleiben dürfen, bevor sie neu angefordert werden. Bei bestimmten Inhalten ist es sogar

sinnvoll, das Caching komplett zu unterbinden – beispielsweise bei Seiten, die sich bei jedem Abruf ändern.

Daten (also Bilder, mit HTML ausgezeichneter Text, JavaScript und so weiter), die im Cache abgelegt werden, verraten übrigens viel darüber, welche Webseiten Sie regelmäßig besuchen und welche Inhalte Sie dort betrachten. Erlangt eine andere Person Zugriff auf diesen Cache, kann sie weitreichende Rückschlüsse über Ihre Surfgewohnheiten ziehen. Außerdem kann ein sehr aufgeblähter Cache Ihren Browser deutlich verlangsamen.

Aus diesen Gründen möchten Sie vielleicht Einfluss darauf nehmen, wann was wie lange im Cache festgehalten wird. In modernen Browsern können Sie einstellen, wie groß der Cache werden darf und wann Cache-Einträge entfernt werden sollen, um Platz zu sparen und für eine bessere Performance des Browsers zu sorgen. Wie sparsam Sie mit dem Cache umgehen können, ohne dass Sie anfangen, gewisse Bequemlichkeiten zu vermissen (zum Beispiel die automatische Vervollständigung von Formularen auf Seiten, die Sie länger nicht mehr besucht haben), das sollten Sie einfach mal austesten. Die Optionen, um den Cache zu leeren und einzustellen, wie der Cache in Zukunft gefüllt werden soll, finden Sie bei allen gängigen Browsern im Menü »Optionen« beziehungsweise »Einstellungen«, meist in der Nähe der Optionen, mit denen Sie den Verlauf einstellen können.

Hinweis

Browser-Add-ons für Cache und Verlauf

Es gibt mittlerweile viele Browser-Add-ons am Markt, die Ihnen versprechen, sensible Bereiche wie den Browser-Cache oder die Historie aufzuräumen und den Browser damit schneller und sicherer zu machen. Vieles davon ist reines Placebo, weil die Mehrzahl der Browser die in den Erweiterungen angepriesenen Funktionen von vornherein unterstützt. Bei vielen dieser Programme liegt die Vermutung nahe, dass sie zu Werbezwecken oder zum Abschöpfen von Daten eingesetzt werden, ohne einen wirklichen Mehrwert zu bieten. Daher gilt im Zweifel: Finger weg.

3.2.4. Add-ons – die Zubehörpalette

Add-ons greifen auf Schnittstellen (*API, Advanced Programming Interfaces*) zurück, die vom jeweiligen Browser bereitgestellt werden. Ein API ermöglicht es einer Erweiterung, mit dem Browser zu kommunizieren und so zum Beispiel Informationen über die gerade angezeigte

Webseite zu bekommen, eigene Menüpunkte in die Menüstruktur des Browsers zu integrieren, eigene Datenverbindungen aufzubauen und vieles mehr. Solche Erweiterungen bringen die gleichen Sicherheitsrisiken mit sich wie vollwertige, alleinstehende Programme.

Nahezu alle großen Browser-Hersteller bieten mittlerweile Plattformen an, über die sich Erweiterungen mit wenigen Klicks (meist kostenfrei, aber auch kostenpflichtig) herunterladen und installieren lassen. In den letzten Jahren ist hier ein regelrechter Markt entstanden. Browser-Erweiterungen werden nicht länger ausschließlich von Computerenthusiasten veröffentlicht – mittlerweile sind hier auch viele Unternehmen und auch Privatpersonen unterwegs, manche mit recht zwielichtigem Hintergrund.

Da ein Add-on durch die starke Verzahnung mit Ihrem Browser weitreichende Kenntnisse über und immense Zugriffsmöglichkeiten auf Ihre Daten hat, muss man bei der Auswahl und Installation ein bisschen wachsam sein.

Nehmen Sie beispielsweise einmal an, Sie haben eine Browser-Erweiterung installiert, die augenscheinlich das aktuelle Wetter und eine Fünf-Tage-Vorhersage in einem kleinen Bereich neben der Adresszeile anzeigt. Das Add-on macht seinen Job eigentlich ganz gut, die Bildchen für Regenschauer und andere Wetterphänomene sind nett animiert und sehen gut aus. Wenn Sie, wie auch übrigens die Autoren dieses Buches, wenig bis keine Ahnung davon haben, wie so eine Erweiterung programmiert wird, bleibt Ihnen erst einmal nichts anderes übrig, als dem Hersteller des Add-ons dahingehend zu vertrauen, dass die Erweiterung wirklich nur das Wetter anzeigt und auch nur die für diese Aufgabe notwendigen Informationen mit einem entsprechenden Webdienst austauscht.

Aufgrund der weitreichenden Zugriffsmöglichkeiten, die einer Browser-Erweiterung zur Verfügung stehen, könnte das Add-on auch protokollieren, welche Webseiten Sie zu welchen Zeitpunkten aufrufen und welche Texte Ihnen auf diesen angezeigt werden. Die so gewonnenen Informationen könnte das Add-on im Anschluss einfach ohne Ihr Wissen an den Hersteller übertragen – vielleicht sogar unverschlüsselt. Technisch ist es für eine Browser-Erweiterung sogar möglich, die dargestellten Informationen zu verändern oder ihre Anzeige ganz zu verhindern. Ad-Blocker (also solche Add-ons, mit denen Sie verhindern können, dass Sie beim Surfen blinkende Werbebanner angezeigt bekommen) funktionieren zum Beispiel auf diese Art und Weise.

Bei der Auswahl von Add-ons gibt es ein paar Indikatoren, die Ihnen bei der Einschätzung ihrer Vertrauenswürdigkeit helfen können:

- Schauen Sie sich auf der jeweiligen Add-on-Plattform um, wie die Rezensionen des Add-ons aussehen. Klingen sie zu gut, um wahr zu sein? Berichten andere Nutzer von Problemen mit dem Datenschutz?
- Liegt der Quelltext des Add-ons für alle Nutzer zur Einsicht vor – das heißt, ist das Add-on Open Source? Wie wir schon an anderer Stelle erklärt haben, heißt das nicht, dass Sie den Quelltext wirklich selbst auf Sicherheitslücken inspizieren müssen. Open-Source-Programme unterliegen in der Regel der Kontrolle einer ganzen Reihe von freiwilligen Softwareenthusiasten, die genau das tun (insbesondere, wenn Probleme oder Unklarheiten zu dem Add-on auftauchen) – den Quelltext auf Fehler und Unseriositäten untersuchen.
- Steckt ein großes Unternehmen, dem Sie ohnehin bereits vertrauen, hinter der Browser-Erweiterung oder ist es stark an deren Entwicklung beteiligt? Nicht dass wir glauben, dass große Unternehmen per se vertrauenswürdig sind (beispielsweise hat sich Microsoft in der NSA-Affäre nicht mit Ruhm bekleckert, und über den Datenhunger von Google haben wir ebenfalls an anderer Stelle schon gesprochen). Aber die Software großer Unternehmen hat zum einen oft eine weit größere Nutzergemeinde als die kleinerer Unternehmen oder Privatpersonen, sodass die Wahrscheinlichkeit steigt, dass Unstimmigkeiten in der Benutzung auffallen. Zum anderen ist kleinkriminelles Datenfischen, beispielsweise nach Kreditkartendaten, für einzelne böswillige Programmierer durchaus ein gangbares Geschäftsmodell, größere Unternehmen dagegen lassen sich darauf eher nicht ein, da ein Vertrauensverlust ihrer Kunden für sie einen viel größeren wirtschaftlichen Schaden bedeutet.
- Ist das Add-on in einer vertrauenswürdigen Art und Weise zertifiziert oder wird es ausdrücklich durch eine vertrauenswürdige Organisation wie die EFF (Electronic Frontier Foundation) empfohlen?

Manche Add-ons lassen sich nicht direkt über eine der browserspezifischen Add-on-Plattformen herunterladen, sondern müssen manuell installiert werden. Achten Sie in diesem

Falle darauf, dass Sie das Add-on über eine sichere Verbindung (https://..) und von einer vertrauenswürdigen Stelle beziehen.

Hinweis

Prism Break

Eine sehr empfehlenswerte Seite, auf der Sie Bewertungen und Empfehlungen zu vielen Browser-Add-ons und anderen Programmen finden, ist *Prism Break*. Die deutsche Sprachversion finden Sie auf https://prism-break.org/de.

3.2.5. Ausblick

Für lange Jahre war *Microsoft Internet Explorer* der meistverwendete Browser auf Windows-Geräten (und daher auch der meistverwendete Browser überhaupt), unterstützt vor allem durch die Marktmacht von Microsoft. In den letzten Jahren hat der Internet Explorer allerdings deutlich an Nutzern verloren, insbesondere zugunsten von Chrome, Firefox und Safari. Anfang 2015 wurde bekannt, dass der Internet Explorer nun abgelöst werden soll – Microsoft plant einen neuen Browser, der im März 2015 in einer Testversion veröffentlicht wurde. Die Entwicklung erfolgte unter dem Codenamen Spartan, der fertige Browser kommt nun unter dem Namen *Microsoft Edge* als Standardbrowser von Windows 10 auf den Markt. Der Internet Explorer wird jedoch noch nicht ganz in Rente geschickt, sondern aus Kompatibilitätsgründen noch eine Weile weiter gepflegt. Microsoft Edge soll vor allem erweiterte Möglichkeiten der Synchronisation mit der Cloud anbieten. Wie gut die Daten der Nutzer dabei geschützt werden, wird sich wohl erst im Lauf der Zeit zeigen.

Im Hause Apple bestand zwar lange der Trend, die Verwendung von Browsern anderer Hersteller so weit wie möglich zu erschweren, vor allem auf den Apple-Mobilgeräten: Die freien Browser *Opera*, *Chrome* und *Firefox* sind aber inzwischen für OS X erhältlich, und unter iOS laufen *Chrome* und *Opera*, aber nicht *Firefox*. Apple-Kunden nehmen das bewusst oder unbewusst in Kauf, weil sie den Bedienkomfort des Apple-Kosmos schätzen.

3.3 Cookies – digitale Krümelmonster

Im Zusammenhang mit dem Browser haben wir sie schon kurz erwähnt – *Cookies* sind kleine Textdateien, die auf Ihrem Rechner gespeichert werden und zeitlich beschränkt bestimmte

Informationen archivieren. Cookies werden meist dazu verwendet, um Informationen über schon besuchte Webseiten, die verwendete Browser-Software oder bestimmte Einstellungen und Erweiterungen des Browsers zu speichern. Cookies sind in Verruf geraten, da sie zum Teil sehr detailliert das gesamte Surfverhalten speichern und ungefragt, also ohne Ihre Zustimmung, weitergeben. Diese detaillierten Informationen können dazu dienen, Ihren Rechner wiedererkennbar zu machen: Das heißt, selbst wenn keine persönlichen Daten durch die Cookies bekannt werden, kann man doch sehen, welche Seiten Sie an welchen Tagen besucht haben.

Cookies haben aber auch sehr sinnvolle Funktionen im WWW, etwa wenn Websites eine Anmeldung erfordern: Durch die Verwendung von Cookies ist es nicht erforderlich, dass der Nutzer sich jedes Mal neu anmeldet. Eine generelle Blockierung von Cookies in den Einstellungen (siehe unten) kann daher schnell zu Problemen beim nächsten Interneteinkauf oder beim Einloggen in einen Account führen.

Welche Cookies in Ihrem Browser gespeichert sind, finden Sie in den Datenschutzoptionen:

- *Firefox*: EINSTELLUNGEN > DATENSCHUTZ > COOKIES ANZEIGEN
- *Chrome*: EINSTELLUNGEN > EINSTELLUNGEN (linke Seitenleiste) > ERWEITERTE EINSTELLUNGEN ANZEIGEN > INHALTSEINSTELLUNGEN (unter DATENSCHUTZ) > ALLE COOKIES UND WEBSITEDATEN
- *Internet Explorer*:
  EINSTELLUNGEN > ALLGEMEIN > BROWSERVERLAUF > EINSTELLUNGEN > DATEIEN ANZEIGEN
  (Cookies erkennen Sie an einem vorangestellten »cookie« im Dateinamen)
- *Safari*: EINSTELLUNGEN > DATENSCHUTZ> dort Einstellungen zu den Cookies
- *Opera*: EINSTELLUNGEN > DATENSCHUTZ&SICHERHEIT > COOKIES > ALLE COOKIES UND WEBSITEDATEN einsehen

Gemäß geltenden Datenschutzbestimmungen (EU-Richtlinie von 2009) dürfen Cookies nur nach vorheriger Einwilligung durch den Nutzer gesetzt werden. Nichtsdestotrotz setzen viele Websites Cookies, ohne Sie als Nutzer um die Erlaubnis zu fragen – bei anderen erhalten Sie den Hinweis, dass Cookies gesetzt werden, und müssen sich einverstanden erklären, wenn Sie den Inhalt der Webseite sehen wollen. Cookies sind jedoch nicht versteckt, Sie können sie also einsehen und löschen:

- *Firefox*: EINSTELLUNGEN > DATENSCHUTZ > dort EINSTELLUNGEN ZU DEN COOKIES

- *Chrome*: Einstellungen > Einstellungen (linke Seitenleiste) > Erweiterte Einstellungen anzeigen > Inhaltseinstellungen (unter Datenschutz) > dort Einstellungen für Cookies
- *Internet Explorer*: Extras > Sicherheit > Browserverlauf löschen (dabei ein Häkchen bei Cookies setzen)
- *Safari*: Einstellungen > Datenschutz > Cookies
- *Opera*: Einstellungen > Datenschutz&Sicherheit > Cookies

Mögliche Einstellungen für Cookies sind:

- Cookies nicht zulassen oder zulassen (hier können jeweils Ausnahmen definiert werden)
- Cookies nur von bereits besuchten oder aktuellen Webseiten akzeptieren
- Cookies von Drittanbietern akzeptieren (hier noch Unterscheidung in besuchte und nicht besuchte Drittanbieter, siehe auch Abbildung 3.10)
- Cookies können bei Schließen des Browsers gelöscht werden.

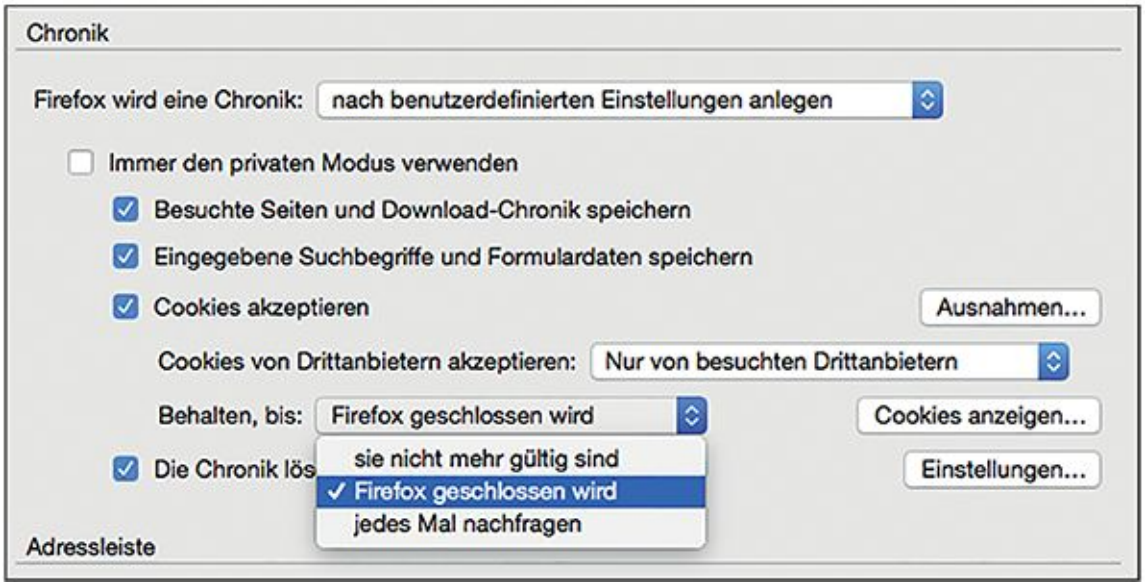


Abb. 3.10 Cookies im Browser Firefox

3.4 Gefällt mir? Werbetracking, Like-Button und Browser-Fingerprints

Im vorigen Abschnitt ging es darum, wie Betreiber von Webseiten mithilfe von Cookies sehen können, welche Webseiten Sie bereits besucht haben. Das wird auch als *Tracking*bezeichnet – man verfolgt sozusagen Ihre Spur im Netz. Warum sollten Webseitenbetreiber ein Interesse daran haben? Klar – auch hier will man Ihnen wieder Werbung unterschieben. Vielleicht ist Ihnen das schon einmal aufgefallen: Nachdem Sie auf einer Shoppingseite Reiseführer für die Pyrenäen, lederne Aktentaschen oder grüne Ringelsocken angeschaut haben, will scheinbar das ganze Netz Ihnen Reiseführer, Aktentaschen oder Ringelsocken verkaufen. Auf allen folgenden Seiten, die Werbeeinblendungen haben, zeigen die Banner ganz ähnliche Produkte wie die, nach denen Sie zuletzt gesucht haben. Das ist dann ein Fall von Werbetracking. Beim Werbetracking erkennen also die zweite, dritte und vierte Webseite, die Sie besuchen, anhand Ihrer Cookies, dass Sie diejenige waren, die auf der ersten Webseite nach Ringelsocken gesucht hat.

Klassische Cookies, wie wir sie im letzten Abschnitt beschrieben haben, sind bis zu vier Kilobyte große (also recht kleine) Textdateien, die im Cookie-Ordner des Browsers abgelegt werden. Es gibt aber schon die nächste, »verbesserte« Generation von Cookies, die es dem

Benutzer bewusst schwer machen wollen, sie zu finden und auszumerzen: die sogenannten Supercookies.

Die am weitesten verbreitete Art von Supercookie ist der *Flash-Cookie* – eine bis zu 100 Kilobyte große Datei, die dem Browser mithilfe von Adobe Flash untergeschoben wird und die sich auch außerhalb des Cookie-Ordners verstecken kann. Einige Flash-Cookies sind besonders perfide und nisten sich an zwei oder mehr Stellen gleichzeitig ein und lassen sich nur endgültig entfernen, wenn man sie an allen Stellen löscht, da sie sich sonst wieder regenerieren – sogenannte Zombie-Cookies. Häufig halten sich die Urheber von Flash-Cookies nicht an die Regel, dass vor der Verwendung von Cookies der Benutzer um Erlaubnis gefragt werden muss. Das Einnisten von Flash-Cookies können Sie jedoch durch Deaktivierung von Flash verhindern. Alternativ können Sie über das Einstellungspanel[8] von Adobe Flash einstellen, wie viel Speicherplatz Flash-Cookies auf Ihrem Rechner einnehmen dürfen.

Besonders meisterhaft versteht es Facebook, Leuten im Netz mit Cookies nachzustellen. Dabei zielt Facebook perfiderweise nicht nur auf seine eigenen Nutzer ab (wobei es keinen Unterschied macht, ob diese ein- oder ausgeloggt sind), sondern auch auf Surfer, die nur zufällig eine Seite ansteuern, auf der sich ein »Like«- oder »Teilen«-Button befindet. Der Besucher bekommt auf solchen Seiten ohne sein Einverständnis einen Cookie untergeschoben, anhand dessen er oder sie auf anderen Webseiten dann wiedererkannt wird. Als Facebook von der belgischen Datenschutzbehörde mit der Unrechtmäßigkeit dieser Praxis konfrontiert wurde, behauptete das Unternehmen zunächst, es handle sich dabei um einen Bug im Code – es sei also gar keine Absicht, sondern ein dummes Versehen gewesen, und man wolle den Fehler bald beheben. Im Mai 2015 veröffentlichte die Datenschutzbehörde einen Bericht, in dem sie die Praktiken von Facebook im Zusammenhang mit den Social-Media-Buttons scharf kritisierte; im Juni 2015 schließlich zog sie gegen Facebook in Brüssel vor Gericht.

Es gibt eine ganze Reihe von Add-ons und Plug-ins, die Ihnen helfen wollen, Cookies und Supercookies zu bekämpfen und Werbetracking zu vermeiden, beispielsweise *Ghostery*, *AdBlock Plus* und *Disconnect*. Besonders empfehlenswert scheint im Moment ein Add-On zu sein, das von der gemeinnützigen Electronic Frontier Foundation (EFF) entwickelt wurde: *Privacy Badger*[9]. Die EFF sagt selbst, dass ihr Ziel war, ein Add-on anzubieten, das sowohl Open Source als auch anwenderfreundlich ist, also mit wenig Einstellungen von Seiten des Benutzers eine hohe Sicherheit und Bedienkomfort bietet. Ziel von Privacy Badger ist nicht, die

Speicherung von Cookies auf Ihrem Rechner allgemein zu unterbinden, da viele Webseiten ohne Cookies kaum richtig funktionieren (beispielsweise jene, für die Sie sich einloggen müssen). Vielmehr blockiert das Programm Cookies von Drittanbietern, also beispielsweise Werbetreibenden. Da die Werbefirmen Ihnen die Werbung personalisiert anzeigen und hierfür Cookies verwenden, hat die Verwendung von Privacy Badger den netten Nebeneffekt, dass Sie insgesamt weniger Werbung angezeigt bekommen, auch wenn es sich nicht explizit um einen Werbeblocker handelt. Leider ist Privacy Badger bisher nur für Chrome und Firefox verfügbar – laut Webseite des Programms wird an der Unterstützung anderer Browser jedoch gearbeitet. Wenn Sie einen der nicht unterstützten Browser benutzen, kommen noch das Open-Source-Programm Disconnect, der Klassiker Adblock Plus (ebenfalls Open Source) und das Programm Ghostery in Frage. Ghostery ist Closed Source und wurde darüber hinaus schon vielfach für die Weitergabe von Informationen an die Werbeindustrie kritisiert, wird aber von einigen Leuten als benutzerfreundlicher empfunden als Disconnect.

Adblock Plus (Screenshot siehe Abbildung 3.11) ist für Firefox, Chrome und Opera verfügbar. Es verwendet Filter, die von vielen Nutzern gepflegt werden, und in denen festgelegt ist, welche Inhalte einer bestimmten Seite Werbung sind – diese Inhalte werden dann nicht angezeigt. Adblock Plus hat in der Netzgemeinde allerdings schon einiges an Gegenwind erfahren, denn es arbeitet mit Webseitenbetreibern zusammen, die dafür bezahlt haben, dass ihre (als unaufdringlich bewertete) Werbung standardmäßig nicht blockiert wird. Wenn Sie auch diese Werbebanner ausblenden möchten, können Sie das aber selbst einstellen:

Unter EXTRAS > ADD-ONS > ERWEITERUNGEN > EINSTELLUNGEN: im Feld ADBLOCK PLUS sollte das Feld ÜBERALL DEAKTIVIEREN kein Häkchen haben, das *Tab zum Blockieren von Flash und Java* dagegen schon. Unter *Filtereinstellungen* finden Sie das Feld EINIGE NICHT AUFDRINGLICHE WERBUNG *zulassen*, das Sie deaktivieren können (oder über LISTE ÖFFNEN bearbeiten). Dort finden Sie auch Ihre Filterlisten und können neue Filterabonnements hinzufügen.

Als Alternative zu Adblock Plus gibt es mittlerweile das Add-on *uBlock* (für Firefox, Chrome und Safari), das auf diese bezahlte Whitelist verzichtet und zudem weniger Systemressourcen beansprucht, was sich positiv auf die Geschwindigkeit beim Browsen auswirkt.

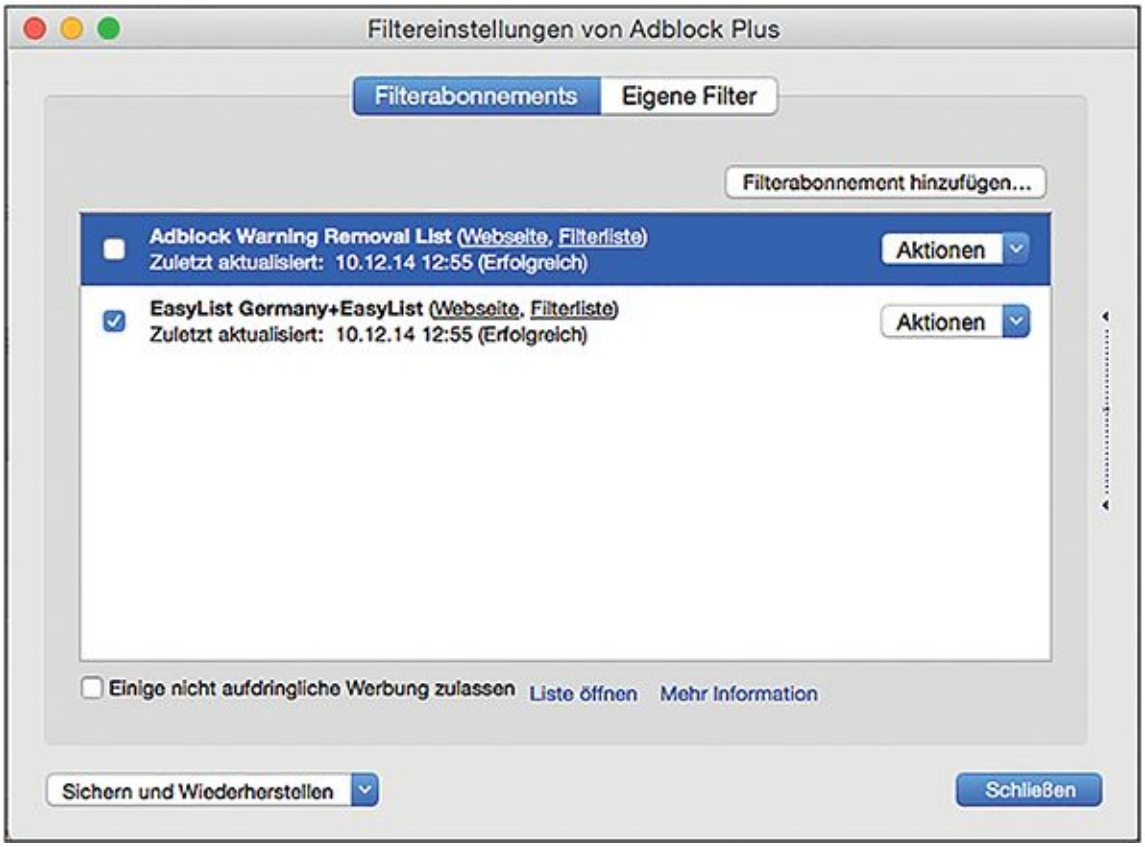


Abb. 3.11 Adblock Plus im Firefox-Browser

Werbetracking kann nicht nur anhand von Cookies und Supercookies erfolgen. Cookies haben ja den Zweck, wie Sie schon gesehen haben, Ihren Browser wiedererkennbar zu machen. Findige Webentwickler haben sich aber überlegt, dass Browser ja auch durch andere Kennzeichen mehr oder weniger eindeutig wiederzuerkennen sind.

Da Webseiten abhängig von den Einstellungen des Clients ganz unterschiedlich aussehen können, schickt Ihr Browser beim Abruf einer Webseite gleichzeitig eine ganze Reihe von Informationen an den Webserver: seine eigene Bezeichnung und die Version, das Betriebssystem, auf dem er läuft, welche Plug-ins Sie installiert haben, in welcher Zeitzone diese laufen, welche Auflösung der Bildschirm hat und natürlich auch, ob Cookies aktiviert sind. Wenn man alle diese Informationen zusammennimmt, gibt es kaum zwei Browser auf der ganzen Welt, die sich gleichen! Die Electronic Frontier Foundation (EFF) hat hierzu eine Studie[10] durchgeführt, bei der Leute ihre Browser-Konfiguration kostenlos testen konnten (und, Stand Juli 2015, immer noch können). Diese Studie ergab, dass unter 470.000 Browsern 85 Prozent mit dieser Konfiguration nur ein einziges Mal vorkamen – und in fünf Prozent der Fälle

kam die gleiche Konfiguration maximal noch bei einem zweiten Besucher vor. Dabei wurden in dieser Studie nicht einmal alle Merkmale berücksichtigt, die ein Browser über sich selbst verrät. Theoretisch könnte die Identifizierbarkeit also noch höher liegen. Das Wiedererkennen Ihres Browsers anhand Ihrer individuellen Konfiguration von Browser und Computer wird auch als *Browser-Fingerprinting* bezeichnet. Mithilfe des Add-ons *Panopticlick*[11] können Sie testen, wie einzigartig Ihre Browser-Konfiguration ist – je seltener genau die Kombination von Einstellungen vorkommt, die Sie haben, desto leichter sind Sie im Web wiederzuerkennen.

Gegen Browser-Fingerprinting gibt es zurzeit nur ein effektives Mittel: das anonyme Surfen, das wir im weiteren Verlauf dieses Kapitels vorstellen werden. Allerdings wird an Add-ons gearbeitet, die Browser-Fingerprinting ebenfalls unterbinden sollen – die EFF will diese Funktion beispielsweise in den *Privacy Badger* aufnehmen.

Um dem zunehmenden Tracking im WWW besser zu begegnen, wurde eine »Do not track«-Funktion mittlerweile von vornherein in viele Browser eingebaut. Mit dieser kann der Nutzer einer Webseite mitteilen, dass er nicht verfolgt werden möchte. Meistens lässt sich diese Funktion über die Einstellungen des Browsers aktivieren:

- *Firefox*: Einstellungen > Datenschutz > Websites mitteilen, meine Aktivitäten nicht zu verfolgen
- *Chrome*: Einstellungen > Einstellungen (linke Seitenleiste) > Erweiterte Einstellungen anzeigen > Mit Browserzugriffen eine »Do not track«-Aufforderung senden
- *Internet Explorer*: Einstellungen > Datenschutz > Tracking-Schutz > Listen für den Tracking-Schutz hinzufügen
- *Safari*: Einstellungen > Datenschutz > dort: Einstellungen zum Website-Tracking
- *Opera*: Einstellungen > Datenschutz&Sicherheit > Eine »Do not track«-Anforderung bei Browserzugriffen mitsenden

Ob die aufgerufene Webseite Ihre Trackingeinstellung respektiert oder nicht, entscheidet allerdings der Betreiber der Webseite selbst. Da die Einstellung Ihnen zumindest keinen Nachteil bringt, würden wir empfehlen, »Do not track« zu aktivieren – sich aber nicht darauf zu verlassen, sondern Cookies im Zweifelsfall von Hand zu löschen.

3.5 Digitale Springteufel: Pop-ups

Pop-ups oder *Pop-up-Fenster* sind plötzlich auftauchende Browser-Fenster oder Registerkarten, die oft Werbung und gelegentlich automatisch abspielende Audio- oder Videodateien enthalten. Pop-up-Fenster kosten einen nicht nur den letzten Nerv, sondern können auch Schad- oder Spionagesoftware enthalten. Das Blockieren von Pop-ups macht das Surfen also nicht nur komfortabler, sondern – je nachdem, welche Seiten Sie besuchen – auch sicherer.

Pop-ups werden meist mithilfe von JavaScript gestartet, das wir im nächsten Abschnitt näher vorstellen. Das heißt, mit der Blockade oder Verwaltung von JavaScript und anderen Skripten, wie weiter unten beschrieben, können Sie viele dieser Pop-ups verhindert werden. Pop-ups können mittlerweile in vielen Browsern auch ohne die Verwendung von Skriptblockern blockiert werden (siehe Abbildungen 3.12 bis 3.14). Sie bekommen dann in der Regel vom Browser eine Meldung angezeigt, dass ein Pop-up blockiert wurde, und haben die Möglichkeit, es von Hand zuzulassen (wenn es beispielsweise ein für die Benutzung der Webseite notwendiges Log-in-Fenster ist).

Abb. 3.12 Meldung über blockiertes Pop-up im Browser Firefox

Abb. 3.13 Meldung über blockiertes Pop-up im Browser Chrome

Abb. 3.14 Meldung über blockiertes Pop-up im Browser Opera

Generell ist es also empfehlenswert, Pop-ups gar nicht oder nur für ausgewählte Internetseiten zuzulassen. Dies können Sie in den Einstellungen oder Optionen Ihres Browsers einstellen.

Firefox: EINSTELLUNGEN > INHALT > POP-UP-FENSTER BLOCKIEREN; wenn Sie möchten, *Ausnahmen* definieren

Chrome: EINSTELLUNGEN > EINSTELLUNGEN (linke Seitenleiste) > ERWEITERTE EINSTELLUNGEN ANZEIGEN > INHALTSEINSTELLUNGEN (unter DATENSCHUTZ) > dort EINSTELLUNGEN ZU POP-UPS

Internet Explorer: EXTRAS > INTERNETOPTIONEN > DATENSCHUTZ > POPUP-BLOCKER AKTIVIEREN; außerdem EINSTELLUNGEN > AUSNAHMEN VERWALTEN

Safari: EINSTELLUNGEN > SICHERHEIT > POP-UPS

Opera: EINSTELLUNGEN > WEBSITES (linke Seitenleiste) > POP-UPS > dort EINSTELLUNGEN ZU POP-UPS und gegebenenfalls AUSNAHMEN VERWALTEN

3.6 Freud und Leid mit JavaScript & Co.

Die gängigen Bedienkonzepte moderner Webseiten wären heute undenkbar ohne *JavaScript*: eine Programmiersprache (auch als *Skriptsprache* bezeichnet), in der kleine Programme geschrieben werden, die im Browser ausgeführt werden. JavaScript kann Sie aber auch in Schwierigkeiten bringen, wenn die Betreiber der Webseiten, die Sie besuchen, ihre Seiten nicht ausreichend gegen JavaScript-kundige Angreifer abgesichert haben.

3.6.1. Ein Hintertürchen für den Angreifer: JavaScript und XSS

Cross-Site-Scripting (XSS) ist ein solches Verfahren, mit dem Sie beim Besuch von Webseiten angegriffen werden können. XSS kann an Webseiten durchgeführt werden, an die der herkömmliche Benutzer Daten verschickt, also nicht an reinen Textseiten. Da heutzutage aber sehr viele Webseiten auch Benutzereingaben akzeptieren – ob in Suchfeldern, Masken für die Eingabe eigener Texte oder Log-in-Fenstern – sind auch fast alle Webseiten zumindest theoretisch empfänglich für XSS.

Der Angreifer geht beim XSS folgendermaßen vor: An einer Stelle, an der eigentlich eine harmlose Texteingabe vom Benutzer erwartet wird, schickt er stattdessen schädlichen Code an den Server. Angenommen, das Ziel des XSS-Angriffs ist eine Onlineauktionsseite. Der Angreifer könnte in diesem Fall so tun, als wollte er ein neues Angebot eröffnen. Statt einer Texteingabe fügt er in die Artikelbeschreibung den oben erwähnten Schadcode ein. Dieser wird mitsamt den anderen Angaben aus dem Onlineformular zum Webserver gesendet und dort als neues Angebot gespeichert – beispielsweise für ein gebrauchtes Auto. Wenn Sie nun dieses Angebot für einen kaum gefahrenen Opel Astra in Metallic Neptuntürkis aufrufen, veranlassen Sie, dass

der Schadcode auf Ihrem eigenen Computer ausgeführt wird. Neben JavaScript kommen auch andere Programmiersprachen und -plattformen in Frage, etwa Adobe Flash (mit der Programmiersprache ActionScript). Auch das AJAX-Konzept (AJAX steht dabei für Asynchronous JavaScript and XML) kann für solche Angriffe genutzt werden: Durch AJAX werden neue Inhalte auf eine Seite geladen, ohne dass die Seite selbst neu geladen wird, beispielsweise, wenn Sie auf einem Blog oder Gästebuch immer weiter nach unten scrollen.

Was genau der Schadcode tut und welche Rechner oder Systeme sein Ziel sind, hängt von den Zielen des Angreifers ab. Ein weit verbreiteter Angriff ist der *Cookie-Diebstahl*. Dabei passiert genau das, was der Name vermuten lässt: Der Angreifer erbeutet Ihren aktuellen *Sitzungscookie* und kann dann in Ihrem Account, das heißt, in Ihrem Namen, alles tun, was auch Sie auf der entsprechenden Webseite tun können. Im Falle eines Onlineauktionshauses wäre das fatal: Er könnte in Ihrem Namen für Auktionen bieten und die Lieferadresse ändern, Artikel zum Verkauf einstellen, Ihre alten Nachrichten lesen und neue schreiben und möglicherweise sogar Ihre gespeicherten Bankdaten abgreifen.

Hinweis

Sitzungscookie

Mithilfe des Sitzungscookies weist ein Nutzer sich gegenüber dem Webserver aus. Wenn Sie sich also beispielsweise bei Amazon einloggen, dann eine Suche ausführen und ein Buch in Ihren Warenkorb legen und dann vielleicht noch ein zweites Buch aufrufen, haben Sie die Webseite mehrmals neu geladen – trotzdem weiß die Amazon-Seite noch, dass Sie Sie sind und dass Sie genau dieses eine Buch im Warenkorb haben. Das ist so dank des Sitzungscookies, der Amazon gegenüber anzeigt, dass Sie der gleiche Nutzer sind, der auch die letzten paar Seiten aufgerufen hat.

Neben Cookie-Diebstahl sind aber auch andere Aktionen des Schadcodes möglich: beispielsweise Dateien von Ihrem Computer an den Angreifer zu schicken.

Bösartiger JavaScript-Code kann darüber hinaus auch auf Webseiten auftauchen, die eigens für diesen Zweck konstruiert sind und nicht vom Angreifer zweckentfremdet wurden. Beispielsweise könnte ein Angreifer seinen Schadcode auf einer Webseite auf seinem eigenen Server unterbringen und per Spam einen Link auf diese Webseite verschicken. Das ist einer der Gründe, warum Sie keinen Links folgen sollten, die Sie ohne Aufforderung geschickt

bekommen. In diesem Zusammenhang spricht man nicht von Cross-Site-Scripting, die Auswirkungen des Schadcodes sind aber prinzipiell die gleichen.

Die Verantwortung zur Verhütung von XSS und schädlichem Programmcode allgemein liegt vor allem bei den Betreibern von Webseiten – die Eingaben, die ein Server akzeptiert, müssen daraufhin geprüft werden, ob sie Schadcode enthalten.

Wenn ein Betreiber dieser Verantwortung nicht nachkommt, bleiben Sie auf dem Problem sitzen. Was können Sie also selbst tun, um XSS zu verhindern? XSS ist darauf angewiesen, dass aktive Elemente auf der Webseite ausgeführt werden, die Sie besuchen. Sicherer ist es also, JavaScript und Flash auszuschalten, wenn Sie Webseiten besuchen, die einen unseriösen Eindruck machen. Im Menü OPTIONEN beziehungsweise EINSTELLUNGEN lässt sich bei allen gängigen Browsern festlegen, ob Programme verschiedener Plattformen (beispielsweise Flash oder JavaScript) ausgeführt werden sollen. Wenn Sie sicher surfen wollen, sollten Sie überlegen, ob Sie diese nicht standardmäßig ausschalten – wenn Sie auf einer Webseite sind, die ohne diese Elemente nicht funktioniert, erhalten Sie eine Meldung und können in diesem Moment immer noch individuell entscheiden, die Ausführung des Programms für diese eine Seite zu erlauben. Diese Maßnahme kann allerdings dazu führen, dass Sie sich anfangs in jedem Onlineshop, in jedem Forum und bei jedem Blog, das AJAX einsetzt, durch Warnmeldungen klicken müssen.

Eine bequemere Lösung ist das Open-Source-Plug-in *NoScript*[12], das unter anderem von Edward Snowden empfohlen wurde. NoScript bietet Ihnen die Möglichkeit, sich eine sogenannte Whitelist von Webseiten anzulegen, die Sie als vertrauenswürdig ansehen und auf denen JavaScript, Flash und andere Skripte ausgeführt werden dürfen (siehe Abbildung 3.15). Diese Whitelist müssen Sie zu Beginn selbst anlegen und pflegen, zum Beispiel, indem Sie JavaScript und andere Skripte auf der Seite des Onlineauktionshauses Ihres Vertrauens immer (oder für eine jeweilige Sitzung) erlauben. Alternativ können Sie auch eine Whitelist aus einer vertrauenswürdigen Quelle importieren. NoScript erlaubt insgesamt eine sehr detaillierte Verwaltung verschiedenster Skripte und Situationen. Leider ist NoScript bisher nur für Mozilla Firefox und verwandte Browser (*SeaMonkey*, *IceWeasel*) verfügbar.

Sollte einmal gar nichts mehr funktionieren, können Sie temporär auch alle Skripte für eine Webseite aufheben (TEMPORÄR ALLE BESCHRÄNKUNGEN FÜR DIESE SEITE AUFHEBEN) oder, wenn das nicht

ausreicht, *Skripte allgemein erlauben*. Alternativen für andere Browser sind *ScriptSafe* und *ScriptBlock* (*Chrome*) und *JavaScriptBlocker* (*Safari).*

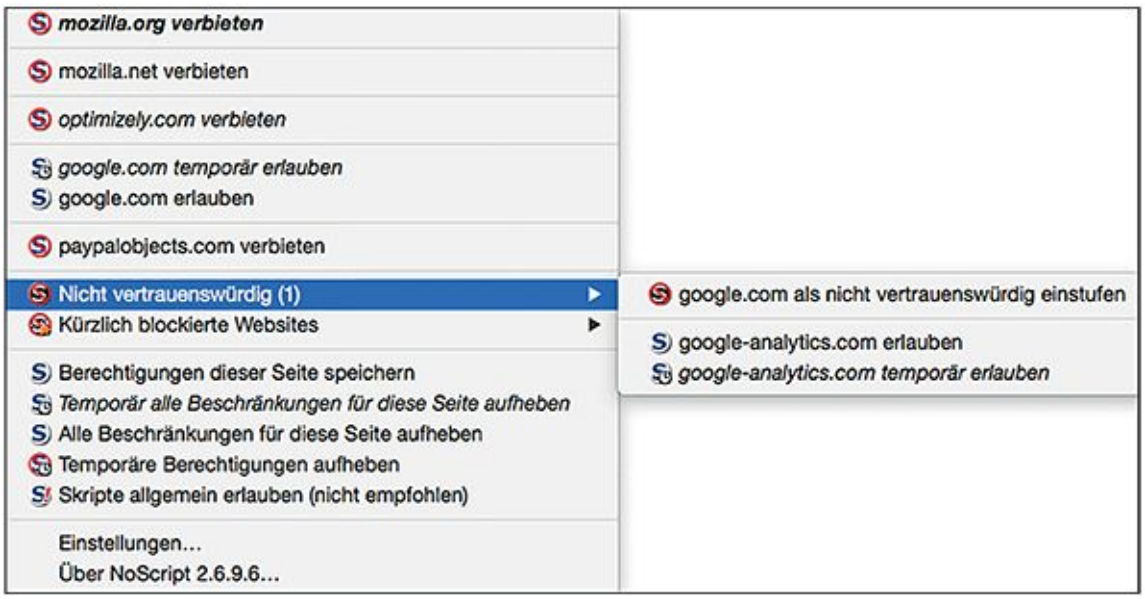


Abb. 3.15 NoScript für den Browser Firefox

QuickJava (*Firefox*) ist ebenfalls Open Source und bietet neben den Einstellungen für Java und JavaScript auch die Möglichkeit, Einstellungen für Cookies, Bilder und animierte Bilder festzulegen (siehe Abbildung 3.16). Insgesamt ist QuickJava einfacher zu bedienen als NoScript, bietet aber keine webseitenspezifischen Einstellungen im Sinne einer Positiv/Negativ-Liste (Whitelist) oder Speicherung dieser Einstellungen an (siehe Abbildung).

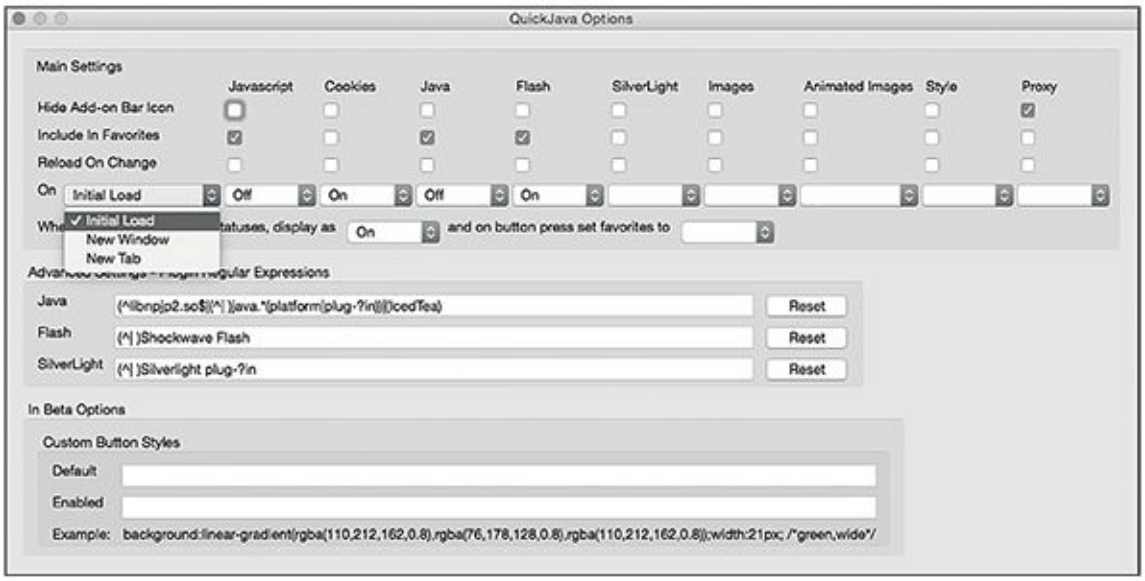


Abb. 3.16 QuickJava für den Browser Firefox

Die Verwendung von Script-Tools ist am Anfang gewöhnungsbedürftig: Sie müssen erst einige Zeit mit Ihrem Browser auf verschiedenen Seiten unterwegs sein, um zu sehen, welche Plug-ins oder Skripte beispielsweise Ihre Bank benötigt, und dann manuell die Verwendung erlauben oder verbieten. Nach ein wenig Eingewöhnungszeit haben Sie dann aber mit einem solchen Skriptblocker die komplette Kontrolle über die Plug-ins und Skripte, die auf Ihrem Rechner ausgeführt werden.

3.6.2. Standortbestimmung: Wo bin ich und warum?

Auch die Ortserkennung ist eine Form, Nutzer und ihr Verhalten zu verfolgen: Haben Sie sich auch schon mal gefragt, wieso immer genau die Stadt oder Gegend, aus der Sie eine Website wie Google Maps aufrufen, schon voreingestellt angezeigt wird? Woher weiß der Kartendienst Ihren Aufenthaltsort, ohne dass Sie ihn ihm explizit mitgeteilt haben, also ohne dass Sie einen GPS-Empfänger (zum Beispiel mit dem Smartphone) genutzt oder sich mit einem Account angemeldet haben?

Diese *Standortbestimmung* wird auch als *Geolokalisierung* oder *Geolocation* bezeichnet und wird ebenfalls in der Regel mithilfe von JavaScript umgesetzt. Wenn Sie mobil unterwegs sind, sich also mit einem Smartphone oder über ein WLAN ins Internet einwählen, sendet der Browser alle verfügbaren WLANs und Mobilfunkstationen inklusive Empfangsstärke an einen Lokalisierungsdienst, der dann Ihren Standort ermittelt. Google (und einige andere Dienste)

haben die Kennung von WLAN-Routern kartografiert und können Sie anhand der gespeicherten WLAN/Mobilfunkstationen recht genau zuordnen. Aber auch einen Rechner, der per Netzwerkkabel (LAN) ans Internet angeschlossen ist, kann man lokalisieren: Hier wird Ihre IP-Adresse verwendet, die Sie von Ihrem Provider erhalten haben und die lokal vergeben wird. Die Lokalisation mithilfe der IP-Adresse ist etwas ungenauer und zeigt oft nur die Stadt oder ggf. den Stadtbezirk (und nicht die genaue Straße) an, in dem Sie sich befinden – eine Information, die Sie aber vielleicht auch nicht immer teilen möchten. Da Sie nur über die IP-Adresse von der Gegenseite angesprochen werden können, müssen Sie immer eine IP-Adresse senden – Sie können daher das Problem der Standortbestimmung über die IP-Adresse nur vermeiden, wenn Sie eine anonyme IP-Adresse verwenden. Wie das geht, zeigen wir Ihnen weiter unten.

Die Ermittlung Ihres Standorts per IP-Adresse ist allerdings nur eine Möglichkeit für Webseiten, Sie zu lokalisieren. Alternativ kann eine Webseite nämlich auch Ihren Browser bitten, Ihren Standort mitzuteilen. Der Browser weiß dies beispielsweise aus den Einstellungen des Betriebssystems oder, im Falle eines Mobilgeräts, aus GPS-Informationen. Sie können Ihrem Browser auch untersagen, diese Informationen zu senden:

Firefox: about:config in die Adressleiste eingeben > Suche nach geo.enabled > Wert durch Doppelklick auf false setzen

Chrome: Einstellungen > Einstellungen (linke Seitenleiste) > Erweiterte Einstellungen anzeigen > Inhaltseinstellungen (unter Datenschutz) > dort Einstellungen zum Standort

Internet Explorer: Extras > Internetoptionen > Datenschutz > Nie zulassen, dass Websites Ihren physikalischen Standort anfordern

Safari: Einstellungen > Datenschutz > dort: Einstellungen zu Website-Verwendung von Ortungsdiensten

Opera: Einstellungen > Datenschutz&Sicherheit > dort Einstellungen zur Standortbestimmung

3.6.3. Plug-ins

Wie oben dargestellt, können HTML-Dateien neben Text auch andere Bestandteile enthalten – die meisten Browser unterstützen beispielsweise standardmäßig gängige Bildformate wie JPEG oder GIF.

Videos und andere Multimedia-Inhalte benötigen zur Anzeige im Browser oft spezielle Plug-ins. Wenn Sie eine Seite besuchen, die ein bestimmtes Format abspielen will, und Ihnen das entsprechende Plug-in fehlt, erscheint meist ein Hinweisfenster, in dem die Installation dieses Plug-ins empfohlen wird. Häufig benötige Plug-ins sind etwa *Shockwave*, *Flash*, *QuickTime Player* (beide vor allem für Audio- und Videodateien), *Java* und *Silverlight*.

Plug-ins können Einfallstore für Schadsoftware sein, weil ein Plug-in ein externes Programm ist – anders als ein Add-on wird es genau genommen nicht Teil des Browsers, wenn es installiert wird. Es unterliegt daher nicht unbedingt den Sicherheitsbeschränkungen des Browsers und kann auf andere externe Programme auf Ihrem Rechner zugreifen. Dadurch können bei entsprechenden Sicherheitslücken im Plug-in auch fremde Programme auf Ihrem Rechner gestartet oder vorhandene Programme und Inhalte verändert werden. Wichtig ist daher, dass Sie Ihre Plug-ins immer aktuell halten, also Updates nach Verfügbarkeit sofort herunterladen und installieren, um neu entdeckte Sicherheitslücken zu schließen.

In den Einstellungen oder Optionen Ihres Browsers können Sie festlegen, wie Plug-ins sich auf Ihrem Rechner verhalten sollen. Abgesehen vom Sicherheitsaspekt können Plug-ins ja auch ziemlich nervig sein, wenn zum Beispiel Videos ohne eine Startsignal und ohne Vorwarnung (etwa im Großraumbüro ..) abgespielt werden. Über die Einstellungen Ihres Browsers können Sie daher nicht nur die aktuell installierten Plug-ins anzeigen lassen, sondern auch festlegen, dass sie nur auf Mausklick hin (statt automatisch) gestartet werden sollen.

Firefox: EXTRAS > ADD-ONS > PLUGINS (linke Seitenleiste) > dort Anzeige aller installierten Plug-ins und Einstellungen[13] (siehe auch Abbildung 3.17)

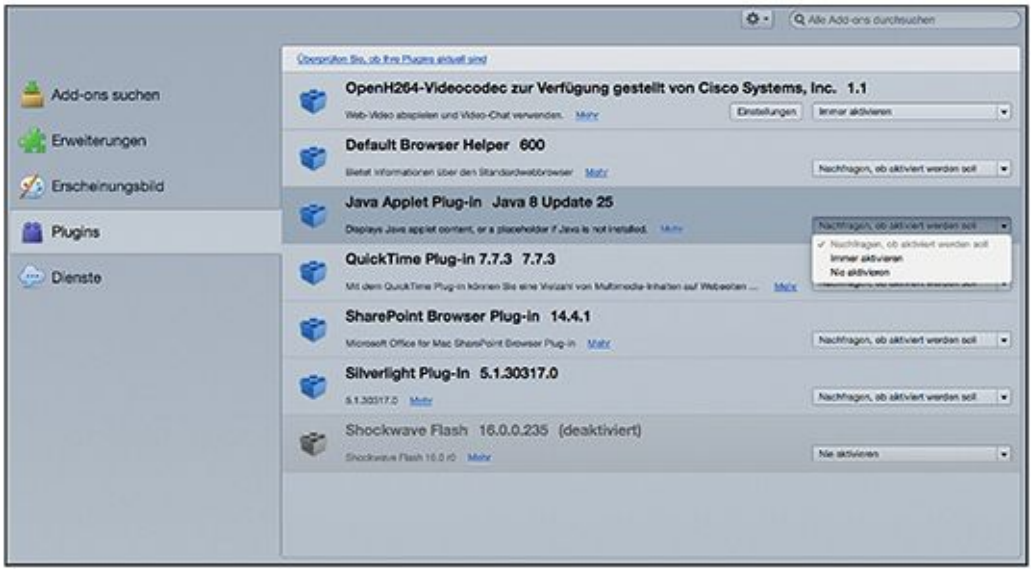


Abb. 3.17 Plug-ins im Browser Firefox

Chrome: EINSTELLUNGEN > EINSTELLUNGEN (linke Seitenleiste) > ERWEITERTE EINSTELLUNGEN ANZEIGEN > INHALTSEINSTELLUNGEN (unter DATENSCHUTZ) > dort Einstellungen zu Plug-ins (*Automatisch ausführen*, *Click-to-Play* oder *Block all*; siehe auch Abbildung 3.18) sowie EINZELNE PLUG-INS DEAKTIVIEREN

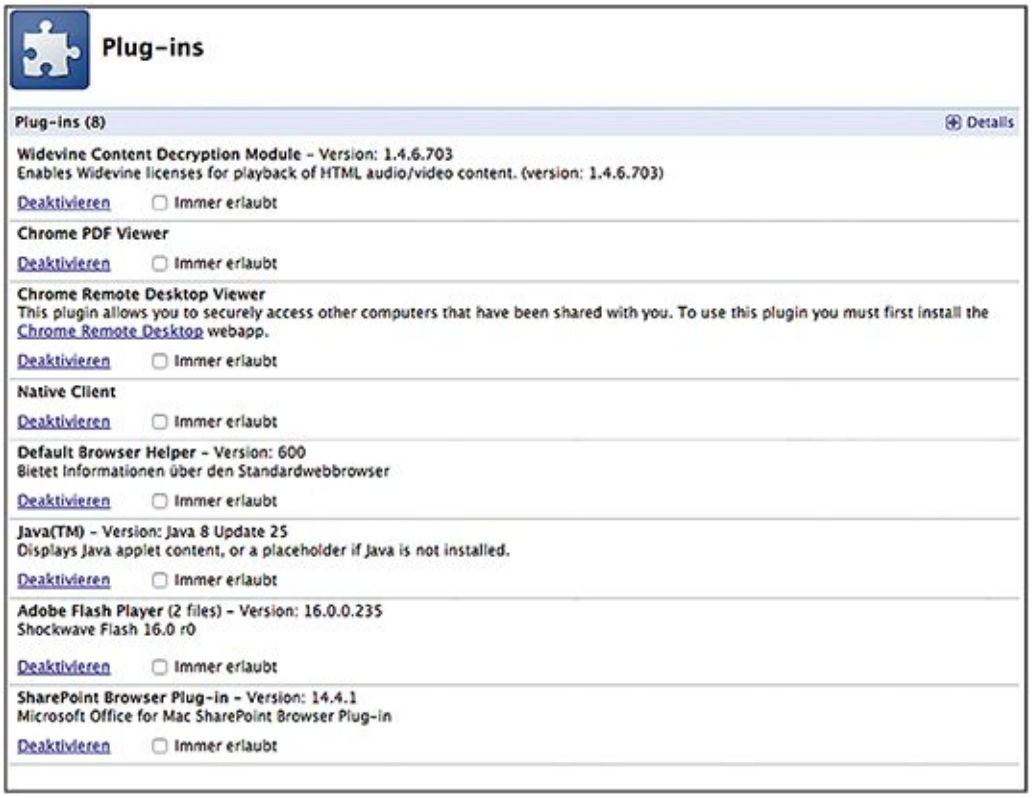


Abb. 3.18 Plug-ins im Browser Chrome

Weiter unten in den Chrome-Inhaltseinstellungen finden Sie noch Einstellungen zum *Plug-in-Zugriff ohne Sandbox* (diese sollten Sie verbieten oder nur auf Nachfrage starten).

Internet Explorer: EXTRAS > ADD-ONS VERWALTEN > ANZEIGEN > ALLE ADD-ONS > DEAKTIVIEREN (um einzelne Plug-ins zu deaktivieren, siehe auch Abbildung 3.19) oder EXTRAS > INTERNETOPTIONEN > ERWEITERT>SICHERHEIT>ERWEITERTEN GESCHÜTZTEN MODUS AKTIVIEREN (um einzustellen, dass vor jedem Plug-in-Start um Erlaubnis gefragt wird)

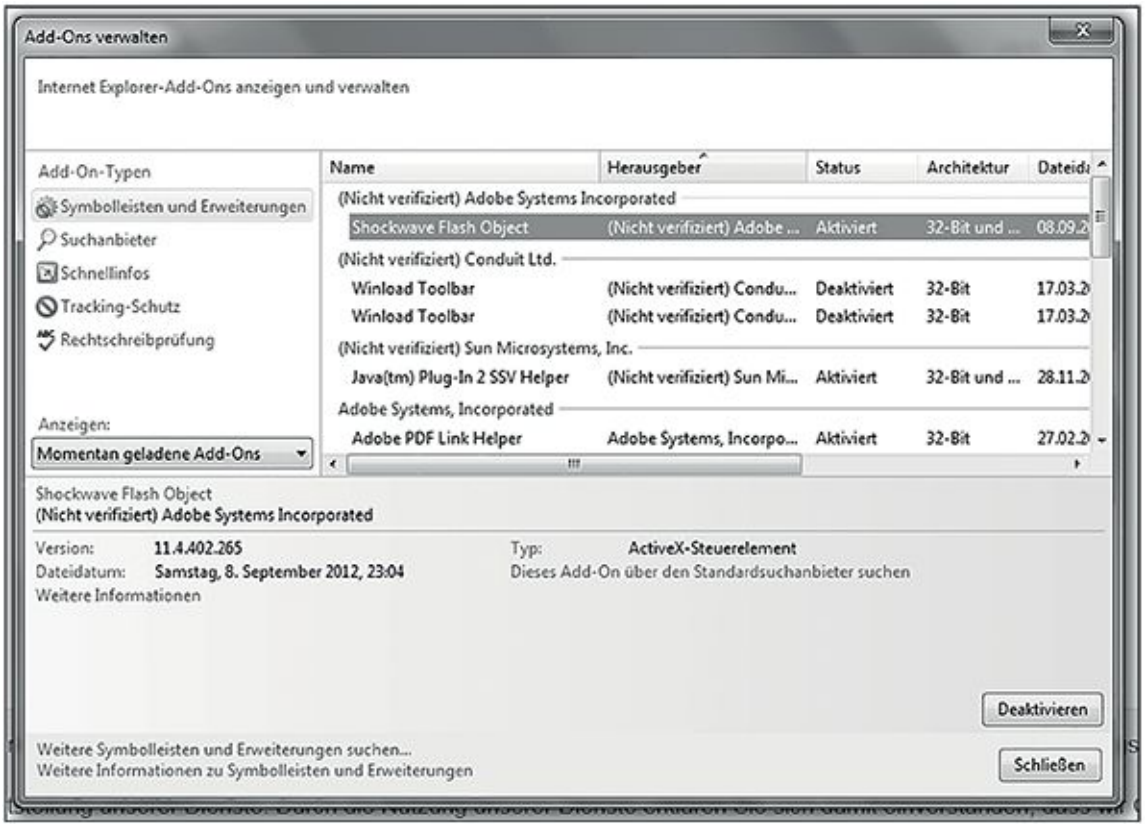


Abb. 3.19 Plug-ins im Browser Internet Explorer

Safari: EINSTELLUNGEN > SICHERHEIT > dort PLUG-INS ERLAUBEN und WEBSITE-EINSTELLUNGEN (siehe auch Abbildung 3.20)

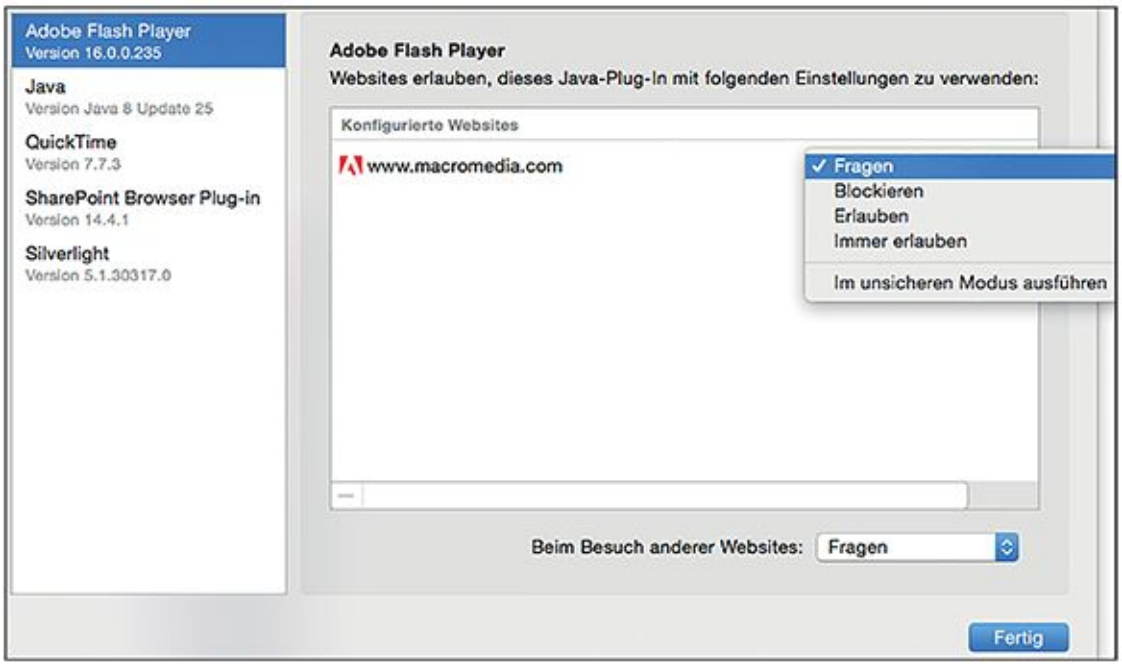


Abb. 3.20 Plug-ins im Browser Safari

Opera: EINSTELLUNGEN > WEBSITES (linke Seitenleiste) > dort Einstellungen zu PLUG-INS (*Plug-ins automatisch starten, Zum Abspielen klicken* oder *Alle Plug-ins blockieren*), AUSNAHMENVERWALTEN und/oder EINZELNE PLUG-INS DEAKTIVIEREN (Abbildung 3.21)

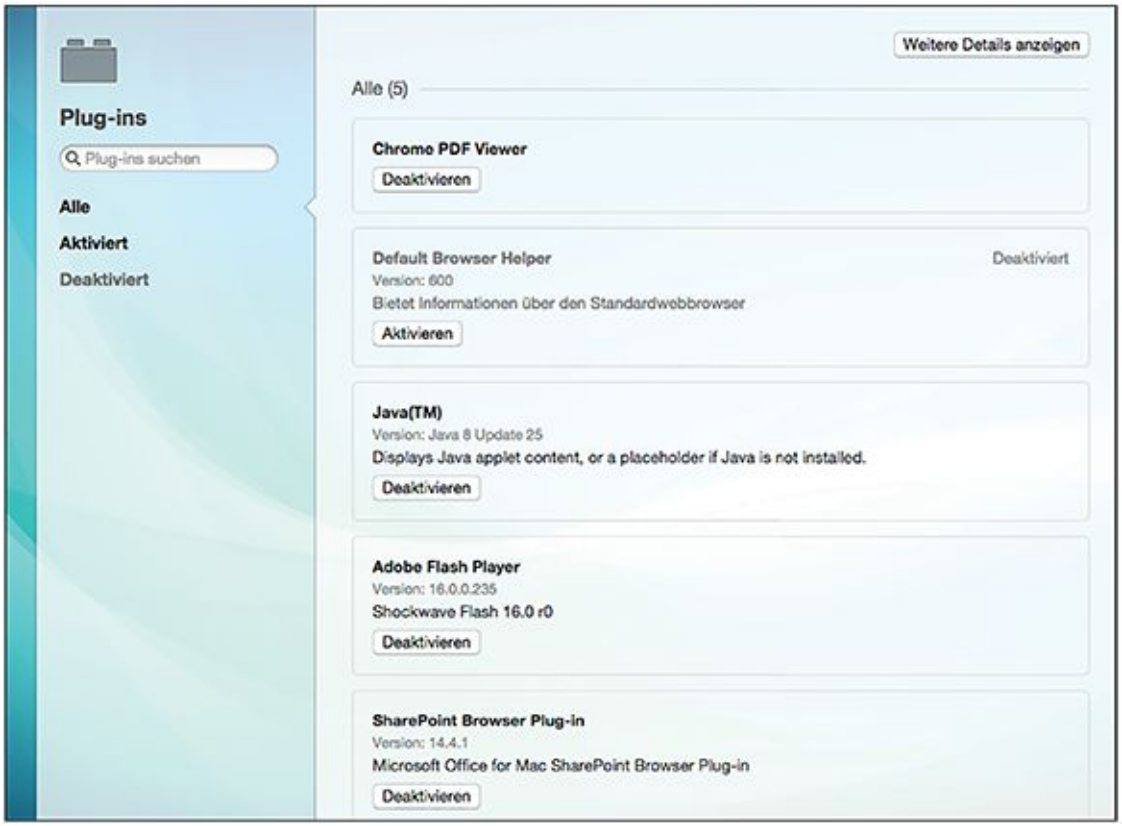


Abb. 3.21 Plug-ins im Browser Opera

3.7 Inkognito im Netz – anonym surfen

Was passiert, wenn Sie im Internet eine Webseite anschauen? Bei einer herkömmlichen Internetverbindung werden Ihre Anfragen von Ihrem Rechner, der eine von Ihrem Provider zugewiesene IP-Adresse hat, über das Netz von Computer zu Computer bis an den Server weitergereicht, auf dem die Webseite liegt und der seine eigene, eindeutige IP-Adresse hat.

Hinweis

Traceroute

Den Weg eines Datenpakets vom Server zu Ihrem Computer können Sie mittels des kleinen Programms *Traceroute* nachvollziehen. Unter Windows können Sie dies in der Eingabeaufforderung mit dem Befehl *tracert* aufrufen, unter Linux in der Konsole mit dem Befehl *traceroute*. Danach nennen Sie die IP-Adresse oder Domain des Zielrechners. Das Programm spuckt Ihnen dann die Liste der IP-Adressen aus, die zwischen Ihnen und dem Zielrechner liegen, sowie die jeweilige Antwortzeit in Millisekunden. Wenn Sie in einer Suchmaschine nach »visual traceroute« oder »graphical traceroute« suchen, werden Sie auch einige Webseiten und Tools finden, die die Informationen aus Traceroute mit geografischen Informationen verknüpfen, Ihnen also anzeigen, wo auf der Weltkarte die zwischengeschalteten Knoten stehen.

Diese Kommunikation über verschiedene Rechner als Zwischenstationen ist ein grundlegendes Charakteristikum des Internets und sorgt unter anderem dafür, dass ein Ausfall einer Zwischenstation durch andere Zwischenstationen kompensiert wird und das Internet weniger störanfällig ist, als es bei einer zentralisierten Struktur der Fall wäre. Das bedeutet aber auch, dass alle Rechner, die als Zwischenstation der Kommunikation dienen, mitlesen können, wer an wen eine Anfrage gestellt hat. Hat man nun einen Zugang zu einem Austauschpunkt für den gesamten Datenverkehr im Internet, einem sogenannten Netzknoten (*Internet Exchange Point, IXP*), so kann man die gesamte Kommunikation (und nicht nur einzelne Pakete) mitlesen. Auch wenn über HTTPS verschlüsselte Nachrichten und Anfragen für die Zwischenstationen nicht lesbar sind, sind die Metadaten (also wer mit wem kommuniziert, siehe auch Kasten) weiterhin für jeden auslesbar. Das heißt, wir wissen zwar nicht, wie viel Geld Alice über die BobCredit überweist, aber wir können sehen, dass sie mehrfach am Tag mit der BobCredit kommuniziert.

Wirklich anonym surfen können Sie also nur, wenn eine verschlüsselte Verbindung über verschiedene, zufällig ausgewählte Netzwerkstationen führt und diese Kommunikationswege nicht gespeichert werden. Ein Nachteil der Anonymisierung über verschiedene Netzwerkstationen ist jedoch, dass Ihre Netzverbindung langsamer wird.

Hinweis

Metadaten

Als Metadaten bezeichnet man den Teil einer Kommunikation, der nicht den eigentlichen Inhalt ausmacht, sondern Informationen »über« dieses Gespräch: Wer hat mit wem wann von wo aus wie lange kommuniziert. Wenn Angela also Bob anruft und mitteilt »Ich komme um 20.15 Uhr zu Hause an«, dann ist ihre Ankunftszeit der Inhalt der Kommunikation. Die Metadaten sind zum Beispiel: Angela kommuniziert über ihr Smartphone mit iOS Version 8.4 mit Bobs Smartphone mit Android Version 4.3 am 23.7.2015 um 18.00 Uhr für 35 Sekunden. Sie ist dabei in den Telefonmasten der Telekom am Berliner Alexanderplatz eingeloggt, Bob dagegen in der Uckermark.

Unser erster Reflex ist, die Metadaten als den weniger schützenswerten Teil der Kommunikation anzusehen, da doch der Inhalt der Kommunikation das Intime ist und nicht die Metadaten. Wenn Sie aber ausreichend viele Metadaten der Kommunikation einer Person kennen, lassen sich daraus erschreckend viele Schlüsse ziehen – am Anfang von Kapitel 6 gehen wir im Detail darauf ein.

Bei der Diskussion um Anonymisierung im Internet wird oft kritisiert, dass solche Netzwerke und Tools nicht nur von Demokratie- und Menschenrechtsaktivisten verwendet werden, sondern auch zur Verschleierung von Straftaten (Drogenhandel, Terrorismus, Kinderpornografie) dienen können. Man sollte aber nicht vergessen, dass es sich beim Internet nur um ein Medium handelt, das per se weder gut noch böse ist – so wie auch über die Festnetzleitung des Telefons der Großmutter zum Geburtstag gratuliert werden oder eine Bombendrohung gegenüber einem Flughafen ausgesprochen werden kann. Die Gesamtheit der Seiten, die nur über Anonymisierungsdienste aufgerufen werden können und nicht von herkömmlichen Suchmaschinen indexiert werden, wird auch als *Dark Web* bezeichnet. Im Dark Web tummeln sich tatsächlich viele Kriminelle und bieten alles Vorstellbare von Drogen, fremden Kreditkartendaten über Waffen und Hehlerware bis hin zu Auftragsmorden zum Verkauf an. Bezahlt wird dabei beispielsweise mit der anonymen Währung *Bitcoin*. Die Verfügbarkeit dieser Waren und »Dienstleistungen« im Internet macht all dies aber natürlich nicht legal, und Straftaten, die über das Dark Web organisiert werden, unterliegen immer noch der Strafverfolgung in den Heimatländern der beteiligten Personen. So wurde der Schwarzmarkt *Silk Road* Ende 2014 ausgehoben und sein Urheber Ross Ulbricht Anfang 2015 in den USA unter anderem wegen Drogenhandels, Betreiben einer kriminellen Vereinigung, Handel mit gefälschten Ausweispapieren und Geldwäsche verurteilt.

Um internetvermittelte Kriminalität zu bekämpfen, wurden 2009 die deutschen Internetprovider zu einer *Vorratsdatenspeicherung* (VDS) für sechs Monate verpflichtet. Dabei wird nicht der Inhalt der Kommunikation gespeichert, sondern Metadaten: Jede Internetverbindung jedes Nutzers wird für sechs Monate beim Provider gespeichert werden. Das bedeutet, Ihre zugewiesene IP-Adresse, der verwendete Port[14], Beginn und Ende der Datenverbindung werden mit Ihren Anschlussdaten gespeichert, bei E-Mails und Internettelefonie (VoIP) auch die Daten Ihres Kommunikationspartners. Diese Daten sind von Sicherheitsbehörden im schlechtesten Fall ohne Gerichtsbeschluss einsehbar. Wie oben aufgeführt, lassen sich über die Metadaten viele und sensible Rückschlüsse über Ihre Kommunikationsgewohnheiten ziehen: Welche Seiten haben Sie nur kurz besucht, welche Seiten[15] besuchen Sie regelmäßig, wiederholt und länger oder wohin haben Sie selbst größere Datenmengen geschickt, das heißt, vielleicht einen Beitrag geschrieben oder Dateien hochgeladen. Auch können durch die Metadaten, die in der Vorratsdatenspeicherung festgehalten werden, ziemlich genaue Bewegungsprofile des Nutzers erstellt werden. Die Vorratsdatenspeicherung ist umstritten und vom Bundesverfassungsgericht 2010 beziehungsweise vom Europäischen Gerichtshof 2014 für unzulässig erklärt worden, wurde aber Mitte 2015 mit den Stimmen der Großen Koalition (gegen die Proteste eines großen Teils der Netzgemeinde) erneut beschlossen. Die Diskussion um die Vorratsdatenspeicherung ist bisher nicht beendet, und ein tieferer Einstieg würde den Umfang dieses Buches sicher sprengen. Durch die Diskussion wurde aber unbestritten die Entwicklung von *Anonymisierungsdiensten* (Anonymizern) vorangetrieben, von denen wir im Folgenden einige vorstellen möchten.

3.7.1. Proxy – Browsen über einen Stellvertreter

Ein erster Schritt in Richtung Anonymisierung (aber nicht der ganze Weg dahin) ist die Verwendung eines *Proxy*. Ein Proxy in einem Netzwerk (von englisch »*proxy*« = Stellvertreter beziehungsweise lateinisch »*proximus*« = der Nächste) nimmt Anfragen entgegen und leitet sie unter der eigenen Adresse weiter. Dadurch ist für den Kommunikationspartner, der die Anfrage erhält, nicht mehr ersichtlich, wer die Anfrage ursprünglich gestellt hat. Proxy-Server können darüber hinaus Anfragen auch inhaltlich verarbeiten: So können häufig benutzte Internetseiten auf dem Proxy-Server zwischengespeichert und dann weitergeleitet werden. Der

Vorteil ist, dass Sie als Nutzer die häufiger aufgerufenen Webseiten schneller angezeigt bekommen. Der Nachteil ist allerdings, dass Sie nur eine Kopie der Seite, nicht das Original sehen – Seiten können auf diesem Weg manipuliert werden oder auch einfach veraltet sein.

Proxies können auch Teil einer Firewall sein, über die der Inhalt der Kommunikation auf Schadprogramme oder Werbung untersucht wird und diese gegebenenfalls blockiert werden. Aber auch die Zensur von Webseiten kann über Proxy-Server erfolgen: Wenn in Ihrer Firma oder in einer Schule bestimmte Webseiten gesperrt sind, liegt das wahrscheinlich an einem entsprechend eingestellten Proxy-Server.

Ziehen wir wieder einmal Bob und Alice als Beispiel heran: Bob will ein Paket an Alice verschicken (in diesem Fall ist Alice ein Webserver, und Bob schickt ihr eine Anfrage). Wenn ein Proxy verwendet wird, ist das so, als ob Bob das Paket seinem Stellvertreter Zach schickt, dem er vertraut. Zach versendet das Paket dann an Alice. Dabei ändert Zach den Absender Bob in seine eigene Absenderadresse – Alice bekommt das Paket also von Zach und kann nicht sehen, dass es ursprünglich von Bob stammt.

Das Beispiel macht klar, dass eine »Anonymisierung« nur zwischen Zach und Alice stattfinden kann. Zach kennt die Identität von Bob in jedem Fall, und wenn er sich entscheidet, sie an Alice oder jemand anderen zu verraten, ist die Anonymität von Bob hinfällig.

Stellen wir uns jetzt vor, Bob schickt das Paket an den Proxy Eve. Eve, die Lauscherin, haben Sie in Kapitel 1 schon kennengelernt. Eve kann das Paket öffnen, kennt den Inhalt des Paketes und kann diesen verändern, entfernen oder ergänzen, ohne dass Alice oder Bob dies merken. Daher sollte die Datenverbindung zu einem Proxy immer verschlüsselt sein – auf diese Art bekommt Eve nur ein versiegeltes Paket, das sie nicht einsehen kann, und kann übertragene Anmeldedaten und Passwörter nicht mitlesen.

Bei der Verwendung insbesondere kostenfreier Proxies sollten Sie sich daher immer fragen, welches Interesse jemand hat, seinen Server für einen solchen Dienst zur Verfügung zu stellen. Einige Proxies werden von Kriminellen nur dazu betrieben, den Datenverkehr für ihre Zwecke auszunutzen. Neben den kostenlosen gibt es auch zahlreiche Anbieter von kostenpflichtigen Proxy-Diensten, die eine Anonymisierung Ihres Surfverhaltens und eine verschlüsselte Kommunikation anbieten.

Wenn Sie ernsthaftes Interesse an anonymisiertem Surfen haben, empfehlen wir Ihnen jedoch, nicht auf einen einfachen Proxy-Dienst zurückzugreifen – aufgrund der oben beschriebenen

Tatsache, dass Sie gegenüber dem Proxy selbst nicht anonym sein können. Eine bessere Chance, dass Ihr Surfverhalten unbeobachtet bleibt – mit einer Ausnahme, wie Sie gleich sehen werden – haben Sie mit dem Tor-Netzwerk.

3.7.2. Tor – anonymes Browsen nach dem Zwiebelprinzip

Ein einzelner Proxy schützt also noch nicht Ihre Anonymität, wie Sie gerade gesehen haben – mehrere Proxies dagegen bringen Sie schon einen Schritt näher ans Ziel. Angenommen, Sie haben einen verschlüsselten Proxy, der Ihre Anfrage an einen anderen Proxy weiterreicht, der ebenfalls verschlüsselt, und so weiter, bis zum Ziel Ihrer Anfrage: Dann wird es für einen Lauscher schon wesentlich schwerer, den Inhalt Ihrer Kommunikation und Ihre Identität herauszufinden. Nach diesem Prinzip funktioniert das Browsen im *Tor-Netzwerk*.

Das Tor-Netzwerk besteht aus verschlüsselten Proxy-Servern, die ihre Dienste für die anonymisierte Kommunikation zur Verfügung stellen. Der Name Tor stand ursprünglich für *The Onion Routing* – Onion, also Zwiebel, weil die Kommunikation unter verschiedenen Schichten von Verschlüsselung vor Beobachtern versteckt ist, wie die Häute einer Zwiebel. Eine Zwiebel ist auch heute noch das Logo des Tor-Projekts.

Interessanterweise wurde Tor ursprünglich für die US Navy entwickelt, um sensible Regierungskommunikation vor dem Abhören zu schützen. Heute ist das Tor-Netzwerk ein Zusammenschluss von Freiwilligen aus der ganzen Welt und wird von unterschiedlichsten Personen – zum Guten wie zum Schlechten – genutzt. Tor wird beispielsweise von der oben bereits erwähnten *Electronic Frontier Foundation* (EFF) unterstützt und empfohlen.

Um Tor zu verwenden, installieren Sie zunächst einen Tor-Client auf Ihrem Rechner. Dieser Proxy verbindet sich mit dem Tor-Netzwerk über einen Tor-Server. Diese Server sind mit einer digitalen Signatur versehen, und die Kommunikation zum und im Netzwerk erfolgt verschlüsselt. Jeder Server kennt seinen Vorgänger und seinen Nachfolger, aber keine weiteren Server in der Kommunikationskette (wie Sie im Schema in Abbildung 3.22 sehen), und die Verbindungsstrecken werden ungefähr alle zehn Minuten gewechselt.

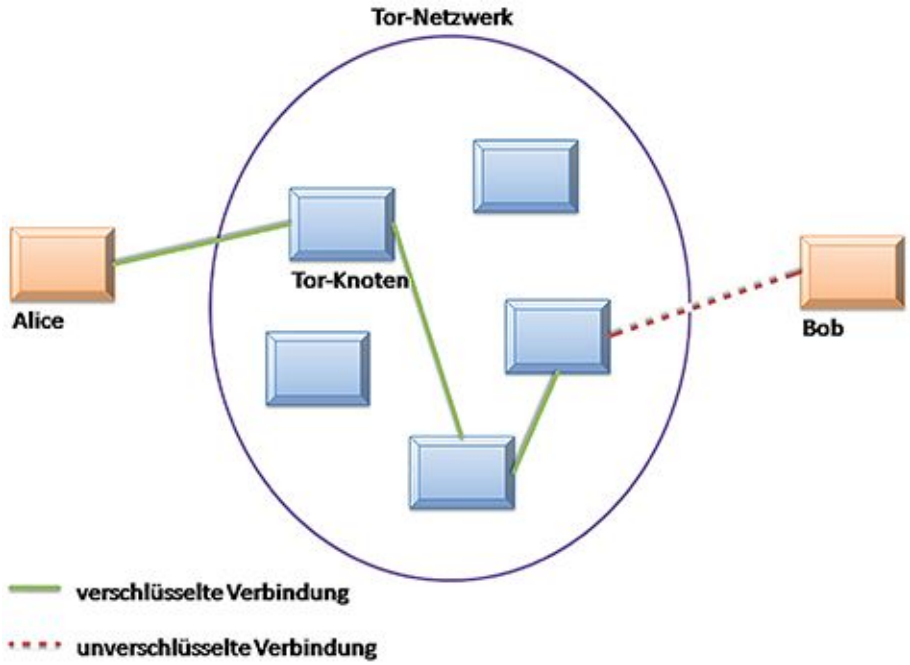


Abb. 3.22 Schema des Tor-Netzwerks

Im Prinzip können Sie mit jedem Browser auf das Tor-Netzwerk zugreifen. Empfehlenswert ist es aber, dies zunächst nur über den *Tor-Browser* zu tun (Screenshot siehe Abbildung 3.23). Dieser ist für alle Betriebssysteme (Windows, Mac OS, Linux sowie für Smartphones) verfügbar. Großer Vorteil bei der Verwendung des Tor-Browsers ist es nämlich, dass er bereits so konfiguriert ist, dass er tatsächlich sicheres Surfen über Tor ermöglicht. Wenn Sie einen anderen Browser verwenden, müssen Sie die Einstellungen selbst so anpassen, dass er Sie nicht aus Versehen auffliegen lässt (also beispielsweise Ihre IP-Adresse verrät) – etwas, das leicht schiefgehen kann, wenn Sie neu in der Tor-Benutzung sind.

Alternativ zum eigenständigen Tor-Browser können Sie auch das *Browser-Bundle* verwenden, das aus einem fertig eingerichteten Browser und einem Client besteht, der auf das Netzwerk zugreift. Das Browser-Bundle ist portabel, das heißt, Sie können es von einem USB-Stick oder einem anderen Wechseldatenträger starten und benötigen keine Installation.

Vor allem in Ländern mit einer ausgeprägten Zensur verweigern Internetprovider ihren Kunden häufig die Verbindung zu bekannten Tor-Einstiegsknoten. In diesem Fall können die Benutzer auf sogenannte Brücken (Bridges) zurückgreifen, also Knoten, die nicht öffentlich bekannt sind. Näheres zu diesem Verfahren findet sich auf den Webseiten des Tor-Projekts (https://www.torproject.org). Hier finden sich auch weitere Hinweise dazu, wie Sie

verhindern, dass Sie aus Versehen die Anonymität aufgeben: beispielsweise, indem Sie auf Torrents (eine bestimmte Art des File-Sharings) verzichten und heruntergeladene Dateien nicht auf Ihrem Computer öffnen, solange Sie noch Tor verwenden.

Wenn Sie im Tor-Netzwerk surfen, kann also zum einen Ihr Surfverhalten nicht mehr nachvollzogen werden. Zum anderen ermöglich Tor auch den Zugang zu Websites, die blockiert sind – ein Aspekt, der mit der steigenden Anzahl von Zugangssperren (leider auch in Ländern mit demokratisch gewählten Regierungen[16]) immer bedeutender wird.

Wie schon angekündigt, garantiert aber auch die Verwendung von Tor keine perfekte Anonymität im Netz. Im Jahr 2014 wurde bekannt, dass einzelne Tor-Benutzer identifiziert werden können, wenn der Angreifer genügend Ressourcen hat, um annähernd den kompletten Verkehr des Tor-Netzwerks, inklusive Ein- und Ausgängen, zu überwachen. Ein Angreifer mit diesen Ressourcen kann nach jetzigem Wissensstand nur der Geheimdienst eines Landes sein. Wenn also ein Geheimdienst es darauf abgesehen hat, Ihren Internetverkehr zu überwachen, können Sie sich also auch mit Tor nicht sicher dagegen zur Wehr setzen.

Abb. 3.23 Startseite des Tor-Browsers nach der Installation

[1] Hypertext bezeichnet eine Protokollfamilie, mit der sich Textinformationen übertragen lassen.

[2] Das muss nicht immer der Fall sein, aber wir gehen hier der Einfachheit halber davon aus.

[3] https://www.eff.org

[4] zum Beispiel Suchanfragen und Standort des Nutzers, sowie Kategorie der aufgerufenen Seiten

[5] zum Beispiel verwendetes Gerät, Alter, Geschlecht, Art des Mobilfunkvertrages

[6] zum Beispiel Klick- und Wahrnehmungsmuster, Anzahl der Klicks und Messung des Erfolgs einer Werbekampagne

[7] Nach persönlicher Erfahrung einer Autorin führte diese Technik bei Opera auf iOS allerdings eher zu einem langsameren Aufbau der mobilen Webseiten als zu einer Beschleunigung. Die Umleitung über den Opera-Server lässt sich allerdings in den Einstellungen deaktivieren.

[8] http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager07.html

[9] https://www.eff.org/privacybadger

[10] https://panopticlick.eff.org/browser-uniqueness.pdf

[11] https://panopticlick.eff.org/

[12] https://noscript.net

[13] Alternativ auch über die Seite https://www.mozilla.org/de/plugincheck/

[14] der Rückschlüsse über den verwendeten Dienst erlaubt, beispielsweise HTTP, E-Mail oder FTP

[15] Da nur einsehbar ist, mit welcher IP-Adresse Sie kommuniziert haben, ist bei kleineren Webpräsenzen, die sich einen Webserver mit anderen teilen, nicht klar, welche davon auf dem Server Sie besucht haben. Nur bei großen Angeboten, die unter einer eigenen IP-Adresse erreichbar sind, ist dies eindeutig festzustellen.

[16] siehe beispielsweise die DNS-Sperren in der Türkei: http://www.pc-magazin.de/news/tuerkei-internet-sperre-dns-server-alternative-twitter-youtube-2142526.html

Kapitel 4 Sicheres E-Mailen

4.1 Wie funktioniert E-Mail?

Herzlichen Glückwunsch! Sie haben soeben eine E-Mail in englischer Sprache von Mr. Johnson Emmanuel aus Nigeria erhalten. Dieser möchte Sie im Geheimen darüber informieren, dass Sie der mutmaßliche Erbe eines 9,5 Millionen Dollar umfassenden Vermögens bei der African Development Bank (ADB) sind. Der rechtmäßige Besitzer ist tragischerweise bei einem Flugzeugabsturz ums Leben gekommen. Mr. Johnson Emmanuel bittet Sie um Ihre Hilfe bei der Abwicklung der Erbschaft und natürlich um Ihre Bankverbindung, damit die Auszahlung schnellstmöglich vorgenommen werden kann. »I need also to trust that you will not tell people or your bank about this business.« – »Ich muss Ihnen [dahingehend] vertrauen können, dass Sie gegenüber anderen Menschen oder Ihrer Bank über dieses Geschäft Stillschweigen bewahren.« Würden Sie Mr. Johnson Emmanuel nun tatsächlich antworten, ihm vielleicht sogar Ihre Bankdaten geben und die »Abwicklungsgebühren« zahlen, die er im Verlauf der weiteren Konversation verlangen wird, wären Sie das Opfer sogenannten »Phishings« geworden. Bestenfalls würden Sie das überwiesene Geld nicht zurückerhalten und auch nie wieder etwas von Mr. Johnson Emmanuel hören.

Im weiteren Verlauf dieses Kapitels werden Sie sehen, dass gegen eine einzelne Phishing- oder Spammails nicht direkt mit Verschlüsselung & Co. vorgegangen werden kann – im Gegenteil, Verschlüsselung kann den Spamfilter sogar behindern, da ein Spamfilter einer verschlüsselten Mail nicht ansehen kann, ob sie eine Einladung zu einer Geburtstagsparty oder zu einem zweifelhaften Investment enthält. Durch den Einsatz von Verschlüsselung und anderen Sicherheitsmaßnahmen wird Spammern aber generell das Leben schwerer gemacht – zum Beispiel weil es für Spammer einen massiven Mehraufwand bedeuten würde, wenn E-Mails nur noch verschlüsselt verschickt werden würden: Schließlich wäre es nicht mehr damit getan, auf einem Schwarzmarkt eine Liste von E-Mail-Adressen zu kaufen, sondern sie müssten beispielsweise auch den zugehörigen Public Key jedes Adressaten ermitteln.

Kaum ein Internetdienst wird also heute so sehr ge- und vor allem missbraucht wie E-Mail. Einerseits ist die E-Mail (Abkürzung für »electronic mail«) der altmodischen Briefpost (auch

gerne als Snail-Mail bezeichnet – englisch »snail« = Schnecke) weit überlegen, weil Nachrichten innerhalb von wenigen Augenblicken übertragen werden können und dabei keine Zustellungsgebühren anfallen. Andererseits bereitet Sie Ihnen vielleicht auch gelegentlich Kopfschmerzen: Wenn Sie beispielsweise aus dem Urlaub zurückkehren und von 1287 ungelesenen Nachrichten in Ihrer Inbox begrüßt werden. 95 Prozent davon sind dann wahrscheinlich unschlagbar günstige Angebote für »Amateur XXX CAMS LIVE« oder brandaktuelle »Strictly Confidential and Urgent Business Proposals«, also im weitesten Sinne digitaler Schrott. Zu allem Überfluss haben unverschlüsselte E-Mails, wie Sie schon wissen, in etwa den gleichen Geheimhaltungswert wie eine der bunten Ansichtskarten, die Sie Ihrem Opa aus dem Urlaub an der italienischen Riviera geschickt haben.

So unsicher und auch lästig es sein mag, so ist E-Mail an sich für viele Zwecke unschlagbar und aus unserem Leben nicht mehr wegzudenken. Für so ziemlich jede personalisierte Anwendung des Internets benötigen Sie zumindest eine E-Mail-Adresse, mit der Sie beispielsweise Anmeldeprozesse bestätigen oder verlorene Passwörter zurücksetzen können. Daneben zweckentfremden viele Menschen E-Mail auch als To-do-Liste, Notizbuch und sogar als Dateiablage (was übrigens auch auf mindestens einen der Autoren dieses Buches zutrifft – die anderen beiden verweigerten hierzu beschämt jegliche Aussage).

Um nun besser auf die Gefahren reagieren zu können, die sich aus der Benutzung von E-Mail ergeben, sollten Sie zunächst verstehen, wie dieser Dienst arbeitet und wo seine verwundbaren Stellen liegen.

4.1.1. E-Mail – die Anfänge

In der 1960er-Jahren, als Heimcomputer noch nicht verbreitet und Tablets und Smartphones undenkbar waren, teilten sich viele verschiedene Benutzer in einer Firma oder einer Universität einen einzigen, großen Computer. Sie begannen, sich gegenseitig Textnachrichten auf dem Computer zu hinterlassen – Vorläufer der heutigen E-Mail. Als diese Computer schließlich an den Vorläufer des Internets, das *ARPANET*, angeschlossen wurden, kam der Elektrotechniker Ray Tomlinson auf die Idee, dass man diese Textnachrichten auch von einem Computer zum anderen senden könnte. So schickte er also im Jahr 1971 die erste E-Mail auf den Weg (und vergaß prompt den Inhalt dieser geschichtsträchtigen Nachricht).

4.1.2. Die E-Mail-Adresse

Die Ursprünge dieser ersten E-Mail spiegeln sich heute noch in jeder E-Mail-Adressewider:

Was eine E-Mail-Adresse sofort als solche erkennbar macht, ist das @-Zeichen in der Mitte. Dieses Zeichen, auf Deutsch liebevoll auch als »Klammeraffe« bezeichnet, heißt auf Englisch »at«, zu Deutsch »auf«, »an« oder »bei«. Damit wird sofort klar, was die Mailadresse alice@cryptocheck.de bedeutet: die Benutzerin Alice auf (dem) Computer cryptocheck.de. Der Teil nach dem @-Zeichen wird auch als Host (wörtlich »Gastgeber«) bezeichnet.

4.1.3. Der Aufbau einer E-Mail-Nachricht

Vereinfacht gesehen sind E-Mails nichts anderes als Textdateien, die mittels verschiedener Protokolle von einem Computer zu einem anderen übertragen werden.

```
From: Alice <alice@cryptocheck.de>
Subject: =?utf-8?Q?N=C3=A4chste_Woche_Mittagessen=3F?=
Date: Sat, 9 May 2015 15:52:58 +0200
Message-Id: <70AD1909-1F06-41EF-A125-
EFC41817DD5E@cryptocheck.de>
To: Bob <bob@cryptocheck.de>
Content-Transfer-Encoding: quoted-printable
Content-Type: text/plain; charset=utf-8

Hallo Bob, hast Du Lust, in der n=C3=A4chsten Woche essen zu
 gehen?

Liebe Gr=C3=BC=C3=9Fe,
Alice
```

Wie Sie sehen, sind nahezu alle in einer E-Mail enthaltenen Informationen für einen Menschen auf den ersten Blick lesbar, wenn diese, wie im obigen Beispiel geschehen, ohne Verschlüsselung übertragen werden.

Eine E-Mail hat folgende grundlegende Elemente:

- eine Absenderadresse (From)

- eine Empfängeradresse (To)
- eine Betreffzeile (Subject)
- den eigentlichen Textkörper (Body)

Das sind also in etwa die gleichen Komponenten, die auch ein geschäftlicher Brief enthalten würde.

Eine E-Mail kann außerdem noch einen Anhang enthalten, also eine oder mehrere Dateien, die mit der E-Mail gemeinsam verschickt werden. Vergleichbar ist der Anhang mit einem Prospekt, der einem Geschäftsbrief beiliegt, oder einem Schnappschuss des Familienhundes, den Sie vor Einführung der E-Mail per Schneckenpost an Tante Erna verschickt haben.

Die E-Mail hat aber noch weitere Komponenten, die keine direkte Entsprechung zur Papierpost haben:

- einen Zeitstempel, der die Zeit der Zustellung in das Postfach des Empfängers angibt (anders als der Poststempel auf einem traditionellen Brief, der den Tag des Briefversandes angibt)
- eine Adresse, an die eine Antwort gehen soll (Reply to) – diese muss nur angegeben werden, falls sie von der Absenderadresse abweicht
- sonstige Steuerinformationen wie zum Beispiel, ob eine Mail als Spam eingestuft wurde, oder welches E-Mail-Programm zum Erstellen der Nachricht verwendet wurde

Alle oben genannten Informationen, außer dem Textkörper und eventuellen Dateianhängen, werden beim Versand der E-Mail im sogenannten »Header« zusammengefasst. Dieser steht immer am Anfang des Quellcodes der E-Mail. Jede Zeile des Headers beginnt mit einem Schlüssel (beispielsweise From, To oder Date), gefolgt von einem Leerzeichen und dem zugehörigen Wert (beispielsweise To: Bob <bob@cryptocheck.de>).

```
Content-Type: multipart/encrypted; protocol="application/pgp-encrypted";
Subject: =?utf-8?Q?N=C3=A4chste_Woche_Mittagessen=3F?=
X-Pgp-Agent: GPGMail 2.5b6
From: Alice <alice@cryptocheck.de>
Date: Sat, 9 May 2015 19:30:53 +0200
Content-Transfer-Encoding: 7bit
```

Message-Id: <110C3F2C-6AFB-4942-97C9-E347AE3A7EC0@cryptocheck.de>
Content-Description: OpenPGP encrypted message
To: Bob <bob@cryptocheck.de>

This is an OpenPGP/MIME encrypted message (RFC 2440 and 3156)
--Apple-Mail=_01BE26A8-D8B1-41F3-A285-B784748FE7C2
Content-Transfer-Encoding: 7bit
Content-Type: application/pgp-encrypted
Content-Description: PGP/MIME Versions Identification

Version: 1

--Apple-Mail=_01BE26A8-D8B1-41F3-A285-B784748FE7C2
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
 filename=encrypted.asc
Content-Type: application/octet-stream;
 name=encrypted.asc
Content-Description: OpenPGP encrypted message

-----BEGIN PGP MESSAGE-----
Comment: GPGTools - https://gpgtools.org

hQIMA8vhQS1fpx1oARAAmrC9lHpdaJgGDYWgm6YJVU8s7Pl7CAXTsLW9dTUqavOn
GoaiYBgfYmd4CuVxM3kc5VuH/ea+fIsudYUWDi1SsZuG4B4

qmKS5uPztBD61ISzQ
Xm1n3vxVlDFrrk/I5+P0H1xyKLQ75Vk51GYmMnMTcY4WR
cYYSbjf4l0BFU1JNyrA

[gekürzt!]

PNbL104kFjDC7e//sidgslIj0D35S7zRiS65mGW0moN+qM/j0g
kzEBeZm1Q+fi28
IdUwr5UtgpQemyZYmhR01sta8Ap54P6nEsqKHLPyPNbtC11
mVPSL1Y0XB9+7klgb
f37X
=YcmH
-----END PGP MESSAGE-----

Wenn an anderer Stelle in diesem Buch von Metadaten die Rede ist, schließt das übrigens ausdrücklich Informationen aus dem E-Mail-Header mit ein. Weil der Header wichtige Steuerinformationen für die Zustellung der E-Mail enthält, kann er nach dem aktuellen Stand der Technik leider auch nicht Ende zu Ende verschlüsselt werden. Wie Sie im obigen Beispiel einer mit PGP verschlüsselten E-Mail sehen, muss der Header stets für die an der Zustellung beteiligten Server und Dienste lesbar bleiben.

4.1.4. E-Mails senden und empfangen

Mit der Vernetzung von immer mehr Großrechnern und durch die Öffnung des Internets für private Zwecke wuchsen auch die Ansprüche an E-Mail rapide. So wurde aus dem zunächst lokal sehr begrenzten Kommunikationssystem ein globaler Dienst mit Millionen von Nutzern. Der Großteil dieser Anwender bestand nun nicht mehr aus Technikern und Wissenschaftlern, die sich den persönlichen Zugriff auf einen ständig mit dem Internet verbundenen Großrechner teilten. Vielmehr gab es nun viele Nutzer, die jeweils ihren eigenen Computer besaßen. Die meisten dieser Computer waren keineswegs ständig online. Dies stand aber der Nutzung und Verbreitung von E-Mail nicht im Weg, da es sich um eine *asynchrone* Art der Kommunikation[1] handelt.

Um zu verstehen, wo die Sicherheitsprobleme liegen, die E-Mail mit sich bringt, sollten Sie sich zunächst anschauen, wie Versand und Empfang einer solchen Nachricht konkret funktionieren. Was passiert, wenn Alice Bob eine E-Mail schicken möchte, um sich in der kommenden Woche mit ihm zum Mittagessen zu verabreden?

Alices E-Mail-Adresse lautet alice@cryptocheck.de. Bob hingegen nennt die Adresse bob@cryptocheck.de sein Eigen. Die Hostteile beider E-Mail-Adressen sind also identisch. Das bedeutet vereinfacht, dass für Versand und Empfang der Nachricht derselbe E-Mail-Server zuständig ist.

Um die E-Mail an Bob zu verfassen, verwendet Alice einen E-Mail-Client. Dies kann sowohl ein sogenannter Desktop-Client (zum Beispiel Mozilla Thunderbird oder Apple Mail) oder auch eine vergleichbare webbasierte Anwendung sein (mehr zu E-Mail-Clients weiter unten in diesem Kapitel). Sobald Alice nun mit dem Schreiben der Nachricht fertig ist, löst sie mit einem Klick den Sendevorgang aus. Daraufhin versucht ihr Client, den für Alices Account hinterlegten Mailserver smtp.cryptocheck.de zu erreichen. Vorher muss allerdings der Hostname des Servers in eine IP-Adresse übersetzt werden (siehe Kasten DNS).

Hinweis

Das Domain Name System – DNS

Jeder Computer im Internet wird anhand einer sogenannten IP-Adresse identifiziert. Bisher (nach IP Version 4) war dies eine Kombination aus vier maximal vierstelligen Dezimalzahlen, beispielsweise 89.146.220.134. Nach dem zukünftigen Standard IPv6 besteht eine IP-Adresse aus acht hexadezimalen Zahlen, beispielsweise FEBC:A574:382B:23C1:AA49:4592:4EFE:9982.

IP-Adressen sind von ihrer Natur her mit Postanschriften oder Telefonnummern vergleichbar. Weil Menschen sich diese nur schwer (oder im Fall von IPv6 nahezu unmöglich) merken können, kann jeder IP-Adresse ein menschenlesbarer Name, eine sogenannte Domain zugeordnet werden – zum Beispiel www.heise.de, www.google.com oder www.cryptocheck.de. Eine Reihe sogenannter DNS-Server, die im Grunde genommen nichts anderes als große Adress- oder Telefonbücher sind, halten Verzeichnisse mit der Zuordnung von IP-Adresse zu Domainname bereit. Wenn Sie also www.heise.de in die Adresszeile Ihres Browsers eingeben, fragt dieser sofort beim zuständigen DNS-Server nach der IP-Adresse, die sich hinter diesem Namen verbirgt. DNS kann aber noch mehr. Beispielsweise kann im Falle von E-Mail ein sogenannter Mail Transfer Agent (MTA) – im Wesentlichen ein Serverdienst zur Verteilung von E-Mail-Nachrichten – direkt bei einem DNS-Server die Adresse des für die Zustellung von E-Mails verantwortlichen Computers einer Domain erfragen.

Daraufhin verbindet sich der E-Mail-Client mit dem unter der IP-Adresse erreichbaren Mailserver. Die Kommunikation zwischen Server und Client erfolgt hierbei über das sogenannte *Simple Mail Transfer Protocol* (SMTP). Der Dienst, der auf Seiten des Mailservers die Verbindung annimmt und sich um die weitere Verarbeitung der Nachricht kümmert, wird auch als Mail Transfer Agent (MTA) bezeichnet. Der MTA überprüft nun anhand der Zieladresse der E-Mail, ob er selbst für deren Zustellung verantwortlich ist. Hier existieren nun zwei Möglichkeiten.

In unserem oben beschriebenen Fall ist der Dienst tatsächlich für E-Mail-Adressen mit der Domain cryptocheck.de zuständig. Daher muss er nichts weiter tun, als diese an den sogenannten Mail Delivery Agent (MDA) zu übergeben. Dieser zusätzliche Dienst kümmert sich um die Verwaltung der einzelnen E-Mail-Postfächer und legt die an Bob adressierte Nachricht in dessen virtuellem Posteingang (auch als Inbox bezeichnet) ab.

Wenn Alice nicht Bob eine E-Mail schickt, sondern beispielsweise dem Internet-Orakel[2], das die E-Mail-Adresse orakel@olymp.org hat, dann ist Alices MTA nicht für diese Nachricht zuständig (da der Host olymp.org lautet, nicht cryptocheck.de). Er versucht stattdessen, die E-Mail an den verantwortlichen Mailserver weiterzuleiten. Dazu fragt er bei einem ihm bekannten DNS-Dienst die IP-Adresse des zuständigen Mailservers (den sogenannten MX-Record) für olymp.org an. Existiert ein solcher Eintrag, kontaktiert er wiederum über das SMTP-Protokoll den entsprechenden Dienst und reicht die Nachricht an diesen weiter. Da aber nicht immer nur

zwei Mailserver an der Verarbeitung einer E-Mail beteiligt sein müssen, sondern es nahezu beliebig viele sein können, wiederholt sich dieser Vorgang so lange, bis die E-Mail in einem passenden Postfach angekommen ist. Kann eine E-Mail aus irgendwelchen Gründen nicht zugestellt werden, wird sie abgewiesen (im Jargon nennt man sowas auch bouncen, von englisch »to bounce« = zurückprallen) und der Absender wird darüber im Normalfall benachrichtigt.

Wollen Bob oder das Internet-Orakel nun die E-Mail lesen, die Alice ihnen geschickt hat, benutzen sie dazu ebenfalls ihren Mailclient. Genau wie beim Versenden einer E-Mail wird zunächst die Adresse des Posteingangsservers aufgelöst. In diesem Beispiel sind das mail.cryptocheck.de beziehungsweise imap.gmail.com (olymp.org verwendet aktuell anscheinend Google Mail). Zum Auflisten und Abrufen von E-Mail-Nachrichten haben Bob und das Orakel zwei Alternativen: *POP3* (Post Office Protocol Version 3) ist eigentlich ein Relikt aus vergangenen Tagen, wird aber immer noch von vielen E-Mail-Providern und -Clients unterstützt. *IMAP4* (Internet Message Access Protocol Version 4) ist ein wenig jünger und kann mehr als POP3. Beispielsweise werden Nachrichten erst vollständig heruntergeladen, wenn Sie sie zum Lesen auswählen. Zudem wird der Status einer E-Mail auf dem Server gespeichert. Das heißt, wenn Sie eine Nachricht auf Ihrem Smartphone als gelesen markiert haben, wird Ihnen dieselbe Nachricht auch auf Ihrem Computer als gelesen angezeigt werden.

In den meisten Fällen verstehen die Posteingangsserver beide Protokolle. Vor allem, wenn Sie von mehreren Geräten aus Ihre Nachrichten lesen möchten (und das trifft im Zeitalter von Zweit- und Drittlaptops und Smartphones auf fast jeden zu), ist die Nutzung von IMAP sinnvoll, da hier die Nachrichten auf dem Server verbleiben und auch dort als gelesen markiert werden.

Antworten nun Bob und das Orakel auf Alices E-Mails, läuft das Ganze von vorn ab, nur in umgekehrter Richtung.

4.1.5. Sicher e-mailen

Aus den Ursprüngen der E-Mail, die ja als informelles Kommunikationsmittel für einen kleinen Kreis von Wissenschaftlern und Tüftlern geschaffen wurde, folgt, dass die gesamte E-Mail-Infrastruktur gar nicht dazu geschaffen wurde, um vertraulich zu kommunizieren! Alle Maßnahmen, die E-Mail sicherer zu machen, sind nachträgliche Ergänzungen. Häufig werden E-Mails mit Postkarten verglichen, die zwischen Absender und Empfänger von jedem gelesen

werden können, der die Nachricht in die Hände bekommt. Bei der Nutzung von E-Mail bestehen daher folgende grundsätzliche Herausforderungen:

Reine SMTP-, POP3-, oder IMAP-Verbindungen sind, ohne dass weitere Maßnahmen ergriffen werden, *nicht verschlüsselt*! Jegliche Kommunikation über diese Protokolle kann unter Verwendung einfachster Methoden mitgelesen werden. Das schließt übrigens die Authentifizierung, also die Übertragung Ihrer Zugangsdaten zur Anmeldung an Posteingangs- oder Postausgangsserver, explizit mit ein.

SMTP-, POP3-, oder IMAP4-Verbindungen lassen sich mittels TLS (siehe Kasten TLS im Kapitel 3) schützen. Die über eine solche Transportverschlüsselunggesicherte Verbindung besteht aber nur zwischen Ihrem Client und dem Mailserver Ihres Anbieters. Leitet dieser die Nachricht an einen anderen Server weiter, können Sie weder feststellen noch erzwingen, dass die weitergehende Verbindung ebenfalls mittels TLS geschützt wird. Im Zweifel ist sie eben nicht geschützt, womit wir wieder beim vorherigen Punkt angelangt wären.

Viele Mailserver überprüfen bei einer SMTP-Verbindung die Angabe der Absenderadresse einer Nachricht nicht. Wenn Sie Zugang zu einem solchen Mailserver haben, können Sie E-Mails unter Angabe eines falschen Absenders verschicken und sich sogar als eine andere Person oder Institution ausgeben. Dieses Problem wird gerne von Spammern und Phishing-Betrügern (siehe Kapitel 1 und Einleitung dieses Kapitels) ausgenutzt.

Die meisten Mailserver und Clients unterstützen mittlerweile die Transportverschlüsselung mittels TLS. Allerdings gibt es an dieser Stelle ein Problem: Sie bekommen es nicht zwangsläufig mit, wenn *kein* TLS verwendet wird, weil entweder Client oder Server »kein TLS sprechen«. Im Zweifelsfall müssen Sie sich beim Anbieter selbst schlaumachen, ob er TLS verwendet. Beispielsweise haben Anfang 2014 mehrere große deutsche Mailprovider erklärt, nur noch E-Mails mit TLS zulassen zu wollen.

Die bisher besprochenen Schwächen der E-Mail-Infrastruktur kann ein Angreifer, also Eve, einzeln oder in Kombination mit anderen Techniken ausnutzen. Wir wollen die Transportkette dabei einmal von vorn bis hinten durchgehen:

- Wenn Eve persönlich vor Ort ist, kann sie Alice beim Schreiben der E-Mail (oder dem Empfänger beim Lesen der E-Mail) über die Schulter schauen.
- Hat Eve physikalischen oder anderen Zugriff auf eines der beteiligten Computersysteme (PC des Absenders, PC des Empfängers, einen der beteiligten

Mailserver), ist sie unter Umständen in der Lage, die E-Mails direkt an ihrem Speicherort (Posteingang, Entwurfsordner, Gesendete Nachrichten) zu lesen.

- Wenn Eve Zugriff auf eine der Netzwerkkomponenten hat, die zwischen Alices Computer, den Mailservern und dem Computer des Empfängers liegen (also zum Beispiel Router, Switches, Firewalls), kann sie die gesamte Datenverbindung abhören. Ist diese nicht verschlüsselt, kann sie nicht nur ausgetauschte E-Mail-Nachrichten mitlesen, sondern unter Umständen auch die Zugangsdaten zu Alices E-Mail-Postfach. Diese kann sie wiederum benutzen, um sich in Alices E-Mail-Postfach anzumelden und die dort liegenden Kopien aller gesendeten und empfangenen E-Mails zu lesen.

Welche Maßnahmen können Alice und ihre Verbündeten nun ergreifen, um es der allzu neugierigen Eve schwer zu machen, ihre Nachrichten mitzulesen?

Auf Shoulder Surfing und Co. sind wir im letzten Abschnitt des zweiten Kapitels eingegangen – sie sind nicht spezifisch für E-Mail, stellen aber trotzdem eine nicht zu unterschätzende Sicherheitslücke dar.

Gegen das unbefugte Lesen von E-Mails direkt auf den beteiligten Systemen selbst hilft Ihnen eine verlässliche *Ende-zu-Ende-Verschlüsselung*. Diese ist auch gegen das Auslesen von E-Mails auf dem Transportweg wirksam und lässt sich mittels bewährter Verfahren wie PGP oder S/MIME realisieren. Hierbei sollte darauf geachtet werden, dass E-Mails auch bereits im Entwurfsstadium verschlüsselt werden. Wenn Sie noch keine derartige Verschlüsselung verwenden (weil zum Beispiel Ihre Gesprächspartner nicht verschlüsseln), kann zumindest Ihr E-Mail-Eingang weniger verwundbar gestaltet werden, indem Sie eine sogenannte *Eingangsverschlüsselung* verwenden. Das bedeutet, dass E-Mails zwar unverschlüsselt bei Ihnen ankommen, also theoretisch von einem Angreifer auf dem gesamten Weg abgefangen werden können. Sobald sie in Ihrem Posteingang sind, werden sie aber verschlüsselt gespeichert, sodass zumindest jemand, der in Ihren Posteingang eindringt, Ihre Korrespondenz nicht lesen kann. Eingangsverschlüsselung lässt sich beispielsweise unter Thunderbird mit dem Plug-in Enigmail realisieren, auf das wir in einem der folgenden Abschnitte eingehen. Der E-Mail-Provider Posteo[3] bietet Eingangsverschlüsselung auch ohne Installation eines Plug-ins (siehe weiter unten in diesem Kapitel).

Gegen das Abgreifen Ihrer Log-in-Daten können Sie sich schützen, indem Sie bei der Anmeldung an den Mailserver die *Transportverschlüsselung* TLS verwenden. Einige Mailclients unterstützen sogar das Erzwingen von TLS-geschützten Verbindungen. Kann keine gesicherte Verbindung zum Server aufgebaut werden, wird der anschließende Aufbau einer ungesicherten Verbindung (was oft das Standardverhalten darstellt) unterbunden. So können Sie zwar temporär nicht Ihre E-Mails lesen, aber Sie laufen auch nicht Gefahr, einem Lauscher unbemerkt Ihr Passwort preiszugeben. Da auch etablierte Zertifizierungsstellen, die im Zusammenhang mit TLS verwendet werden, nicht immer vertrauenswürdig sind beziehungsweise wahrheitsgemäße Informationen liefern, wurde ein zweiter Mechanismus namens DANE geschaffen, der dieses System ergänzen soll. DANE nutzt den Standard DNSSEC, der bisher leider ebenfalls nicht sehr weit verbreitet ist. Bei DNSSEC werden im DNS-Eintrag eines Servers auch Informationen über die Echtheit seines Zertifikats gespeichert und digital signiert (zu DNS siehe Kasten). Bisher wird unter deutschen E-Mail-Providern DANE nur von Posteo angeboten. TLS kann übrigens auch beim Transfer von E-Mail-Nachrichten zwischen den verschiedenen Mailservern genutzt werden. Als Anwender haben Sie allerdings keinen Einfluss darauf, ob das tatsächlich geschieht. Aus diesen Gründen sollten Sie sich, wenn Sie wirklich Wert auf Vertraulichkeit legen, nicht ausschließlich auf TLS verlassen, sondern zusätzlich immer auch eine Ende-zu-Ende-Verschlüsselung wie PGP oder S/MIME verwenden.

4.2 Outlook, Thunderbird, OSX Mail & Co. – der E-Mail-Client

Es gibt zwei Arten von E-Mail-Programmen, auch Clients genannt: solche, die auf Ihrem persönlichen Computer installiert sind, also *Desktop-Clients*, und sogenannte *Webclients*. Letztere sind nichts anderes als intelligentere Webseiten, also Webanwendungen, die wie Desktop-Clients in der Lage sind, mit einem Mailserver zu kommunizieren.

Einige weit verbreitete Desktop-Clients mit grafischer Benutzeroberfläche:

- Apple Mail
- Mozilla Thunderbird
- Claws Mail
- Eudora
- Microsoft Outlook

- Pegasus Mail
- Evolution

Für eingefleischte Fans der Kommandozeile gibt es auch Mailclients, die keine grafische Benutzeroberfläche haben, beispielsweise:

- Mutt

Neben Google Mail, GMX, Web.de und vielen anderen gibt es auch Webclients, die Sie (als ziemlich fortgeschrittener Benutzer) auf Ihrem eigenen Webspace installieren und Ihren Bedürfnissen anpassen können:

- Roundcube
- Zarafa
- Horde
- AfterLogic WebMail Lite

Das wichtigste Merkmal eines Desktop-Clients ist, dass er vollständig Ihrer Kontrolle unterliegt. Das heißt im Detail:

Nachrichten können vollständig vom Server heruntergeladen und dort gelöscht werden, wenn Sie das wünschen. Wenn Sie Mails verschlüsseln, sind diese also auch dann für Fremde nicht lesbar, wenn der Computer in falsche Hände geraten sollte. Unfertig gespeicherte E-Mails, sogenannte Entwürfe, können ebenfalls mit einer Verschlüsselung versehen werden.

Zudem haben Sie die Freiheit, sogenannte Add-ons zu installieren, also Zusatzfunktionen, die den eigentlichen Client ergänzen. Mithilfe eines solchen Add-ons können Sie Ihre Mails mittels OpenPGP verschlüsseln (siehe Enigmail weiter unten in diesem Kapitel) – aber es gibt auch andere nützliche (und weniger nützliche) Erweiterungen, die Ihren E-Mail-Client beispielsweise mit umfangreichen Kalenderfunktionen versehen, das Design ändern, Rechtschreibung und Grammatik Ihrer E-Mails überprüfen, die Synchronisierung Ihres Adressbuches mit einem Verzeichnisdienst ermöglichen und so weiter.

Welche Add-ons für einen Client zur Verfügung stehen, ist davon abhängig, wie produktiv und erfindungsreich dessen Entwickler sind (im Falle von kommerzieller Software), beziehungsweise davon, ob der Client eine aktive Gemeinde von Open-Source-Entwicklern hat.

Ein guter und brauchbarer Open-Source-Client ist Thunderbird von der Mozilla Foundation. Mozilla ist neben Thunderbird auch für den weit verbreiteten Webbrowser Firefox verantwortlich – die grafischen Benutzeroberflächen sehen sich daher recht ähnlich.

Auch Claws Mail ist ein Open-Source-Client, der beispielsweise in das sichere Linux-basierte Betriebssystem Tails (Abbildung 4.1; siehe auch Kapitel 6) schon integriert ist. Claws Mail bringt von vornherein die Fähigkeit zur Verschlüsselung mittels GPG mit.

Abb. 4.1 Screenshot des sicheren Betriebssystems Tails

4.3 GMail, GMX, WEB.DE & Co. – Vor- und Nachteile webbasierter Clients

Der große Vorteil von webbasierten Clients ist der, dass Sie von jedem Rechner aus Zugang auf Ihre Mails erhalten können – beispielsweise auch, wenn Sie ohne Laptop verreist sind (oder Ihr Hotel kein WLAN hat) und Sie deswegen ein Internetcafé in Istanbul, Buenos Aires oder Neuruppin aufsuchen müssen.

Sicheres, also verschlüsseltes, E-Mailen ist von einem Webclient aus jedoch schwieriger zu realisieren, in manchen Fällen auch unmöglich. Man muss dabei zwei Situationen unterscheiden:

1. Sie loggen sich von Ihrem *persönlichen Computer* aus in einen Webclient ein.

2. Sie verwenden einen Webclient von einem *öffentlichen Computer* aus, zum Beispiel aus dem oben erwähnten Internetcafé.

Wie Sie sich aus den vorangegangenen Kapiteln erinnern, benötigen Sie zum verschlüsselten Mailen (jedenfalls zum Lesen verschlüsselter E-Mails, die an Sie gerichtet sind) einen privaten Schlüssel, der auf keinen Fall in die Hände eines Dritten gelangen darf – auch nicht in die Ihres E-Mail-Providers! Der einzig richtige Aufbewahrungsort für einen privaten Schlüssel ist ein Medium, auf das nur Sie Zugriff haben: ein USB-Stick, den Sie in der Tasche tragen, oder die Festplatte eines Laptops, den Sie nicht aus den Händen geben. Sie sollten Ihren privaten Schlüssel keinesfalls auf den Server Ihres E-Mail-Providers hochladen. Auch, wenn Sie ihm vertrauen (wovon wir abraten), besteht dort immer noch die Möglichkeit des unberechtigten Zugriffs durch Angreifer, die es auf die Kundendaten Ihres Providers abgesehen haben. Die Möglichkeit, dass Sie im Webmailclient eine E-Mail verfassen, die dann auf dem Server des Providers mit Ihrem privaten Schlüssel verschlüsselt und auf dem privaten Rechner (oder analog dazu beim E-Mail-Provider) des Empfängers entschlüsselt wird, fällt also schon einmal aus. Die Verschlüsselung muss auf einem Computer erfolgen, über den Sie allein die Kontrolle haben.

Das bedeutet leider, dass von einem öffentlichen Rechner aus keine sichere Public-Key-Verschlüsselung erfolgen kann – jedenfalls solange Sie mit dem Betriebssystem und auf der Festplatte dieses Computers arbeiten. Theoretisch wäre es zwar möglich, verschlüsselte Mails zu verschicken, da der Provider dazu nur den öffentlichen Schlüssel des Empfängers kennen muss – er würde aber gleichzeitig in den Besitz des Klartextes gelangen, was eine ganze Reihe von Angriffsmöglichkeiten öffnet. Das Lesen von verschlüsselten E-Mails auf dem Server eines E-Mail-Providers ist noch weniger erstrebenswert – der Provider würde nicht nur in den Besitz des Klartextes kommen, sondern auch in den Ihres privaten Schlüssels!

Es gibt jedoch einen Weg, um sichere Kommunikation auch von öffentlichen Rechnern aus zu ermöglichen – das Betriebssystem Tails, das Sie von einem USB-Stick aus ausführen können und das das Betriebssystem und die Datenträger des Gastrechners vollständig übergeht. Auf Tails gehen wir in Kapitel 6 näher ein. Falls Sie jedoch nicht Tails (oder ein ähnliches System, das möglicherweise in der Zukunft, nach Erscheinen dieses Buches, entwickelt wird) benutzen, merken Sie sich einfach:

Jegliche Kommunikation von einem öffentlichen Rechner aus muss als unsicher betrachtet werden.

Und wenn Sie einen Webclient von Ihrem persönlichen Laptop aus verwenden? Als Ersatz für einen E-Mail-Client mit Verschlüsselungs-Add-on können Sie eine ähnliche Erweiterung für Ihren Browser installieren. Empfehlenswert ist Mailvelope[4] (für Firefox und Chrome), das Ihnen die Benutzung von PGP mit Ihrem Webmailzugang gestattet. Mailvelope ist ebenfalls Open Source.

Da viele Webmailanbieter Ihre E-Mails während der Erstellung zwischenspeichern (damit Sie den bereits geschriebenen Text nicht verlieren, wenn Sie aus Versehen das Browserfenster schließen oder der Browser abstürzt), kann es jedoch trotz Benutzung von Mailvelope passieren, dass der Provider Ihre Mail im Klartext speichert. Mailvelope ist somit unsicherer als ein dezidierter E-Mail-Client mit PGP-Plug-in.

Wenn Sie bereits PGP-Software installiert haben, jedoch aus diesem oder anderen Gründen kein Browser-Plug-in wie Mailvelope benutzen wollen oder können, gibt es dafür einen Umweg:

Bei dem Verschlüsselungsverfahren, das hinter PGP steckt, handelt es sich eigentlich nicht um etwas, mit dem explizit nur E-Mail-Nachrichten verschlüsselt werden können. Sie können vielmehr jede Textdatei und auch andere Daten mit einem öffentlichen Key ver- und dem passenden privaten Key wieder entschlüsseln. Das kann beispielsweise nützlich sein, um eine codierte Textdatei auf einer ansonsten ungeschützten Festplatte abzulegen. Zum Beispiel, wenn Sie auf Ihrem Laptop hauptsächlich Kochrezepte verwalten und sich deswegen nicht die Mühe einer Festplattenverschlüsselung machen, aber ausnahmsweise mal eine Sicherheitskopie der Steuererklärung ablegen wollen.

Um Benutzern die Möglichkeit zu geben, einzelne Dateien mittels PGP zu chiffrieren, bieten die Programme, die PGP umsetzen, genau diese Möglichkeit, auch ohne Verwendung von E-Mail. Wie konkret das funktioniert, erfahren Sie im Handbuch des jeweiligen Programms. Die Grundlagen der asymmetrischen Verschlüsselung haben Sie ja bereits in Kapitel 1 und 2 kennengelernt, daher erklären wir hier nur kurz das Prinzip:

Wenn Sie mittels eines Webmailclients eine verschlüsselte Mail verschicken wollen, speichern Sie den Klartext der Mail zunächst auf Ihrem Computer und verschlüsseln sie (mit dem öffentlichen Key des Empfängers) auf der Festplatte mit PGP. Sie erhalten dann eine Textdatei

mit dem verschlüsselten Text. Diesen können Sie mit Copy & Paste nun einfach in das Textfeld Ihres Webmailclients einfügen. Wenn Sie umgekehrt eine verschlüsselte E-Mail erhalten haben, können Sie diese als Textdatei auf Ihrem Rechner abspeichern und von Hand mithilfe Ihres privaten Schlüssels lesbar machen.

Ihr E-Mail-Provider gelangt auf diesem Weg zu keinem Zeitpunkt in den Besitz des Klartexts und/oder Ihres privaten Schlüssels.

Was wir bisher besprochen haben, ist die sogenannte Ende-zu-Ende-Verschlüsselung. Ende zu Ende bedeutet, dass die E-Mail von dem Zeitpunkt an, zu dem Sie sie auf Ihrem Computer verfassen, bis zu dem Moment, in dem der Empfänger sie lesen möchte, stets verschlüsselt bleibt. Nur so ist zuverlässige Geheimhaltung möglich.

Alternativ zur Ende-zu-Ende-Verschlüsselung oder im Kontrast dazu dem völlig unverschlüsselten E-Mail-Versand gibt es aber noch ein paar Zwischenlösungen, die den E-Mail-Versand etwas sicherer machen, aber keine vollständige Vertraulichkeit bieten. Wenn Webmailanbieter mit »Verschlüsselung« werben, handelt es sich normalerweise um genau solche Zwischenlösungen, da Ende-zu-Ende-Verschlüsselung in Ihrer Hand (und der des Empfängers) liegt und nicht durch Ihren E-Mail-Provider realisiert werden kann.

Der deutsche Anbieter Posteo[5] verschlüsselt beispielsweise die Festplatten seiner Server (Stand Juli 2015), sodass Nutzerdaten nicht von Dritten gelesen werden können, wenn Datenträger abhanden kommen (beispielsweise gestohlen oder beschlagnahmt werden). Zudem besteht die Möglichkeit, das eigene Adressbuch und den Kalender mit dem Algorithmus AES (der zurzeit noch als sehr sicher gilt) zu verschlüsseln – die Daten liegen somit sehr viel sicherer in der Datenbank von Posteo als beispielsweise bei Google, da sie auch von Mitarbeitern des Providers nicht gelesen werden können. Eingangsverschlüsselung von E-Mails ist ein weiteres begrüßenswertes Feature bei Posteo (siehe erster Abschnitt dieses Kapitels). Auf den Webseiten des Anbieters findet sich außerdem eine auch für Laien gut lesbare Einführung[6] in die Nutzung von PGP und S/MIME. Posteo ist nicht werbefinanziert und erhebt daher von Benutzern eine Gebühr von einem Euro/Monat, die, was ebenfalls recht ungewöhnlich ist, auch anonym durch Einsendung von Bargeld bezahlt werden kann.

4.4 De-Mail – sicher per Gesetz?

Vor einigen Jahren hat auch die deutsche Bundesregierung beschlossen, dass »sichere, vertrauliche und nachweisbare Kommunikation im Internet« eine erstrebenswerte Sache ist, und hat daraufhin im Jahr 2011 das *De-Mail-Gesetz* erlassen. Ziel des Gesetzes ist es, Bürgern zu ermöglichen, mit den Behörden elektronisch statt per Brief zu kommunizieren. Die Bundesregierung hat richtig erkannt, dass unverschlüsselte E-Mails dazu nicht geeignet sind, weil weder die Vertraulichkeit noch die Identität von Absender und Empfänger nachweisbar sind.

Zu diesem Zweck wurde dann De-Mail geschaffen, ein System, das mit der herkömmlichen E-Mail nicht kompatibel ist.

Der Transport von Nachrichten per De-Mail wird mittels TLS abgesichert. Das heißt, dass der Versand der Mail zwischen dem Mailserver des Absenders und dem Mailserver des Empfängers verschlüsselt erfolgt – eine Vorgehensweise, die mittlerweile auch schon bei vielen E-Mail-Providern Standard ist.

Zusätzlich ist bei De-Mail eine Authentifizierung des Absenders und Empfängers vorgesehen. Aus diesem Grund muss man sich zum Eröffnen eines De-Mail-Kontos einer Registrierung mit eindeutiger Identifizierung unterziehen, beispielsweise mit dem Personalausweis.

Des Weiteren wird die Nachricht mittels eines asymmetrischen Verfahrens verschlüsselt und signiert. Damit sollen Vertraulichkeit und Integrität sichergestellt werden. Hier kann allerdings zunächst nicht von einer Ende-zu-Ende-Verschlüsselung gesprochen werden, da die Chiffrierung erst auf den Servern des Anbieters erfolgt und sich der entsprechende private Schlüssel im Besitz des Dienstanbieters befindet. Theoretisch wäre damit ein Angreifer in der Lage, eine rechtsgültige Nachricht an eine Behörde zu schicken – zum Beispiel eine Selbstanzeige. In diesem Fall hätte der Benutzer große Schwierigkeiten zu beweisen, dass er nicht der Urheber der Nachricht ist.

De-Mail wird nicht von einer staatlichen Behörde angeboten, sondern von Unternehmen, die sich verpflichten, die De-Mail-Richtlinien umzusetzen, und dafür vom BSI zertifiziert werden. Das BSI kontrolliert bei zertifizierten De-Mail-Providern auch die Sicherheit der eingesetzten Software.

Ursprünglich war eine Ende-zu-Ende-Verschlüsselung bei De-Mail nicht vorgesehen, aus zwei Gründen:

- Sicherheitsbehörden behielten sich vor, sich bei Verdacht auf eine Straftat (oder sogar nur auf eine Ordnungswidrigkeit) Zugang zum De-Mail-Postfach einer Person zu verschaffen. Eine Maßnahme, die bei einer Ende-zu-Ende-Verschlüsselung sinnlos wäre, da die dort gespeicherten E-Mails ohne Kenntnis des privaten Schlüssels des Postfachbesitzers nicht lesbar sind.
- Es sollte eine Prüfung auf Viren oder Malware stattfinden, die bei Ende-zu-Ende-verschlüsselten Nachrichten nicht möglich wäre.

Dennoch wird seit April 2015 auf PGP basierende Ende-zu-Ende-Verschlüsselung von De-Mail unterstützt. Nutzbar ist dieses Feature zunächst nur für Benutzer von Firefox und Chrome. Diese können hierzu ein spezielles Add-on installieren, das auf Mailvelope (siehe oben) basiert. Die besagte De-Mail-Erweiterung soll sogar Open Source sein, um den Verdacht zu entkräften, dass weiterhin Hintertürchen für ein Mitlesen der Mails durch die Behörden offengehalten werden.

Dass ursprünglich keine Ende-zu-Ende-Verschlüsselung möglich war, wurde seit der Einführung von De-Mail von Datenschutzorganisationen, beispielsweise dem CCC, kritisiert. Das Bundesinnenministerium antwortete darauf aber noch im Jahr 2013, dass OpenPGP und verwandte Software »komplizierte Speziallösungen« seien, »die für Hacker und versierte IT-Spezialisten verwendbar sind, kaum aber für technisch normal begabte Internetnutzerinnen und -nutzer« (Meldung der dpa vom 20.3.2013). Dass das nicht stimmt, haben Sie bei der Lektüre dieses Buchs bestimmt schon gemerkt – und mittlerweile scheint sich die Einsicht auch im Innenministerium durchgesetzt zu haben.

Im gleichen Atemzug wie De-Mail wird oft die Initiative »E-Mail made in Germany« genannt. Diese wird von mehreren großen E-Mail-Anbietern getragen, unter anderem T-Online, GMX und Web.de, und verspricht höhere E-Mail-Sicherheit durch

- Verschlüsselung der E-Mail-Übertragung zwischen den genannten Anbietern mittels TLS und
- ausschließliche Nutzung von Servern, die auf deutschem Boden stehen.

Die Absichten dahinter mögen gut sein, aber sicherer als »herkömmliche« E-Mail wird »E-Mail made in Germany« dadurch kaum, denn

- immer mehr Anbieter gehen ohnehin dazu über, Transportverschlüsselung mittels TLS umzusetzen, und
- durch einen Standort in Deutschland ist keineswegs sichergestellt, dass E-Mails nicht doch auf ihrem Weg von einem deutschen zu einem anderen deutschen Mailserver durch das Ausland geroutet und dort abgegriffen werden.

Außerdem: Ob E-Mails auf deutschen Servern sicherer sind als auf ausländischen Servern, hängt stark von der deutschen Gesetzgebung ab, die sich in diesem Falle jederzeit ändern kann. Durch die angegebenen Verfahren werden E-Mails also weder sicherer noch zuverlässiger als vorher. »E-Mail made in Germany« ist folglich nichts weiter als eine Marketingkampagne.

4.5 »Ziemlich einfache« Verschlüsselung mit PEP

PEP steht für Pretty Easy Privacy, also »ziemlich einfache Geheimhaltung« – eine Anspielung auf PGP (Pretty Good Privacy), übersetzt »ziemlich gute Geheimhaltung«. PEP wurde erstmals 2014 von Mitgliedern des Chaos Computer Club der Schweiz vorgestellt. Es hat zum Ziel, Kryptografie auch für Laien und Nicht-Computerinteressierte einfach benutzbar zu machen, und zwar unter Windows, Linux und diversen anderen Betriebssystemen, auch auf Smartphones. PEP ist ein Plug-in, das nach Aktivierung prüft, ob ein PGP-Programm installiert ist (beispielsweise Gpg4win unter Windows oder GnuPG unter Linux). Aktuell (Stand Juli 2015) gibt es von PEP lediglich eine eingeschränkte Version (genannt Preview), die mit GPG und Windows Outlook funktioniert, und für mehrere vollwertige Versionen laufen Beta-Tests. Man sollte die Software also im Auge behalten[7].

4.6 Vertrauensbasis gemeinsame Freunde – PGP und GPG nutzen

PGP ist neben S/MIME eines von zwei Verfahren zur Ende-zu-Ende-Verschlüsselung, die wir Ihnen in diesem Buch vorstellen möchten. Das Kürzel PGP steht für *Pretty Good Privacy* (englisch für »ziemlich gute Geheimhaltung«) und wurde in seiner Urform schon 1991 von dem Informatiker und Symantec-Mitarbeiter Phil Zimmermann entwickelt.

4.6.1. Was sind PGP und GPG?

PGP ist eine Form der *Public-Key-Kryptografie*. Dieses Prinzip haben Sie in Kapitel 2 schon kennengelernt: Es ermöglicht, dass jeder Ihnen eine verschlüsselte Mail schicken kann, der Ihren öffentlichen Schlüssel besitzt, aber niemand außer Ihnen diese Mail entschlüsseln kann, weil dazu Ihr geheimer privater Schlüssel notwendig ist.

Auf technischer Ebene sieht das Ganze so aus, dass für die Verschlüsselung der E-Mail ein einmaliger Schlüssel vereinbart wird, anhand dessen die symmetrische Verschlüsselung der E-Mail erfolgt. Damit sowohl Absender als auch Empfänger den symmetrischen Schlüssel haben, wird dieser asymmetrisch verschlüsselt, also mit dem öffentlichen Schlüssel des Empfängers, der ihn wiederum mit seinem privaten Schlüssel wieder entschlüsseln kann. In Kapitel 2 haben Sie dieses Verfahren als *hybride Verschlüsselung*kennengelernt.

PGP bedient sich eines *Web of Trust*. Kurz zur Erinnerung: Der erste Schritt in der Entstehung eines Web of Trust ist, wenn Leute, die sich persönlich kennen, sich gegenseitig ihr Vertrauen aussprechen. Im Zusammenhang von PGP bedeutet das, dass sie gegenseitig ihre öffentlichen Schlüssel signieren und damit mit ihrem eigenen »guten Namen« dafür einstehen, dass der Besitzer des Schlüssels der ist, der er vorgibt zu sein. Wenn genügend Leute, denen Sie vertrauen, einer dritten Person vertrauen, so können Sie zuversichtlich sein, dass diese dritte Person die ist, die sie vorgibt zu sein, auch wenn Sie sie nicht persönlich kennen. Je enger das Web of Trust geknüpft ist, desto zuverlässiger lässt es sich auch für Bekanntschaften dritten oder vierten Grades benutzen.

Um PGP zu vermarkten, entstand die PGP Corporation, eine Firma, die PGP als Freeware zur Verfügung stellte. 1997 wurde die PGP Corporation und damit der PGP-Standard von der Firma McAfee (bekannt für die gleichnamige Antivirensoftware) übernommen. McAfee hielt den Quellcode von PGP nun unter Verschluss, sodass PGP nicht mehr Open Source war. Außerdem wurde ein Hintertürchen in den Algorithmus eingebaut, der es auch einem Dritten ermöglichen sollte, mit PGP verschlüsselte E-Mails zu entschlüsseln, einen sogenannten Additional Decryption Key. Beides, die Geheimhaltung des Quellcodes und die mögliche Entschlüsselung der Kommunikation durch Dritte, widersprach fundamental den Absichten, die Phil Zimmermann und die mittlerweile gewachsene PGP-Gemeinde ursprünglich hatten. Aus diesem Grund wurde kurz nach Übernahme von PGP der alternative Standard *OpenPGP* mit frei zugänglichem Quelltext geschaffen.

Die heute immer noch verwendete Software *GnuPG* (oder kurz *GPG*) war die erste Implementierung des OpenPGP-Standards und wurde seitdem kontinuierlich weiterentwickelt. Es gibt jedoch auch andere quelloffene Implementierungen des Verfahrens.

Wie Sie in Kapitel 2 schon gelernt haben, können Sie Ihren öffentlichen PGP-Schlüssel frei herausgeben und in der Welt verbreiten, da er nicht dazu verwendet werden kann, Ihre E-Mails zu entschlüsseln – er taugt nur zum Verschlüsseln von E-Mails, die Sie dann mithilfe Ihres privaten Schlüssels lesen können. Wenn Sie von jemandem verschlüsselte E-Mails empfangen wollten, war es daher ursprünglich notwendig, mit dieser Person erst einmal unverschlüsselt zu kommunizieren – Sie mussten Ihrem Gegenüber ja schließlich Ihren öffentlichen Schlüssel zukommen lassen. Um hier Abhilfe zu schaffen, gibt es mittlerweile eine Reihe sogenannter Schlüsselserver, auf denen Sie Ihren öffentlichen Schlüssel in Verbindung mit Ihrem Namen und Ihrer E-Mail-Adresse deponieren können. Wenn Ihnen eine fremde Person, zum Beispiel Alice, nun eine verschlüsselte E-Mail schicken will, muss Alice nur auf einem der gängigen Schlüsselserver nach Ihrem Namen oder Ihrer E-Mail-Adresse suchen. Ist er dort hinterlegt, kann sie Ihren öffentlichen Schlüssel herunterladen und in ihren E-Mail-Client importieren. Dabei spielt es oft auch keine Rolle mehr, auf welchen Server Sie Ihren Key ursprünglich hochgeladen haben. Die meisten Dienste synchronisieren die Schlüssel untereinander, sodass sich ein Schlüssel innerhalb weniger Stunden auf allen Keyservern verteilt.

Hierdurch ist aber ein neues Problem entstanden, das zurzeit einer der größten Kritikpunkte am PGP-Standard ist: das *Schlüsselserver-Problem*. Es gibt keinen zuverlässigen Mechanismus, der verhindert, dass ein Angreifer (nennen wir ihn oder sie Mallory) selbst einen öffentlichen Schlüssel generiert und ihn unter Ihrem Namen auf den Keyserver hochlädt. Auf diese Art und Weise wird zwar nicht die Sicherheit der E-Mails beeinträchtigt, die mit dem richtigen Schlüssel verschlüsselt werden. Wenn aber Mallory in einer Position ist, in der er oder sie Ihre Mails abfangen kann, dann würde ihm das normalerweise nichts nützen, weil er Ihre verschlüsselte Kommunikation nicht entziffern kann. Wenn Ihr Kommunikationspartner nun aber den falschen, von Mallory generierten Schlüssel verwendet, könnte Mallory die gesamte Kommunikation lesen, da nur er im Besitz des passenden privaten Schlüssels ist. Und auch wenn Mallory Ihre E-Mails nicht abfängt, sondern sich nur einen dummen Scherz erlaubt hat, indem er oder sie einen falschen Schlüssel unter Ihrem Namen erstellt hat, müssen Sie sich möglicherweise über unlesbare Mails in Ihrem Postfach ärgern.

4.6.2. Gpg4win für Microsoft Outlook unter Windows

Wie wir in den vorangegangenen Abschnitten dieses Kapitels gesehen haben, kann eine wirklich sichere Ende-zu-Ende-Verschlüsselung nur mithilfe eines E-Mail-Clients realisiert werden – die Verschlüsselung mit einem Browser-Add-on wie Mailvelope bietet zwar größeren Schutz als der Versand unverschlüsselter Mails, geht jedoch mit dem Risiko einher, dass die Mails bereits in unverschlüsseltem Zustand auf dem Server des Mailproviders des Absenders zwischengespeichert werden.

Wenn Sie Windows-Nutzer sind, benutzen Sie vielleicht schon Microsoft Outlook oder einen anderen E-Mail-Client, wie beispielsweise Mozilla Thunderbird.

Wenn Sie Thunderbird-Benutzer sind, springen Sie einfach zum nächsten Abschnitt – da Thunderbird ein Programm ist, das unter Windows wie auch unter Linux läuft, haben wir die Verschlüsselung mit Enigmail und GnuPG im nächsten Abschnitt unter Linux erklärt. Die Vorgehensweise für Sie als Windows-Nutzer ist aber praktisch die gleiche.

Wenn Sie Outlook-Benutzer sind, möchten wir Ihnen ans Herz legen, zu einer Open-Source-Lösung wie Thunderbird zu wechseln. Da das aber einen gewissen Aufwand bedeutet (und Sie vielleicht zumindest für Ihre beruflichen Mails auf Outlook angewiesen sind), werden wir hier trotzdem die Grundlagen der PGP-Verschlüsselung mit Outlook erklären. Die Macher von Gpg4win weisen jedoch selbst darauf hin, dass es bei der Integration von OpenPGP in Outlook technische Schwierigkeiten gibt, sodass Installation und Bedienung vielleicht nicht ganz so reibungslos sind, wie es bei Thunderbird und Enigmail oder anderen Lösungen der Fall wäre.

Praktischerweise (und anders, als der Name vermuten lässt), unterstützt Gpg4win auch das Verschlüsselungsverfahren S/MIME als Alternative zu PGP, sodass wir später in diesem Kapitel zu Gpg4win noch einmal zurückkommen werden.

Außerdem wird mit Gpg4win ein alternativer E-Mail-Client zu Outlook mitgeliefert – das Programm Claws, das wir im Zusammenhang mit dem sicheren Betriebssystem Tails schon kurz angesprochen haben und in Kapitel 6 noch einmal behandeln werden.

Um Gpg4win mit Outlook zu benutzen, müssen Sie die Software also zunächst einmal von der Gpg4win-Webseite[8] herunterladen. Die Software bringt, wie unter Windows üblich, ihr eigenes Installationsprogramm mit – Sie müssen also zunächst die .exe-Datei ausführen. Ein Assistent führt Sie dann durch den Installationsvorgang.

Wenn Sie gefragt werden, welche Komponenten von Gpg4win Sie installieren möchten, können Sie die vorbestehende Auswahl zunächst einmal so lassen (weitere Komponenten lassen sich später immer noch installieren). Außerdem müssen Sie die unter Windows üblichen Fragen nach dem gewünschten Installationslaufwerk und einer Desktop-Verknüpfung beantworten (hier können Sie ebenfalls ruhig bei den Standardeinstellungen bleiben).

Wenn Gpg4win erfolgreich installiert wurde, starten Sie über das Startmenü das Programm Kleopatra. Wie Sie wissen, müssen Sie für die erfolgreiche Nutzung von PGP ein Schlüsselpaar aus öffentlichem und privatem Schlüssel generieren. Das übernimmt Kleopatra für Sie, wenn Sie in der Kopfleiste den Menüpunkt Datei und dann Neues Zertifikat anwählen. Im nächsten Fenster geben Sie an, dass es sich um ein OpenPGP-Zertifikat handeln soll (statt um ein S/MIME-, also X.509-Zertifikat). Kleopatra fragt Sie dann nach Ihrem Namen, Ihrer E-Mail-Adresse und einem (optionalen) Kommentar – hier könnten Sie zum Beispiel »Arbeit« oder »zu Hause« angeben, um verschiedene Schlüssel für die gleiche E-Mail-Adresse später unterscheiden zu können. Sie können das Feld aber auch freilassen. Wenn Sie Ihre Eingaben geprüft haben, starten Sie das Generieren des Schlüsselpaars. Kleopatra fragt Sie zunächst nach Ihrer Passphrase, mit der später Ihr privater Schlüssel geschützt wird. Auf die Eigenschaften einer guten Passphrase sind wir weiter oben schon eingegangen (in Kürze: lang, schwer zu erraten und natürlich geheim). Der Computer generiert dann das Schlüsselpaar. Sie können ihm helfen, die dafür benötigten Zufallszahlen zu generieren, indem Sie in der Zeit irgendetwas anderes auf dem Computer machen – beispielsweise tippen oder eine andere Anwendung starten. Wenn die Generierung des Schlüsselpaares abgeschlossen ist, können Sie den öffentlichen Schlüssel an einen Schlüsselserver oder einen E-Mail-Kontakt schicken lassen oder eine Sicherheitskopie des privaten Schlüssels erstellen (all das können Sie aber auch später noch machen). Fertig! Sie können das Schlüsselpaar jetzt benutzen – das heißt, Ihre Kontakte können Ihnen verschlüsselte Mails schicken, die Sie dann mit Ihrem privaten Schlüssel entschlüsseln können.

Wie funktioniert das Entschlüsseln? Gpg4win hat Ihnen dazu in Ihr Outlook ein kleines Add-on namens GpgOL installiert. Wenn Sie eine an Sie gerichtete, mit Ihrem Public Key verschlüsselte Mail erhalten, übernimmt GpgOL die Entschlüsselung automatisch, sobald Sie die Passphrase Ihres privaten Schlüssels eingegeben haben.

Und das Versenden von verschlüsselten Mails? Hierzu brauchen Sie den öffentlichen Schlüssel (Gpg4win spricht hier immer von einem »öffentlichen Zertifikat«) des Absenders. Wenn Sie das erste Mal mit diesem Absender verschlüsselt kommunizieren wollen und er Ihnen seinen öffentlichen Schlüssel als Anhang mitgeschickt hat, speichern Sie den Anhang ab. Dann starten Sie Kleopatra und importieren den Schlüssel über den Menüpunkt Datei und dann ZERTIFIKAT IMPORTIEREN. Nun zeigen Sie Kleopatra noch den Speicherort der Datei (mit der Dateiendung .gpg oder .asc). Der Schlüssel ist nun in Ihrer Zertifikatsverwaltung.

Zurück in Outlook können Sie die Verschlüsselung einer E-Mail über die Menüpunkte EXTRAS und dann NACHRICHT VERSCHLÜSSELN aktivieren. GpgOL erkennt automatisch, wenn ein öffentlicher Schlüssel für den Empfänger in Ihrer Zertifikatsverwaltung gespeichert ist. Falls es für den Empfänger sowohl einen OpenPGP-Schlüssel als auch einen S/MIME-Schlüssel gibt, können Sie zwischen beiden wählen.

Hieran sehen Sie übrigens, dass Gpg4win auch S/MIME unterstützt. Da die S/MIME-Unterstützung auch in Outlook selbst eingebaut ist, benötigen Sie Gpg4win für S/MIME unter Outlook allerdings gar nicht, wie Sie weiter unten im Abschnitt »S/MIME für Windows« noch sehen werden.

4.6.3. Enigmail und GnuPG für Thunderbird unter Linux oder Windows

Thunderbird ist der von Mozilla entwickelte E-Mail-Client. Mozilla ist die gleiche Organisation, die auch die Entwicklung des Webbrowsers Firefox vorantreibt. Thunderbird ist genau wie Firefox Open Source. Hierdurch lässt sich die Software im Bezug auf Datensicherheit zunächst schon einmal optimistischer beurteilen als Closed-Source-Software, zum Beispiel Microsoft Outlook. Gleichzeitig ist das Programm sehr benutzerfreundlich und auch für Microsoft Windows verfügbar, sodass es eine brauchbare Alternative zu Outlook darstellt.

Für Thunderbird gibt es das Add-on Enigmail, das die OpenPGP-Implementierung GnuPG nutzt, um Ihre E-Mails zu verschlüsseln. Früher war es nötig, zunächst GnuPG und Thunderbird (in beliebiger Reihenfolge) herunterzuladen und zu installieren und hinterher noch Enigmail nachzuschieben. Das ganze System wurde aber mittlerweile so benutzerfreundlich gestaltet, dass Sie nur noch Thunderbird installieren müssen und Enigmail sowie GnuPG hinterher aus

Thunderbird heraus installieren lassen können, ohne dass Sie sich selbst um Download und Installationsprozess kümmern müssen.

Um Thunderbird zu installieren, gibt es sehr schöne deutschsprachige Anleitungen (für Windows und Linux) auf den Seiten der Mozilla Foundation, die Sie leicht finden werden, wenn Sie »thunderbird installieren« googeln (oder duckduckgoen).

Starten Sie die Software, sobald Thunderbird installiert wurde. Das Programm sollte Sie automatisch fragen, ob Sie ein neues E-Mail-Konto anlegen möchten (wenn nicht, können Sie auch über den Menüpunkt NEUES KONTO HINZUFÜGEN dorthin gelangen). Wenn Sie gefragt werden, ob Sie sich eine ganz neue E-Mail-Adresse einrichten wollen, verneinen Sie dies und wählen stattdessen EXISTIERENDES E-MAIL-KONTO VERWENDEN.

Thunderbird startet nun einen Assistenten zur automatischen Einrichtung eines bestehenden E-Mail-Kontos. Sie werden nach Ihrem Namen (wie er später den Empfängern Ihrer Mails angezeigt werden soll), Ihrer Mailadresse und dem Passwort für Ihr E-Mail-Konto gefragt. Wenn Sie alle Angaben gemacht haben, gelingt es Thunderbird in den meisten Fällen, von selbst den Mailserver Ihres Anbieters zu identifizieren und sich in Ihren Posteingang einzuloggen. Ist das nicht der Fall, wird Ihnen als Nächstes ein weiteres Fenster angezeigt, in das Sie den Namen des Mailservers und weitere Angaben von Hand eingeben müssen – diese Angaben finden Sie meist auf den Hilfeseiten Ihres E-Mail-Providers.

Auch bei einer bestehenden Thunderbird-Installation können Sie einen neuen E-Mail-Account anlegen: Über EXTRAS und KONTEN-EINSTELLUNGEN kommen Sie zur Liste der bestehenden Konten und können dann links unten unter KONTEN-AKTIONEN die Aktion E-MAIL-KONTO HINZUFÜGEN wählen (siehe Abbildung 4.2).

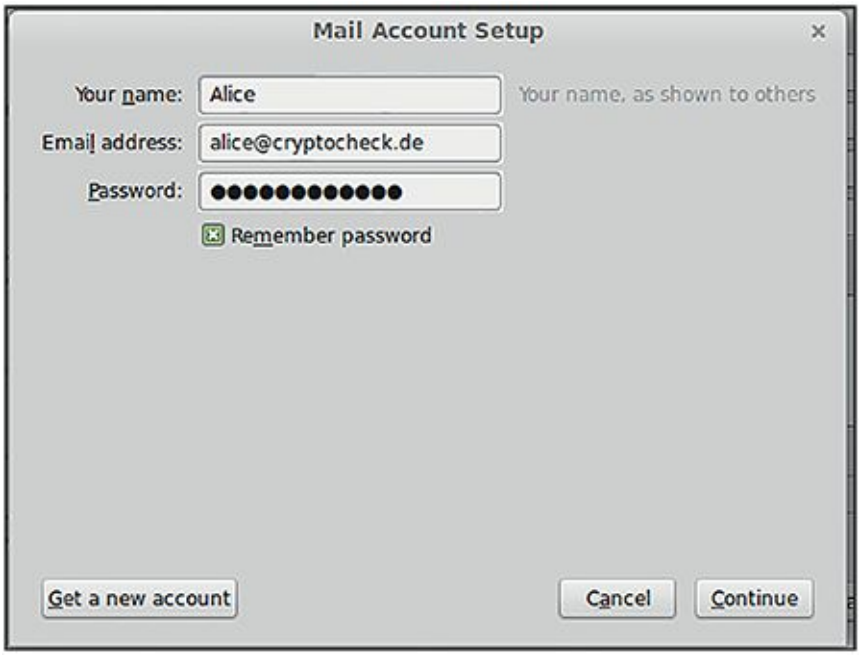


Abb. 4.2 Neuen Mailaccount anlegen im E-Mail-Client Thunderbird

Wenn alles glattgegangen ist, bekommen Sie nach Abschluss der Einrichtung Ihren Posteingangsordner (die Inbox) in der linken Leiste des Fensters angezeigt. Schicken Sie jetzt ruhig mal eine (noch unverschlüsselte) E-Mail zum Test an sich selbst. Wenn alles funktioniert, sind Sie bereit für die Installation von Enigmail. Hierzu wechseln Sie zunächst in Thunderbirds Add-on-Verwaltung (siehe Abbildung 4.3).

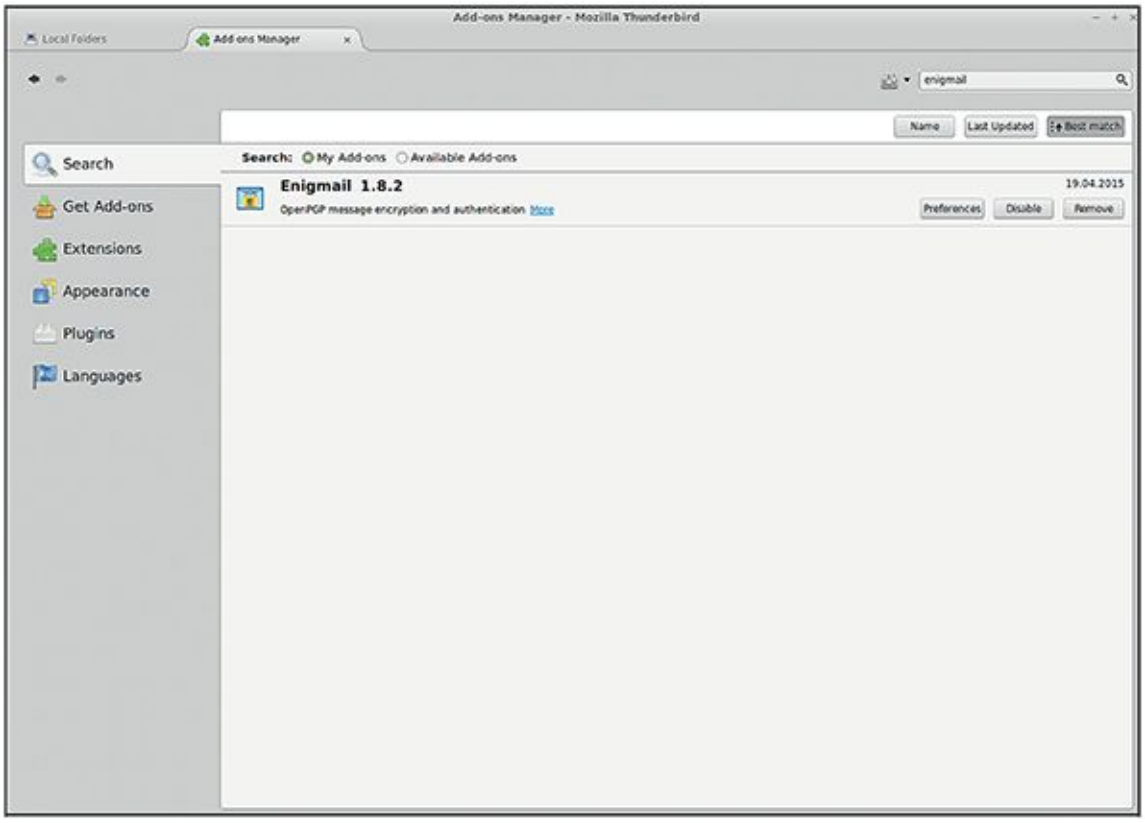


Abb. 4.3 Suche von Add-ons im E-Mail-Client Thunderbird

Sie können mit dem in der oberen Menüleiste gelegenen Suchfeld das Wort »enigmail« suchen. Das Add-on wird Ihnen daraufhin in der Ergebnisliste angezeigt, und Sie können es über eine entsprechende Schaltfläche direkt installieren. (Über dieses Menü können Sie übrigens auch bereits installierte Add-ons wieder deaktivieren.)

Nach gelungener Installation startet der Enigmail-Assistent, der, abhängig von Ihrer Version des Programms, auch OpenPGP-Assistent heißen kann und Sie durch die ersten Einrichtungsschritte führt (siehe auch Abbildung 4.4). Wenn Sie nicht schon GnuPG installiert haben (was wahrscheinlich nicht der Fall ist, wenn Sie Enigmail zum ersten Mal benutzen), schlägt er Ihnen zunächst vor, GnuPG zu installieren, und führt diese Installation automatisch für Sie durch, wenn Sie den Vorschlag akzeptieren.

Abb. 4.4 Enigmail-Assistent (Setup Wizard)

Daraufhin werden Sie aufgefordert, ein paar Entscheidungen zu treffen, wie Sie Enigmail in Zukunft verwenden möchten. Keine Angst, alle diese Optionen können Sie später an anderer Stelle korrigieren, falls das nötig sein sollte. Verschlüsselung: Wählen Sie hier zunächst BEQUEME AUTOMATISCHE VERSCHLÜSSELUNG. Unterschreiben: Dass Ihre E-Mails unterschrieben sind, ist für vertrauliche Kommunikation nicht erforderlich. Wenn Sie erst einmal auf eine digitale Unterschrift verzichten möchten, wählen Sie hier MEINE NACHRICHTEN SOLLEN STANDARDMÄSSIG nicht UNTERSCHRIEBEN WERDEN. Einstellungen: Hier wird Ihnen die Möglichkeit angeboten, Enigmail so einzustellen, dass E-Mails automatisch als Text (statt HTML) versandt werden. Bei der Verschlüsselung mit PGP geht mit dieser Einstellung die Formatierung weniger kaputt. Stellen Sie also ruhig den Textversand von E-Mails ein. Kein OpenPGP-Schlüssel gefunden: Nun wird Enigmail Ihnen mitteilen, dass es kein PGP-Schlüsselpaar von Ihnen gefunden hat. Sie müssen also, wenn Sie Enigmail zum ersten Mal benutzen und kein Schlüsselpaar importieren wollen, neue Schlüssel erstellen. Das übernimmt Enigmail für Sie, wenn Sie auf Fortsetzen klicken. OpenPGP-Schlüssel erzeugen: Sie werden nun aufgefordert, eine Passphrase für Ihren privaten Schlüssel zu wählen. Wie Sie wissen, sollte Ihr privater Schlüssel niemals in fremde Hände gelangen. Wenn das irgendwann aus irgendeinem Grund doch einmal geschehen sollte, bietet die Passphrase eine Art letzte Sicherung. Zudem können Sie, auch wenn Ihr Computer von

mehreren Personen verwendet wird, dadurch sicherstellen, dass Ihr privater Schlüssel auch privat bleibt. Zusammenfassung: Hier werden Ihnen die bisherigen Schritte zur Kontrolle noch einmal angezeigt. Enigmail-Bestätigung: Enigmail bestätigt Ihnen, dass Ihr Schlüsselpaar erzeugt wurde, und bietet Ihnen an, ein Zertifikat zu erstellen, mit dem Sie Ihren Schlüssel widerrufen können, falls der private Schlüssel in falsche Hände geraten sollte.

Dieses können Sie einsetzen, um Ihren öffentlichen Schlüssel bei den Schlüsselservern zurückzuziehen, sodass keine weiteren E-Mails an Sie geschrieben werden, die einen unsicheren Schlüssel verwenden. Wenn Sie dieses Zertifikat erstellen möchten, halten Sie einen Datenträger, zum Beispiel einen USB-Stick bereit, auf dem Sie dieses Zertifikat dann speichern und aufbewahren können. Aus eigener Erfahrung möchte mindestens einer der Autoren Ihnen übrigens dringend zu diesem Schritt raten.

Fertig! Wenn Sie das Fenster des Assistenten nun schließen, werden Sie sehen, dass Thunderbird ein paar neue Menüpunkte und Schaltflächen erhalten hat. Mit diesen können Sie in Zukunft die Ver- und Entschlüsselung von E-Mails, das Signieren und die Verwaltung von Schlüsseln steuern.

Wem können Sie nun eine verschlüsselte Nachricht schreiben? Hier müssen wir Sie kurz enttäuschen – erst mal niemandem außer sich selbst, denn Sie haben bisher keine öffentlichen Schlüssel von anderen Personen in Ihrer Schlüsselverwaltung. Bisher kann Ihnen auch niemand eine verschlüsselte E-Mail schicken, weil niemand Ihren öffentlichen Schlüssel kennt.

Zeit, das zu ändern! Verschicken Sie erst einmal ein paar E-Mails mit Ihrem öffentlichen Schlüssel als Anhang an Ihre Freunde, die ebenfalls PGP benutzen. Ihren öffentlichen Schlüssel können Sie natürlich unverschlüsselt verschicken, da er – genau – öffentlich ist. Dazu können Sie eine Funktion des Schlüsselmanagers benutzen. Klicken Sie in der Übersicht mit der rechten Maustaste auf Ihren kürzlich erzeugten Key und wählen Sie Öffentliche Schlüssel per E-Mail senden. Enigmail öffnet daraufhin eine neue E-Mail-Nachricht, in die Sie nur noch den oder die Empfänger eintragen müssen.

Vielleicht sind Sie auch der oder die Erste in Ihrem Bekanntenkreis, der oder die sich für E-Mail-Verschlüsselung mit PGP entschieden hat. Für diesen Fall haben wir cryptocheck.de eingerichtet: Schicken Sie eine E-Mail mit Ihrem öffentlichen Schlüssel als Anhang an alice@cryptocheck.de oder bob@cryptocheck.de, und Alice oder Bob wird Ihnen eine

verschlüsselte Mail als Antwort zurückschicken. Wenn Sie diese lesen können, wissen Sie, dass Sie nun in der Lage sind, verschlüsselt zu kommunizieren.

Wie gehen Sie den Versand einer verschlüsselten E-Mail nun konkret an? Bitten Sie zunächst jemanden, der bereits PGP verwendet, Ihnen seinen oder ihren öffentlichen Schlüssel zu schicken. Dieser wird in der Regel als Anhang an eine unverschlüsselte Mail versandt. Wenn Sie nun diese E-Mail in Thunderbird angezeigt bekommen, klicken Sie mit rechts auf den Anhang und wählen IMPORTIEREN. Der öffentliche Schlüssel wird nun in Ihre Schlüsselverwaltung aufgenommen.

Im Menü von Thunderbird gelangen Sie über ENIGMAIL und SCHLÜSSELVERWALTUNG zur Liste aller Schlüssel, die Sie bereits erhalten haben. Auch Ihr eigenes Schlüsselpaar ist hier gelistet, und zwar in der Liste fett gedruckt, da hier auch ein privater Schlüssel dabei ist. Alle öffentlichen Schlüssel von anderen Personen, zu denen Sie den privaten Schlüssel nicht haben, sind in normaler Schrift aufgelistet.

Aus dem Fenster SCHLÜSSELVERWALTUNG heraus können Sie auch nach öffentlichen Schlüsseln von Personen suchen, von denen Sie nur die E-Mail-Adresse kennen:

Klicken Sie dazu auf SCHLÜSSELSERVER und SCHLÜSSEL SUCHEN und geben Sie die E-Mail-Adresse an. Enigmail wird nun auf dem darunter ausgewählten Schlüsselserver (die gängigsten sind voreingestellt) nach einem öffentlichen Schlüssel für diese Adresse suchen. Falls ein passender Schlüssel gefunden wird, haben Sie im nächsten Schritt die Möglichkeit, ihn in Ihre Schlüsselverwaltung zu importieren. Automatisieren können Sie diesen Schritt mit dem Menüpunkt SCHLÜSSEL FÜR ALLE KONTAKTE FINDEN – falls Sie Thunderbird schon länger benutzen und ein gut gefülltes Adressbuch haben, wird Enigmail den Keyserver nach öffentlichen Schlüsseln für alle Ihre Kontakte absuchen. Vorsicht: Je nach Anzahl Ihrer Kontakte kann das eine Weile dauern.

Außerdem können Sie aus der Schlüsselverwaltung heraus öffentliche Schlüssel importieren, die Ihnen als Textdatei vorliegen – weil ein Kommunikationspartner Ihnen seinen öffentlichen Schlüssel beispielsweise per USB-Stick auf die Festplatte kopiert hat. Dazu wählen Sie den Menüpunkt DATEI und SCHLÜSSEL AUS DATEI IMPORTIEREN und geben dann die entsprechende Textdatei auf Ihrem System an.

Auch Ihr eigenes Schlüsselpaar können Sie aus der Schlüsselverwaltung heraus als Textdatei abspeichern. Gehen Sie hierzu auf DATEI und SCHLÜSSEL IN DATEI EXPORTIEREN. Dann werden Sie

gefragt, ob Sie Ihr komplettes Schlüsselpaar, inklusive privatem Schlüssel, oder nur Ihren öffentlichen Schlüssel exportieren wollen. Wenn Sie vorhaben, diese Datei in irgendeiner Form an eine andere Person weiterzugeben, exportieren Sie nur Ihren öffentlichen Schlüssel! Wenn Sie aus Versehen das komplette Schlüsselpaar weitergeben, müssen Sie sich ein neues generieren, um weiterhin sicher verschlüsselt kommunizieren zu können. Ihre ganze zurückliegende verschlüsselte Kommunikation ist damit prinzipiell für jemand anderen lesbar geworden. Vorsicht also bei der Herausgabe von exportierten Schlüsseln!

Wenn Sie also nun den einen oder anderen öffentlichen Schlüssel in Ihrer Schlüsselverwaltung haben, können Sie die erste verschlüsselte Mail schreiben. Wenn nicht, auch nicht schlimm: Schreiben Sie die Mail einfach an sich selber, Ihre eigenen öffentlichen Schlüssel haben Sie ja.

Öffnen Sie dazu in Thunderbird eine neue E-Mail. Wenn Sie im Schreibfenster nun auf den Enigmail-Button klicken, bekommen Sie angezeigt, ob die E-Mail verschlüsselt und/oder signiert wird. Wählen Sie nun aus, dass die E-Mail verschlüsselt, aber nicht signiert wird, und schließen Sie das Fenster wieder.

Nebenbei können Sie hier auch wählen, ob Sie Inline-PGP oder PGP/MIME verwenden wollen – bei Inline-PGP werden die PGP-Steuerungsinformationen im E-Mail-Text versandt, bei PGP/MIME als Anhang. Das letztere Verfahren ist zwar neuer und zuverlässiger, allerdings kommen noch nicht alle E-Mail-Clients damit klar (Outlook, das wir im letzten Abschnitt besprochen haben, beispielsweise nicht). Wenn Sie nicht wissen, ob der Empfänger PGP/MIME-Mails lesen kann, Sie aber diesbezüglich sichergehen wollen, probieren Sie es am besten zunächst mit Inline-PGP.

Mit einem Klick auf Senden können Sie nun Ihre erste verschlüsselte E-Mail abschicken.

Und wenn Sie nun die erste verschlüsselte E-Mail erhalten?

Wenn Sie versuchen, die Mail zu öffnen, werden Sie als Erstes nach der Passphrase für Ihren privaten Schlüssel gefragt. Wenn Sie diese korrekt eingegeben haben, erscheint der Klartext der E-Mail. Darüber wird eine Enigmail-Statuszeile eingeblendet, die Ihnen sagt, dass Sie gerade eine entschlüsselte Mail lesen. Wenn Sie nicht die richtige Passphrase eingeben oder die Eingabe abbrechen, sehen Sie stattdessen nur den Buchstabensalat der verschlüsselten E-Mail.

Als Nächstes testen Sie einmal den Versand einer signierten E-Mail. Hierzu öffnen Sie wieder eine neue E-Mail und wählen über die Enigmail-Schaltfläche nun SIGNIEREN statt VERSCHLÜSSELN.

Hängen Sie außerdem Ihren öffentlichen Schlüssel an – das geht über den Menüpunkt ENIGMAIL und MEINEN ÖFFENTLICHEN SCHLÜSSEL ANHÄNGEN.

Nun werden Sie schon beim Absenden der Nachricht nach Ihrer Passphrase gefragt. Das macht auch Sinn, denn wie Sie sich aus Kapitel 2 erinnern, wird die Signatur mithilfe Ihres privaten Schlüssels erzeugt, und der Empfänger kann diese mit Ihrem öffentlichen Schlüssel verifizieren.

Wenn soweit alles funktioniert, kommen wir nun zu dem Punkt, an dem das Web of Trust ins Spiel einsteigt: Sie sollten sich davon überzeugen, dass Ihre Kommunikationspartner auch die sind, die sie vorgeben zu sein. Dazu müssen Sie den öffentlichen Schlüssel einer Person mit dieser Person abgleichen. Gehen Sie hierzu noch einmal in die Schlüsselverwaltung und klicken Sie mit rechts auf den jeweiligen Schlüssel. Wählen Sie den letzten Menüpunkt, SCHLÜSSELEIGENSCHAFTEN. Nun wird Ihnen der Fingerabdruck des Keys angezeigt. Wenn Sie genau hinsehen, werden Sie feststellen, dass die letzten acht Stellen des Fingerabdrucks der Key-ID entsprechen, unter der der Schlüssel beispielsweise auch bei Schlüsselservern gespeichert wird.

Sie sollten nun den Fingerabdruck über irgendeinen Kommunikationskanal, der nicht E-Mail ist, mit dem Besitzer des Schlüssels abgleichen. Rufen Sie Bob zum Beispiel an und lesen Sie ihm den Fingerprint vor, der Ihnen angezeigt wird. Wenn er Ihnen bestätigt, dass das in der Tat der Fingerabdruck von seinem Schlüssel ist, können Sie dem Schlüssel Ihr Vertrauen aussprechen.

Dazu wählen Sie in den Schlüsseleigenschaften den Menüpunkt VERTRAUEN FESTLEGEN. Wenn Sie einen halbwegs zuverlässigen Kommunikationskanal verwendet haben, also beispielsweise das Telefon, ist es vertretbar, dem Schlüssel »volles Vertrauen« auszusprechen.

Das können Sie nun nach und nach für alle Ihre Kommunikationspartner machen (vergessen Sie nicht, auch den Fingerprint Ihres eigenen öffentlichen Keys mit ihnen abzugleichen) und bauen dabei langsam Ihr eigenes Web of Trust auf.

4.6.4. GPG Suite für OS X

Für den E-Mail-Client *Mail* für Mac OS (Apple) gibt es die *GPG Suite*, die alle Bestandteile enthält, die Sie für die Installation von GPG und eines Mail-Plug-ins benötigen:

- das GPGMail-Plug-in
- die GPG Keychain zur Verwaltung eigener und fremder OpenPGP-Schlüssel

- den GPG Service, mit dem Sie GPG auch in anderen Programmen nutzen können
- MacGPG als »Power Engine« der Suite, die die Basis für die anderen Plug-ins bildet und die Sie darüber hinaus auch von der Kommandozeile aus nutzen können (wenn Sie dieses Feature benötigen)

Laden Sie sich die GPG Suite von der Webseite[9] herunter und öffnen Sie das Apple Disk Image. Auf der Webseite finden Sie auch eine Beschreibung zur Erstellung eines Schlüsselpaares, zur Schlüsselverwaltung und zum verschlüsselten E-Mailen.

Starten Sie die Installation durch einen Doppelklick auf INSTALL (Abbildung 4.5) und folgen Sie den üblichen Installationsanleitungen.

Abb. 4.5 Installation der GPG Suite

Nach der Installation öffnen Sie das Programm GPG Keychain (Abbildung 4.6), das Sie nun in Ihrem Programmordner beziehungsweise im Launchpad finden.

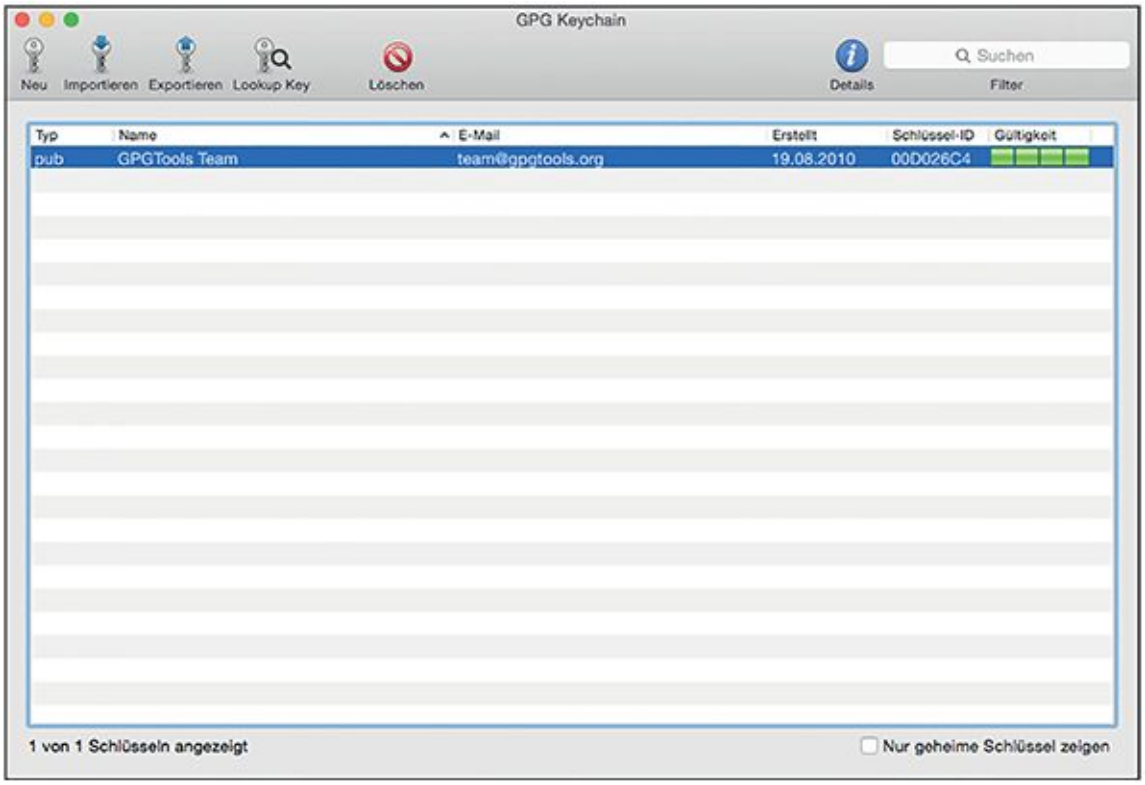


Abb. 4.6 GPG Keychain

Sie können nun Ihr eigenes Schlüsselpaar erstellen (Abbildung 4.7), indem Sie auf den Button New in der Menüleiste klicken. Sie geben nun Ihren Namen und Ihre E-Mail-Adresse ein und können anwählen, dass Ihr neuer öffentlicher Schlüssel gleich auf den Server hochgeladen wird (UPLOAD PUBLICKEY) – ggf. müssen Sie dafür den Menüpunkt ADVANCED OPTIONS öffnen. Nach Eingabe einer Passphrase sind Sie fertig. Nach Klick auf SCHLÜSSEL ERSTELLEN haben Sie Ihr eigenes Schlüsselpaar aus privatem und öffentlichem Schlüssel erstellt. Beide sind in der GPG Keychain gespeichert und werden durch die GPG Suite allen Programmen, zum Beispiel Mail, zur Verfügung gestellt.

Abb. 4.7 GPG Keychain, Schlüsselpaar erstellen

Anschließend können Sie Ihren Schlüssel exportieren (Abbildung 4.8). Ihren öffentlichen Schlüssel können Sie beispielsweise an Freunde, Kollegen und Bekannte schicken oder auf Ihrer Homepage veröffentlichen.

Abb. 4.8 GPG Keychain, Schlüsselpaar exportieren

Wenn Sie dagegen Ihren privaten Schlüssel auch auf einem anderen Gerät nutzen wollten oder wenn es Ihnen sicherer erscheint, diesen auf einem mobilen Datenträger wie einem USB-Stick aufzubewahren statt auf der Festplatte Ihres Computers, so können Sie durch das Anhaken von GEHEIMEN SCHLÜSSEL EBENFALLS EXPORTIEREN Ihren öffentlichen *und* Ihren privaten Schlüssel exportieren. Sie wissen das zwar schon, aber weil es so wichtig ist, erinnern wir noch einmal daran: Schicken Sie Ihren privaten Schlüssel *nie* an jemand anderen.

Haben Sie dagegen schon ein eigenes Schlüsselpaar, zum Beispiel auf einem Datenträger, können Sie diesen in die Schlüsselverwaltung GPG Keychain durch SCHLÜSSEL IMPORTIEREN in der Menüleiste einfügen.

Unter dem Menüpunkt LOOKUP KEY haben Sie die Möglichkeit, den Schlüsselservernach einem Namen oder einer E-Mail-Adresse zu durchsuchen und die öffentlichen Schlüssel dieses Kontaktes hinzuzufügen.

Glückwunsch! Sie sind nun im Besitz Ihres Schlüsselpaares und können mit dem verschlüsselten E-Mailen beginnen. Dazu wechseln Sie zu Ihrem E-Mail-Programm Mail. Dort finden Sie unter EINSTELLUNGEN einen neuen Menüpunkt GPGMAIL. Dort können Sie einstellen, ob standardmäßig alle Ihre E-Mails signiert und wenn möglich verschlüsselt werden sollen (Abbildung 4.9). Außerdem werden mögliche Probleme mit GPGMail dort angezeigt.

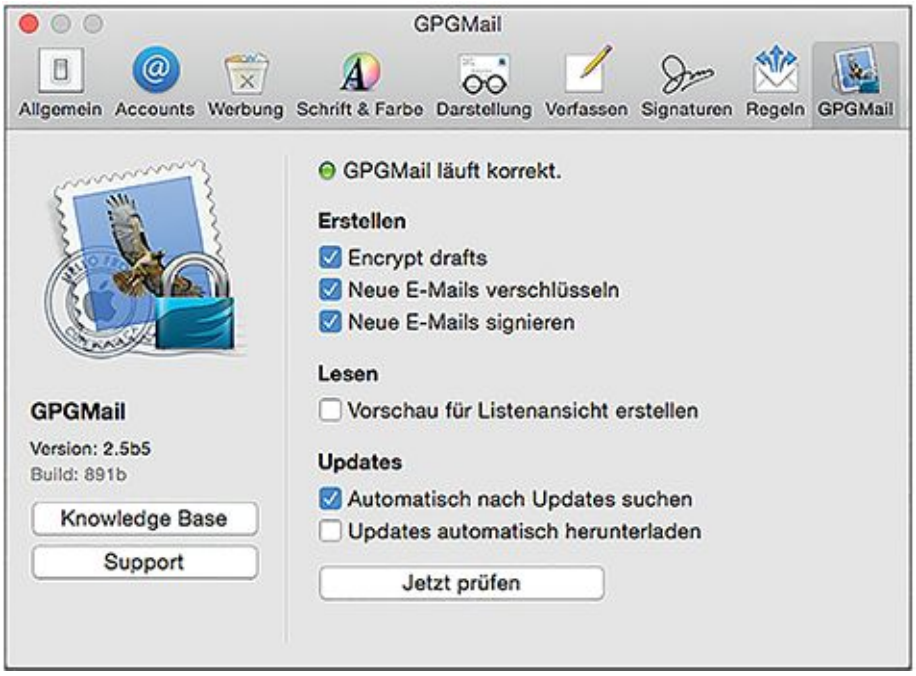


Abb. 4.9 GPGMail-Plug-in in den Einstellungen von Mail

Nun können Sie Ihre erste E-Mail mit dem GPGMail-Plug-in schreiben. Neben der Betreffzeile wird Ihnen angezeigt, ob Ihre Mail verschlüsselt und/oder signiert ist – durch Klick auf diese Symbole können Sie diese Voreinstellungen auch aktivieren und deaktivieren (Abbildung 4.10).

Abb. 4.10 GPGMail-Plug-in, neue Mail schreiben

Schreiben Sie an einen Kontakt, der kein OpenPGP nutzt oder dessen Schlüssel Sie noch nicht importiert haben, können Sie nur einstellen, ob die Mail signiert werden soll oder nicht (Abbildung 4.11).

Abb. 4.11 GPGMail, signierte unverschlüsselte Mail schreiben

Wenn Sie eine verschlüsselte E-Mail erhalten, müssen Sie zumindest beim ersten Mal Ihre Passphrase eingeben. Wenn Sie diese in Ihrem Schlüsselbund auf dem Computer speichern, müssen Sie das nicht jedes Mal erneut tun, wenn Sie eine verschlüsselte E-Mail erhalten. E-Mails, die Sie verschlüsselt erhalten haben und deren Klartext, also deren für Sie lesbarer Inhalt, angezeigt wird, sind durch einen Hinweis im Header der E-Mail, meist unter der Betreff-Zeile, gekennzeichnet.

4.7 Vertrauensbasis neutrale Autorität – S/MIME nutzen

PGP ist nicht das einzige gängige Verfahren der Public-Key-Kryptografie: Eine weit verbreitete Alternative ist S/MIME. Im Folgenden werden Sie die Gemeinsamkeiten und Unterschiede kennenlernen.

4.7.1. Was ist S/MIME?

S/MIME steht für Secure/Multipurpose Internet Mail Extensions und ist, wie PGP auch, eine Form der E-Mail-Verschlüsselung und -Signierung, die auf der Public-Key-Kryptografie beruht. Wie bei PGP haben Sie also einen öffentlichen und einen privaten Schlüssel und müssen Letzteren streng geheim halten.

S/MIME ist die am weitesten verbreitete Form der Verschlüsselung und Signierung, die nicht auf einem Web of Trust, sondern auf Vertrauen in eine zentrale Autorität beruht.

Was bedeutet das? Anders als beim Web of Trust bei PGP werden öffentliche Schlüssel bei S/MIME nicht von möglichst vielen Menschen signiert, die den Besitzer persönlich kennen,

sondern von einer zentralen Stelle, bei der der Besitzer sich ausweisen muss. Diese Stelle wird auch als Zertifizierungsstelle oder Zertifikatsautorität (*Certificate Authority*, CA) bezeichnet.

Wenn die CA den öffentlichen Schlüssel von Alice zertifiziert, bürgt sie sozusagen dafür, dass der Schlüssel tatsächlich zu Alice und ihrer E-Mail-Adresse gehört. Dieses Prinzip haben Sie schon in Kapitel 2 kennengelernt. Als Bestätigung dient ein *Zertifikat*, also ein elektronisches Dokument, in dem Alices Name, ihre E-Mail-Adresse und ihr Schlüssel stehen. Dieses Dokument wird von der CA mit ihrem öffentlichen Schlüssel signiert.

Das wirft die Frage auf, wer dafür geradesteht, dass der private Schlüssel, mit dem Alices Zertifikat signiert ist, tatsächlich der CA gehört. Wie Sie in Kapitel 2 gelernt haben, ist das in diesem Fall die nächsthöhere CA, die der untergeordneten CA auch wieder ein Zertifikat ausstellt, ähnlich dem, das Alice erhalten hat. Weil dieses Prinzip sich pyramidenartig fortsetzt, bis zu einer ganz übergeordneten CA (Root-CA oder, etwas sperrig auf Deutsch, Wurzelzertifizierungsinstanz), bezeichnet man diese Art der Organisation auch als hierarchisch. Die Root-CA bekommt von keiner anderen CA mehr ein Zertifikat ausgestellt, sondern setzt deren Vertrauen einfach voraus. Es existiert auf der Welt nicht nur eine Root-CA, die für alle untergeordneten CAs zuständig ist, wie man vielleicht meinen könnte. Vielmehr gibt es eine Reihe von Root-CAs, die von Firmen, Regierungen und Behörden oder anderen Organisationen betrieben werden, beispielsweise von der Deutschen Telekom, der Firma Symantec oder der Bundesnetzagentur.

Die zentralistische Organisation von S/MIME ist gleichzeitig ihr Vor- und Nachteil: Während das bei PGP verwendete Web of Trust nur dann zu Vertrauen zwischen unbekannten Personen führt, wenn das Netzwerk gemeinsamer Bekannter (auch zweiten, dritten, vierten Grades) groß genug ist, kann jeder Absender sich durch das Zertifikat einer vertrauenswürdigen CA selbst als vertrauenswürdig ausweisen. Andererseits, wie wir schon in Kapitel 2 gesehen haben, ist es leichter, die Datenbanken einer einzelnen zentralen Autorität zu knacken, als ein großes Web of Trust zu unterwandern.

Die Zertifikate des Web of Trust von PGP und die Zertifikate von CAs in S/MIME sind nicht miteinander kompatibel – unter anderem, weil die Zertifikate verschiedene Formate haben. Das heißt, wenn Alice mit S/MIME verschlüsselt und Bob mit OpenPGP, können beide sich so lange keine verschlüsselten oder signierten Mails schicken, bis sie sich auf eins der beiden Verfahren einigen.

Die vertrauensstiftende Wirkung des Zertifikats einer CA beruht also darauf, dass diese »weiß«, dass ein öffentlicher Schlüssel zu einer bestimmten Person mit einer bestimmten E-Mail-Adresse gehört. Im Idealfall sollte sie also von jeder Person, die ein Zertifikat erhält, einen Beweis für die eigene Identität vorgelegt bekommen haben – beispielsweise dadurch, dass der Nutzer mit seinem Personalausweis ins Büro der CA marschiert. Dies ist bei Zertifikaten der Klasse 3 tatsächlich der Fall.

Aus praktischen Gründen gibt es aber noch zwei weitere Klassen mit weniger vertrauenswürdigen Zertifikaten, die dafür aber für die Nutzer auch weniger umständlich zu erlangen sind.

Klasse-1-Zertifikate bestätigen, dass der Besitzer des Zertifikats und des zugehörigen öffentlichen Schlüssels auch Besitzer der im Zertifikat genannten E-Mail-Adresse ist. Es wird nicht geprüft, ob er der ist, der er vorgibt zu sein – Sie können sich also leicht ein Klasse-1-Zertifikat unter dem Namen Wonder Woman mit der Mailadresse wonderwoman42@posteo.de ausstellen lassen, solange Sie ein gültiges Schlüsselpaar generieren und tatsächlich Zugriff auf die E-Mail-Adresse wonderwoman42@posteo.de haben. Für die ersten Schritte mit E-Mail-Verschlüsselung und den Gebrauch unter Freunden für wenig sensible Informationen ist so eine Art von Zertifikat also erst einmal ausreichend.

Den *Klasse-2-Zertifikaten* liegt eine schriftliche Bestätigung des Benutzers über seine eigene Identität zugrunde. Ein Ausweis muss jedoch auch für Klasse-2-Zertifikate nicht vorgezeigt werden. Klasse-2-Zertifikate werden beispielsweise innerhalb von Unternehmen verwendet: Wenn das Unternehmen selbst ein Klasse-3-Zertifikat innehat, kann es seinen Mitarbeitern auf schriftlichen Antrag Klasse-2-Zertfikate ausstellen.

Klasse-3-Zertifikate, wie schon erwähnt, werden ausgestellt, wenn der Antragsteller seine Identität mit einem Ausweisdokument bewiesen hat. Dazu muss er nicht unbedingt persönlich bei der CA erscheinen – das geht beispielsweise auch mit dem PostIdent-Verfahren. (Streng genommen sind Zertifikate, bei denen der Inhaber sich persönlich bei der CA vorgestellt hat, sogar noch vertrauenswürdiger und werden als *Klasse-4-Zertifikate* bezeichnet.) Da auch Firmen Inhaber von Klasse-3-Zertifikaten sein können, dürfen diese ihre Identität stattdessen auch mit einem Auszug aus dem Handelsregister oder dem Gewerbenachweis belegen.

Wichtig zu verstehen: Die Stärke der Verschlüsselung ist bei allen Klassen von Zertifikaten gleich gut (vorausgesetzt, dass Ihr privater Schlüssel wirklich nicht in fremde Hände geraten

ist). Sie unterscheiden sich nur in der Stärke der Authentifizierung, das heißt, der Empfänger kann sich bei einer höheren Klasse von Zertifikat sicherer sein, dass der Absender der ist, der er vorgibt zu sein.

Wie erhalten Sie jetzt so ein Zertifikat, um S/MIME benutzen zu können? Wie wir oben schon besprochen haben, können Sie erst einmal mit einem Klasse-1-Zertifikat anfangen, um das Verfahren zu testen. Hierfür gibt es eine Reihe von kostenlosen Anbietern, beispielsweise Comodo[10]. Zertifikate für S/MIME haben übrigens das Format X.509, sodass Sie, wenn Sie weitere freie Anbieter finden wollen, im Zweifelsfall auch nach diesem Stichwort suchen können. Das Schlüsselpaar selbst wird von einer kryptografischen Funktion Ihres Webbrowsers generiert, nicht von der CA, denn sonst hätte diese ja Ihren privaten Schlüssel in der Hand. Wenn Sie das Zertifikat mit Ihrem Browser herunterladen, wird es je nach Browser entweder direkt im Schlüsselbund des Betriebssystems abgelegt, oder aber im Download-Ordner, wo Sie es dann von Hand aufrufen und dem Schlüsselbund hinzufügen können.

Sobald Sie ein Schlüsselpaar mit einem gültigen Zertifikat haben, können Sie anfangen, mit S/MIME verschlüsselte und signierte E-Mails zu verschicken.

Dass in vielen gängigen E-Mail-Clients S/MIME bereits unterstützt wird, ohne dass Sie zusätzliche Software installieren müssen, ist (noch) ein Vorteil von S/MIME. Die hierarchische Vertrauensstruktur, die das System voraussetzt und die wir oben erklärt haben, ist jedoch ein Nachteil und eine Schwachstelle. Aus diesem Grund rät auch Prism Break von der Nutzung von S/MIME generell ab[11]. Da die S/MIME-Option im bereits vorhandenen E-Mail-Client aber für manche Benutzer der erste Kontakt mit E-Mail-Verschlüsselung überhaupt ist, gehen wir hier auch kurz auf S/MIME ein.

4.7.2. S/MIME für Windows

Sowohl Microsoft Outlook als auch Mozilla Thunderbird unterstützen S/MIME bereits. Outlook greift für die Zertifikatsverwaltung auf den Windows-Schlüsselbund zurück, den Sie am einfachsten über den Internet Explorer aufrufen können (siehe Abbildung 4.12): EXTRAS > INTERNETOPTIONEN > INHALTE > ZERTIFIKATE. Alternativ gelangen Sie auch in die Windows-Zertifikatsverwaltung, wenn Sie in der Eingabeaufforderung certmgr.msc eingeben.

Abb. 4.12 Zertifikatsverwaltung im Internet Explorer

In dem Fenster, das sich nun öffnet (Abbildung 4.13), werden Ihnen zunächst Ihre eigenen Zertifikate angezeigt; in der Kopfleiste können Sie zwischen dieser Ansicht und der Liste der Zertifikate von anderen wechseln. Zudem können Sie hier Zertifikate importieren und exportieren.

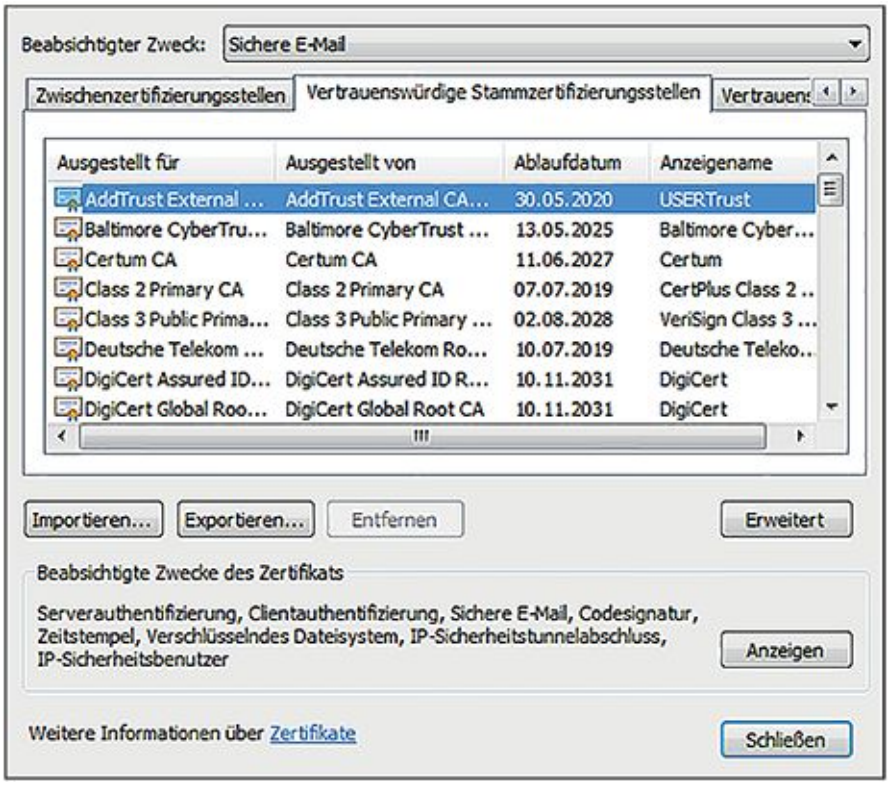


Abb. 4.13 Zertifikatsverwaltung unter Windows

Wenn Sie mithilfe des Internet Explorers Ihr Zertifikat erstellt haben, werden Sie im Verlaufe der Prozedur gefragt, ob Sie es direkt zur Schlüsselverwaltung hinzufügen wollen. Hier antworten Sie einfach mit Ja.

Wenn Sie nun das neu erstellte Zertifikat für S/MIME verwenden möchten, exportieren Sie es noch aus der Zertifikatsverwaltung (Schaltfläche EXPORTIEREN).

Um das exportierte Zertifikat dann unter Outlook auch verwenden zu können, starten Sie Outlook und navigieren zu DATEI > OPTIONEN > TRUST CENTER > EINSTELLUNGEN FÜR DAS TRUST CENTER und schließlich E-Mail-Sicherheit. Unter DIGITALE IDS und IMPORTIEREN/EXPORTIEREN öffnen Sie nun das Menü, in dem Sie die soeben exportierte Zertifikatsdatei angeben können. Outlook importiert dieses Zertifikat nun, und es steht Ihnen für S/MIME zur Verfügung. Wenn Sie eine neue E-Mail schreiben, können Sie nun unter OPTIONEN > SICHERHEITSEINSTELLUNGEN auswählen, dass diese signiert werden soll.

Um verschlüsselte E-Mails zu schreiben, müssen Sie noch das Zertifikat Ihres Kommunikationspartners importieren. Outlook genügt es dazu schon, wenn dieser Ihnen eine signierte E-Mail mit seinem Zertifikat geschickt hat. Das Einschalten der Verschlüsselung

erfolgt dann wie die Signierung über OPTIONEN > SICHERHEITSEINSTELLUNGEN beim Schreiben einer neuen E-Mail.

Die S/MIME-Verschlüsselung mit Thunderbird unter Windows funktioniert wie mit Thunderbird unter Linux – siehe nächster Abschnitt.

4.7.3. S/MIME für Linux

Auch in Thunderbird können Sie auf die schon eingebaute Unterstützung für S/MIME zurückgreifen, und auch hier müssen Sie dazu zunächst das generierte Zertifikat importieren (Abbildung 4.14). Dies geht über das Menü EXTRAS > KONTEN-EINSTELLUNGEN und SICHERHEIT:

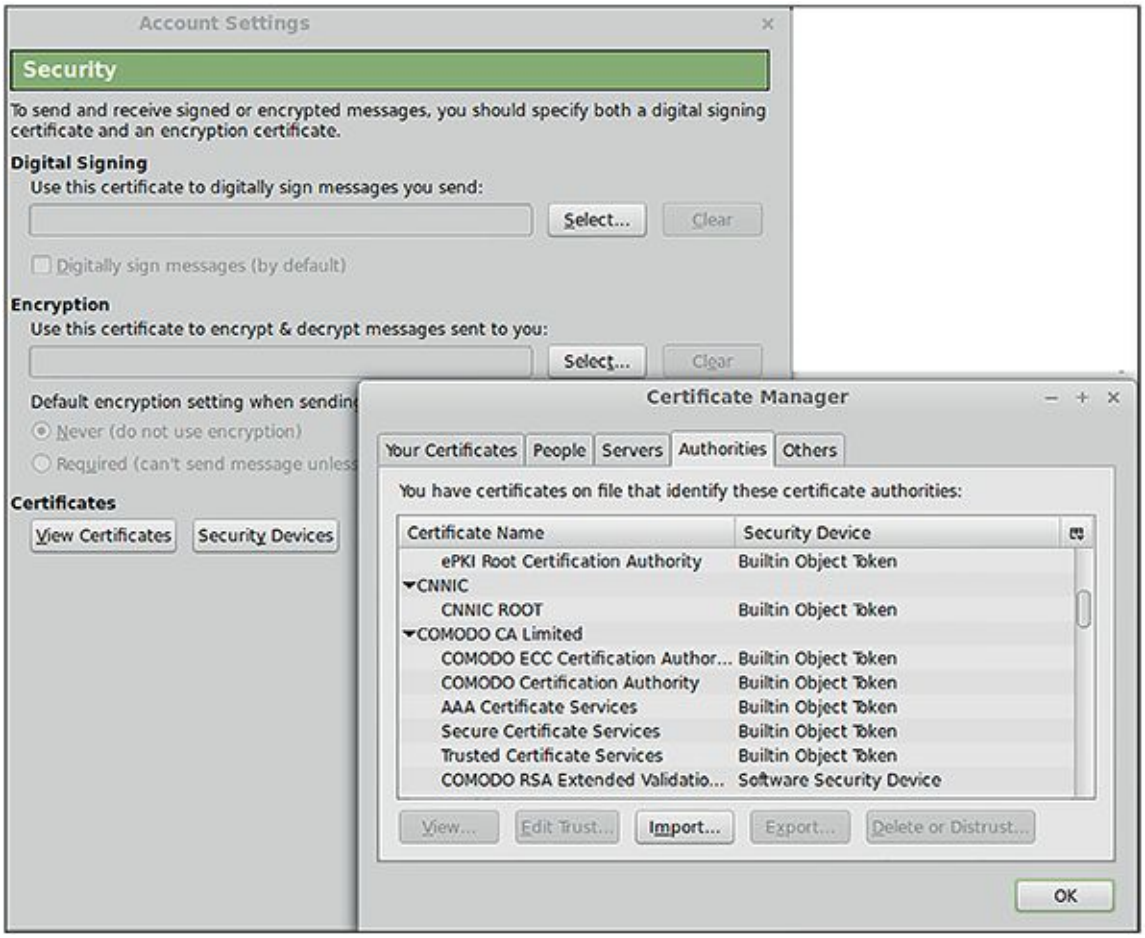


Abb. 4.14 Zertifikatsverwaltung in Thunderbird

Von diesem Fenster aus können Sie über ZERTIFIKATE ANZEIGEN (Tab IHRE ZERTIFIKATE) und den Button IMPORTIEREN dann Ihr Zertifikat in Thunderbird importieren.

Wenn Sie ein Zertifikat importiert haben, wird Ihnen im Menü EXTRAS > KONTEN-EINSTELLUNGEN für Ihr E-Mail-Konto oder Ihre Konten die Option angeboten, S/MIME zu konfigurieren. Dort können Sie dann das zuvor importierte Zertifikat AUSWÄHLEN und gleich auch einstellen, ob Sie standardmäßig mit S/MIME signieren und/oder verschlüsseln möchten.

Nachdem dieser Schritt abgeschlossen ist, können Sie beim Erstellen einer neuen E-Mail einfach über die Schaltfläche S/MIME am oberen Fensterrand die Verschlüsselung und/oder Signierung mit S/MIME veranlassen (Abbildung 4.15).

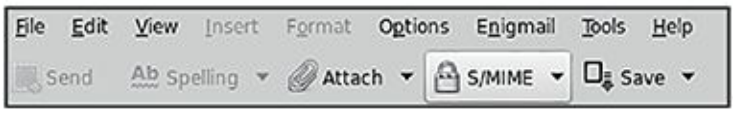


Abb. 4.15 S/MIME-Schaltfläche beim Erstellen einer neuen E-Mail in Thunderbird

Für die Verschlüsselung ist es notwendig, dass Sie das Zertifikat Ihres Gesprächspartners importiert haben. Dies geht am einfachsten, indem dieser Ihnen eine signierte E-Mail schickt.

4.7.4. S/MIME für OS X

Wenn Sie mithilfe von Safari ein Zertifikat bei einer CA erstellt haben, fügt der Browser es, ähnlich wie bei Windows, direkt zur Zertifikatsverwaltung des Betriebssystems hinzu. Sobald Sie im Besitz eines Zertifikats sind, können Sie in Apples nativem MailclientS/MIME aktivieren. Beim Erstellen einer neuen E-Mail (Abbildung 4.16) wählen Sie mittels der Schaltflächen auf der rechten Seite aus, ob Sie die E-Mail verschlüsseln und/oder signieren möchten:

Abb. 4.16 Neue verschlüsselte/signierte E-Mail in Apple Mail

Falls Sie auch eine PGP-Unterstützung installiert haben (wie weiter oben beschrieben), müssen Sie beim Erstellen einer neuen Mail zwischen beiden Systemen wählen (siehe Abbildung 4.17), da PGP und S/MIME miteinander inkompatibel sind und nur jeweils eines davon pro E-Mail verwendet werden kann.

Abb. 4.17 Auswahl zwischen PGP (falls installiert) und S/MIME in Apple Mail

Wenn Sie eine mit S/MIME verschlüsselte (Abbildung 4.18) oder signierte (Abbildung 4.19) E-Mail erhalten, sehen Sie das im Header der E-Mail unter dem Betreff.

Abb. 4.18 Symbol für verschlüsselte E-Mail in Apple Mail

Abb. 4.19 Symbol für signierte E-Mail in Apple Mail

4.8 Herausforderung sicheres E-Mailen auf dem Smartphone

Sichere E-Mail-Kommunikation auf dem Smartphone umzusetzen, ist bis heute ein schwieriges Thema. Im Gegensatz zu Laptop- und Desktop-PCs bringen die Betriebssysteme, die auf Smartphones laufen, sehr viele Einschränkungen der Benutzerrechte mit sich – für den normalen User ist es kaum möglich, vollständige Kontrolle über so ein System zu erhalten. Das bedeutet, dass Sie kaum Möglichkeiten haben, um sicher auszuschließen, dass jemand den privaten Key für Ihre verschlüsselte E-Mail-Kommunikation aus Ihrem Smartphone abzapft. Zum jetzigen Zeitpunkt ist es also leider noch so, dass wir E-Mail über das Smartphone per se als unsicher betrachten müssen. Zudem kommt hinzu, dass PGP- und S/MIME-Apps für Android und iOS dazu verleiten, auch private Keys per E-Mail zu versenden oder über unsichere Dienste wie Dropbox auf das Smartphone zu transferieren. Bitte laufen Sie nicht in diese Stolperfalle! Im Zweifelsfall ist es immer sicherer, das Schlüsselpaar *auf dem Smartphone zu generieren*.

Trotz aller Einschränkungen wollen wir ein paar gängige Apps für verschlüsseltes Mailen für Smartphones hier ansprechen.

4.8.1. PGP und S/MIME für Android

Die am weitesten fortgeschrittenen Lösungen für sicheres, verschlüsseltes Mailen auf einem Android-Smartphone sind die Apps Android Privacy Guard (APG) und OpenKeychain. Beide werden auch von Prism Break empfohlen, und beide benötigen als Basis den E-Mail-Client K9 Mail für Android.

K9 Mail[12] ist ein Open-Source-Client und kostenlos im Google Play Store herunterzuladen (siehe Abbildung 4.20). Als vollwertiger E-Mail-Client kann er auch ohne zusätzliche Verschlüsselungs-Apps verwendet werden.

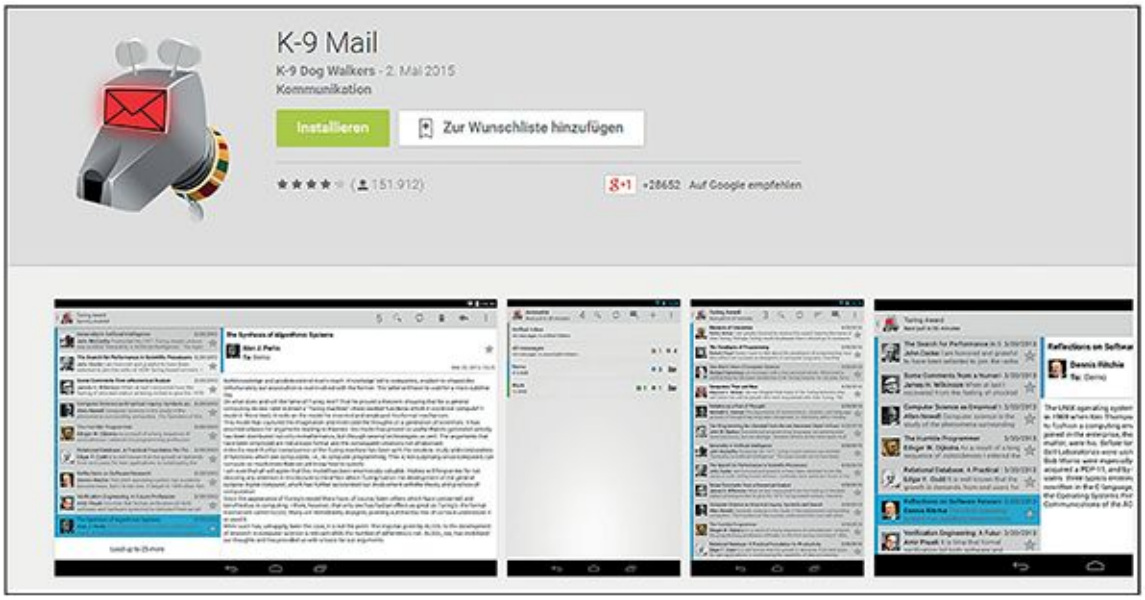


Abb. 4.20 K9 Mail für Android im Google Play Store

APG (kurz für Android Privacy Guard; siehe Abbildung 4.21) war ein Vorreiter auf dem Gebiet der E-Mail-Verschlüsselung für Android – die erste Version wurde schon 2010 veröffentlicht. Leider scheint es seit März 2014 keine Updates mehr gegeben zu haben[13], was für eine sicherheitsrelevante Software wenig vertrauenerweckend ist.

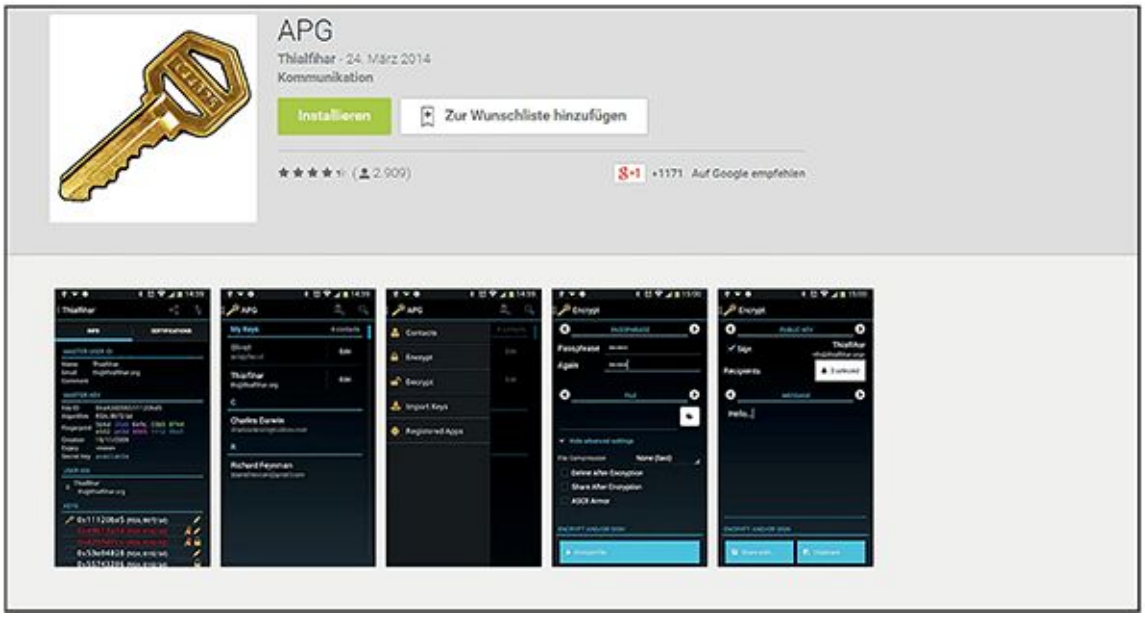


Abb. 4.21 APG (Android Privacy Guard) im Google Play Store

Bevor APG in der Versenkung verschwunden ist, hat es sich aber sozusagen noch fortgepflanzt: Aus einer früheren Version von APG ist die ebenfalls quelloffene Software OpenKeychain entstanden, die von einer aktiven Community stetig weiterentwickelt wird (Stand Juli 2015). OpenKeychain (siehe Abbildung 4.22) basiert auf OpenPGP und übernimmt die Schlüsselverwaltung sowie die Ver- und Entschlüsselung von E-Mails in K9 Mail. Die Grundfunktionen werden ergänzt durch einige praktische Features wie Austausch von öffentlichen Schlüsseln per Scan von QR-Codes oder Near Field Communication (ein ähnlicher Standard wie Bluetooth, allerdings mit einem maximalen Abstand von etwa zehn Zentimetern zwischen Geräten).

Schließlich empfiehlt auch Prism Break[14] OpenKeychain in Kombination mit K9 Mail als Lösung für die Verschlüsselung von E-Mails auf Android-Geräten (siehe Abbildung 4.22). Da zudem die Bedienung von OpenKeychain deutlich einfacher ist als die von APG, ist OpenKeychain im Moment das Mittel der Wahl, wenn Sie die Verschlüsselung von E-Mails auf Ihrem Android ausprobieren möchten. Behalten Sie aber im Hinterkopf, dass dabei nicht das gleiche Sicherheitsniveau wie auf Ihrem Laptop- oder Desktop-Computer erreicht wird.

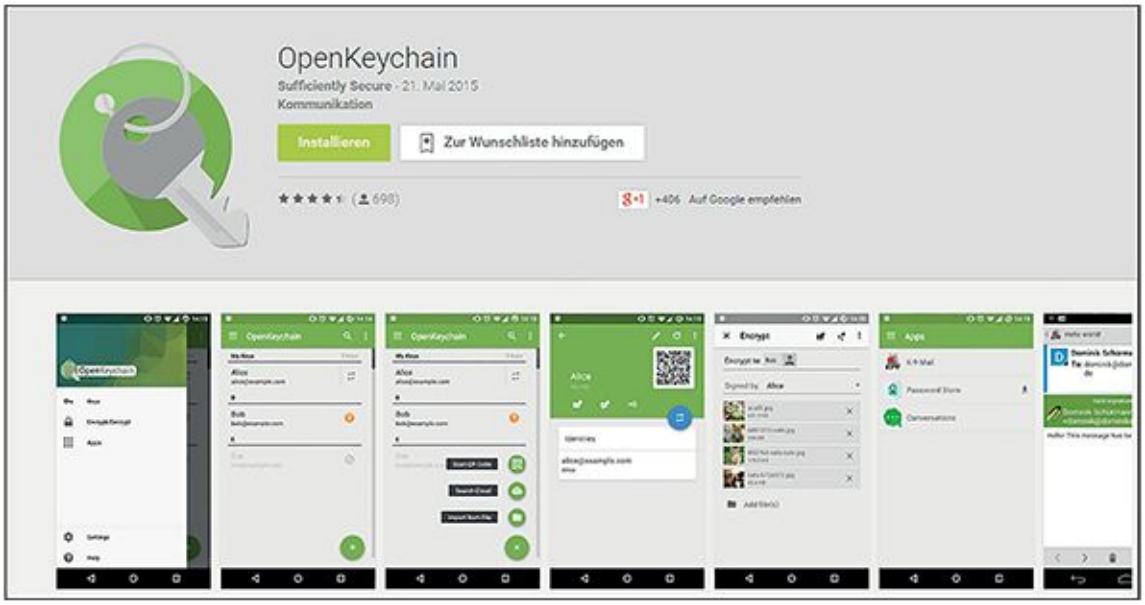


Abb. 4.22 OpenKeyChain für Android

OpenKeychain unterstützt zwar im Prinzip auch S/MIME – der E-Mail-Client K9 Mail jedoch leider noch nicht. Wenn Sie S/MIME unter Android probieren wollen, sollten Sie daher auf einen neuen E-Mail-Client umsteigen, beispielsweise den kostenpflichtigen R2Mail2[15] (Abbildung 4.23) von einem Wiener Entwicklerteam (erhältlich beispielsweise ebenfalls über den Google Play Store). Zum Testen stellt das Team eine kostenlose Version zur Verfügung, die aber nur die letzten zehn Mails anzeigt.

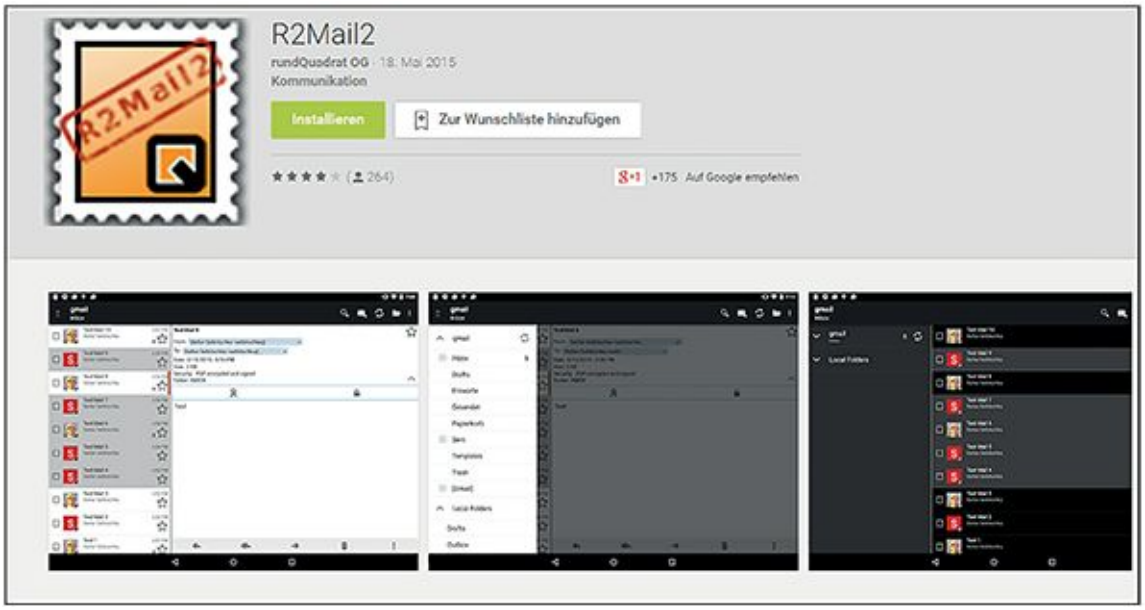


Abb. 4.23 R2Mail2 für Android

4.8.2. PGP und S/MIME für iOS

Für iOS gilt unsere obige Warnung, sich nicht auf die Sicherheit der Verschlüsselung von E-Mails zu verlassen, ganz besonders: Im Gegensatz zu Android handelt es sich bei iOS darüber hinaus um ein Closed-Source-Betriebssystem, das dem Benutzer noch weniger Einblick in die »Eingeweide« des Systems und somit in dessen Sicherheit gestattet. Mit diesem Disclaimer im Hinterkopf schauen wir uns einmal an, welche Apps für Mailverschlüsselung unter iOS zur Verfügung stehen.

Für iPhone und iPad gibt es ebenfalls Implementationen des OpenPGP-Standards. Die vermutlich am meisten genutzte ist die App iPGMail[16] (siehe Abbildung 4.24). Die App bietet alle Funktionen an, die zum komfortablen Nutzen von PGP notwendig sind, also Schlüsselgenerierung, Austausch mit Schlüsselservern, Versenden des öffentlichen Schlüssels per Mail und natürlich Ver- und Entschlüsseln und Signieren von E-Mails. Leider ist iPGMail Closed Source, sodass seine Sicherheit nicht von der Öffentlichkeit beurteilt werden kann.

Etwas weniger einfach in der Benutzung, aber dafür Open Source, ist oPenGP[17] von Grégory Descamps. Hier gab es allerdings schon seit November 2014 kein Update mehr, sodass man im Auge behalten muss, ob die Software aktiv weiterentwickelt wird und Sicherheitslücken kontinuierlich behoben werden können.

Abb. 4.24 iPGMail für iOS

Insgesamt sind die Möglichkeiten zur PGP-Verschlüsselung unter iOS also noch sehr unbefriedigend. Auch in Bezug auf PGP unter iOS lohnt es sich aber, ein Auge auf die Entwicklung von Pretty Easy Privacy (PEP) zu halten – siehe auch weiter oben in diesem Kapitel. Zurzeit (Stand September 2015) wird die iOS-Version von einem kanadischen Kooperationspartner des PEP-Projekts entwickelt, ist aber noch nicht für die Öffentlichkeit verfügbar. Sie beruht auf NetPGP, einer Alternative zu GnuPG.

Für S/MIME benötigen Sie keine zusätzliche Software unter iOS – dieser Standard wird vom eingebauten Client »Mail« bereits unterstützt. Nach Import eines öffentlichen Zertifikats Ihres Kommunikationspartners bietet Mail Ihnen die Möglichkeit, im Fenster zum Erstellen einer neuen E-Mail die Verschlüsselung per S/MIME ein- und auszuschalten, und zeigt Ihnen mittels eines Symbols in der Kopfzeile an, ob eine E-Mail verschlüsselt und/oder signiert ist.

[1] also mit zeitlich versetztem Senden und Empfangen von Nachrichten

[2] Das Internet-Orakel gibt es wirklich – besuchen Sie es mal auf www.fritriac.de/orakel.

[3] https://posteo.de

[4] https://www.mailvelope.com

[5] https://posteo.de

[6] https://posteo.de/site/verschluesselung

[7] http://pep-_project.org

[8] www.gpg4win.de

[9] https://gpgtools.org

[10] www.comodo.com

[11] https://prism-_break.org/de/subcategories/android-_email-_encryption/

[12] https://github.com/k9mail/k-_9/

[13] http://www.thialfihar.org/projects/apg/

[14] https://prism-_break.org

[15] https://r2mail2.com/

[16] https://ipgmail.com/

[17] https://itunes.apple.com/de/app/opengp/id414003727

Kapitel 5 Sicheres Chatten, Instant Messaging und SMS

5.1 Quatschen digital – die Basics

Das Medium, mit dem seit den 90er-Jahren Milliarden von Verabredungen getroffen, zahlreiche neue Wörter kreiert und gerüchteweise auch die eine oder andere Beziehung beendet wurde, startete als Abfallprodukt der Mobilfunktechnologie.

Der deutsche Ingenieur Friedhelm Hillebrand von der Bundespost und sein französischer Kollege Bernard Ghillebaert entwarfen in den 80er-Jahren ein Konzept für einen Kurznachrichtendienst, der auf einem weitgehend ungenutzten Kanal im Mobilfunk aufbaute. Über diesen sollten ursprünglich im GSM-Netz Störungsmeldungen versendet werden. Anfangs kostenlos für die Nutzer, bemerkten die Telefongesellschaften bald das geschäftliche Potenzial und führten Gebühren für die Nutzung des *Short Message Service* (SMS)ein. Dies hielt vor allem Jugendliche nicht davon ab, nach und nach fast ihr ganzes soziales Leben über diesen Kurznachrichtendienst zu organisieren. Als der sogenannte »SMS-Daumen«[1] dann in der ersten Dekade des 21. Jahrhunderts Eltern und Medien beschäftigte, hatte sich das Thema SMS fast schon wieder erledigt. Bald darauf begann mit der Einführung des iPhones der Siegeszug des Smartphones. 2009 besiegelte das Erscheinen von *WhatsApp* und weiterer neuer Instant-Messaging-Dienste das Ende der einstigen Cashcow.

WhatsApp und seine Konkurrenten erhoben keine Gebühren für einzelne Nachrichten und punkteten vor allem mit zusätzlichen Funktionen, die SMS, schon alleine wegen der Beschränkung auf 160 Zeichen, niemals hätte abbilden können.

Parallel zur SMS entwickelte sich in den späten 80er-Jahren das Chatten im damals noch jungen Internet. Eine der ersten Chatplattformen, wie wir sie heute kennen, war beispielsweise der *IRC*[2] (Internet Relay Chat). Im IRC tummelten sich zunächst überwiegend Computerenthusiasten, da die Nutzung des Chatnetzwerkes Kenntnisse erforderte, die vor der Ära des billigen Heimcomputers nicht viele Menschen besaßen. Mit dem AOL-Chat, den der gleichnamige Internetanbieter in den 90er-Jahren als festen Bestandteil seiner Zugangssoftware anbot, wurde das Chatten auch für den durchschnittlichen Internetnutzer

attraktiv. Auch hier waren übrigens, wie wenige Jahre später bei der SMS, Jugendliche die Vorreiter.

Um die Jahrtausendwende herum hatten einige Unternehmen erkannt, dass sich mit Chatten auch Geld verdienen lässt, beispielsweise durch Werbeeinblendungen und bezahlte Zugänge. Beliebte Chatportale dieser Zeit waren in Deutschland unter anderem der Spin-Chat[3] und Knuddels[4], die übrigens beide bis heute existieren. Daneben entwickelte sich das sogenannte *Instant Messaging*. Über Internetdienste und entsprechende Desktop-Clients verschiedenster Anbieter (zum Beispiel Yahoo und Microsoft) konnten und können die Nutzer sich gegenseitig Nachrichten direkt auf ihren virtuellen Schreibtisch schicken. Dabei waren bei den meisten Systemen auch Gruppenchats nach dem Vorbild der Chatportale möglich.

Mit der nahezu flächendeckenden Verfügbarkeit von mobilen Internetzugängen und dem Auftauchen der ersten Smartphones um 2008 herum wollten viele Menschen nun auch von ihrem Telefon aus chatten. Textnachrichten über das Internet auszutauschen war schlichtweg billiger, als teure SMS zu versenden. Zudem fiel die lästige Begrenzung auf 160 Zeichen weg.

Ein wichtiger Grund, weshalb Chat und Instant Messaging bisher nicht einfach wieder in der Versenkung verschwanden, sondern immer wieder erfolgreich angepasst wurden, ist folgender:

Die ständige Erreichbarkeit mittels Internet und Mobilfunk wird durch derartige Dienste wieder auf ein handhabbares Maß zurückgestutzt. Wenn Sie immer gerade dann einen Anruf erhielten, wenn Sie theoretisch erreichbar sind, könnten Sie sich auf nichts anderes mehr konzentrieren. Sie würden keine einzige Aufgabe mehr zu Ende bringen, geschweige denn sich entspannen. Wenn Sie umgekehrt für jede kurze Information oder Rückfrage versuchen müssten, Ihren Kommunikationspartner telefonisch zu erreichen, (während dieser vielleicht bereits telefoniert, unter der Dusche steht oder gerade eingeschlafen ist), wäre das mindestens genau so frustrierend.

Mit Instant Messaging können Sie hingegen Nachrichten absetzen und eingetroffene Mitteilungen lesen, wann es Ihnen beliebt. Und trotzdem fühlt sich das Ganze dabei nicht so zäh und aufwendig wie E-Mail oder die Briefpost an. Der Anwendungsfall von Instant Messaging liegt also zwischen dem stark asynchronen Austausch von langen Textnachrichten wie E-Mail und der Echtzeitkommunikation am Telefon. Zudem wird der Informationsaustausch in einer größeren Gruppe von Menschen durch die bereits angesprochenen Gruppenchats stark

vereinfacht. Jeder, der schon mal eine Telefonkonferenz mit vier oder mehr undisziplinierten Teilnehmern überstehen musste, weiß das zu schätzen.

Auch wenn die Grenzen zwischen mobiler (Smartphone) und stationärer (Laptop- oder Desktop-Computer) Nutzung von Instant-Messaging-Diensten immer mehr verschwimmen, werden wir diese dennoch getrennt voneinander behandeln. Im Hinblick auf einige Sicherheitsaspekte besteht hier nämlich nach wie vor ein eklatanter Unterschied. Wie bereits an anderer Stelle dieses Buches (beispielsweise im E-Mail-Kapitel) erwähnt, haben Sie das Betriebssystem Ihres Computers (noch) völlig unter Ihrer Kontrolle, wenn Sie das wollen. Bei Ihrem Smartphone ist das in den meisten Fällen ohne erheblichen Aufwand und unter Verlust der Herstellergarantie nicht möglich.

5.2 Von Laptop zu Laptop

Zunächst schauen wir uns die Möglichkeiten des Chattens und Instant Messagings zwischen zwei Computern an – statt Laptops können natürlich auch Desktop-Computer beteiligt sein.

5.2.1. Grüße aus den 90ern – ICQ und AIM

Einer der ersten weltweit verbreiteten Instant-Messaging-Clients war *ICQ*[5]. Wenn man das Akronym auf Englisch ausspricht, klingt es wie »I seek you«, also »ich suche dich«. Auf diesem Wortspiel basiert der Name des Dienstes.

ICQ wurde 1996 von der kleinen israelischen Firma Mirabilis entwickelt und 1998 vom damaligen Internetriesen AOL[6] aufgekauft. Seit 2010 gehört es dem russischen Unternehmen Mail.ru[7]. Auch wenn es einen Großteil der ursprünglichen Nutzer verloren hat, existiert ICQ bis heute und bietet mittlerweile auch Clients für Smartphones sowie Videotelefonie an.

Die Benutzer von ICQ wurden von Anfang an mit eindeutigen, fortlaufenden Nummern identifiziert, den sogenannten *Unique Identification Numbers*. Nutzer der ersten Stunde hatten noch sechsstellige Nummern, mittlerweile sind die Nummern neunstellig (darunter jedoch sicherlich viele Karteileichen, da ungenutzte Nummern nicht gelöscht werden können).

ICQ funktioniert über ein Netzwerkprotokoll namens *OSCAR*. Auch der *AOL Instant Messenger* (AIM) arbeitete auf Basis dieses Protokolls, sodass die Benutzer der beiden Programme seit dem Kauf von ICQ durch AOL auch mit Nutzern der jeweils anderen Plattform Nachrichten austauschen konnten.

Die offizielle ICQ-Software ist nicht quelloffen, und die Kommunikation über ICQ wird nicht verschlüsselt. In seinen Lizenzbedingungen verbietet ICQs derzeitiger Besitzer Mail.ru ausdrücklich, seinen Dienst über andere Clients als offiziell durch ICQ lizensierte zu benutzen. Das Gleiche gilt für den AOL Instant Messenger. Trotzdem gibt es einige alternative Clients, die teilweise sogar quelloffen sind. Seit 2008 ist das OSCAR-Protokoll ebenfalls quelloffen.

Vor dieser Zeit mussten die Entwickler besagter Fremdlösungen das ICQ und AIM zugrunde liegende Protokoll mittels sogenanntem *Reverse Engineering* aufschlüsseln, um es überhaupt verstehen und nutzen zu können. Stark vereinfacht heißt das: Durch Beobachtung des Verhaltens und der Struktur der originalen, proprietären Clients wurde abgeleitet, wie das OSCAR-Protokoll genau aussieht und wie man es verwenden kann.

ICQ, AIM, Skype und der Yahoo Messenger sind einige der derzeit größten proprietären Instant-Messenger-Dienste. Alle Originalclients für diese Netzwerke sind proprietäre Software und damit nicht nur intransparent, sondern aufgrund mangelnder Prüfungsmöglichkeiten durch unabhängige Experten und die Öffentlichkeit auch tendenziell unsicherer als Open-Source-Alternativen.

Hier kann allerdings Abhilfe geschaffen werden: Es gibt mittlerweile eine ganze Menge alternativer Instant-Messaging-Clients und -Dienste für nahezu jedes mobile und stationäre Betriebssystem (siehe Tabelle 5.1). Viele davon sind frei und quelloffen, und die meisten unterstützen viele verschiedene Protokolle und können eine beliebige Anzahl von IM-Accounts gleichzeitig verwalten. Viele unterstützen außerdem die Verschlüsselung von eigentlich unsicheren Chatprotokollen mittels OTR, auf das wir später noch genauer eingehen werden, oder implementieren andere brauchbare Verschlüsselungsverfahren.

Ein Protokoll, das anders als OSCAR & Co. von Anfang an quelloffen war und mittlerweile mit seiner weiten Verbreitung alles andere als ein Nischenprodukt ist, ist XMPP oder Jabber. Es wird von allen in der Tabelle genannten Clients unterstützt, und wir wollen es im Folgenden ein bisschen näher beleuchten.

5.2.2. XMPP/Jabber

XMPP (Extensible Messaging and Presence Protocol, früher als *Jabber* bekannt) ist ein freies Instant-Messaging-Protokoll. Es wird seit 1998 entwickelt und ähnelt vom Prinzip her der guten alten E-Mail. Bei XMPP wird ein Benutzer nicht, wie bei ICQ, durch eine Nummer

identifiziert, sondern durch eine Adresse, die einer E-Mail-Adresse täuschend ähnlich sieht, aber als Jabber-ID bezeichnet wird (zum Beispiel alice@jabber.org).

Tabelle 5.1 Alternative quelloffene IM-Clients

Client	Betriebssystem	Kommentar
Miranda www.miranda-im.org	Windows	Entwicklung der deutschen Version[8] wurde eingestellt
Kopete https://userbase.kde.org/Kopete	Linux (KDE)	Deutschsprachige Dokumentation[9] vorhanden
Jitsi https://jitsi.org	alle (Java-basiert)	Dokumentation noch lückenhaft, enthält aber unter anderem Anleitungsvideos[10]; leider nur englischsprachig
Pidgin https://pidgin.im	Linux (Gnome), Windows	Englischsprachige Doku[11], aber deutsche Version des Clients (kann bei Installation gewählt werden)
Adium https://www.adium.im	OS/X	Basiert auf den gleichen Bibliotheken wie Pidgin; englischsprachige Doku[12] und Videos
ChatSecure https://chatsecure.org	iOS und Android	Etwas sparsame englischsprachige Doku; mit Tor-Support[13]
Xabber www.xabber.com	Android	

Auch die Zustellung der Nachrichten verläuft ähnlich: Wenn Sie Alice eine Nachricht schicken wollen, reichen Sie diese zunächst an den XMPP-Server weiter, an dem Sie angemeldet sind. Wenn dieser derselbe ist, auf dem auch Alice ihr Konto hat, gibt er die Mitteilung direkt an Alice weiter. Hat Alice dagegen ihr Konto bei einem anderen Anbieter (vielleicht sogar bei ihrem eigenen XMPP-Server), ermittelt Ihr Server zunächst, welcher XMPP-Server für die Verarbeitung der Nachricht zuständig ist. Das geschieht wie bei der E-Mail auch mithilfe des Hostanteils von Alices Jabber-ID (jabber.org). Die Mitteilung wird dann an Alices Server weitergeleitet, und dieser stellt sie wiederum an Alice zu.

XMPP ist, wie der vollständige Name schon andeutet, nahezu beliebig erweiterbar. Eine solche Erweiterung stellt das von Google entwickelte Protokoll *Jingle* dar. Es ist quelloffen und ermöglicht es, sogenannte *Peer-to-peer-Datenverbindungen* zwischen zwei Chatpartnern auszuhandeln. Diese können wiederum für den Austausch eines Datenstroms zwischen diesen zwei Punkten genutzt werden, beispielsweise für einen Video- oder Audiochat.

XMPP unterstützt zudem sogenannte Transports. Diese machen es möglich, dass XMPP-Nutzer mit Teilnehmern anderer Netzwerke, beispielsweise ICQ/AIM, Facebook oder Google Hangouts, kommunizieren können.

Wenn Sie, wie die meisten von uns, keinen eigenen Server im Keller stehen haben, können Sie sich einen XMPP-Account auch bei einem kostenlosen Anbieter besorgen. Hier empfiehlt sich zum Beispiel www.jabber.de (unter ANMELDUNG).

Eine Reihe anderer kostenloser und öffentlicher XMPP-Server haben in letzter Zeit die Registrierung neuer Accounts eingestellt, beispielsweise www.jabber.org und jabber.ccc.de – Letztere unter anderem mit der Begründung[14], dass auch andere Menschen und Institutionen ermutigt werden sollten, eigene XMPP-Server zu eröffnen.

Auf https://xmpp.net/directory.php finden Sie eine Liste noch vorhandener öffentlicher XMPP-Server mit einer kurzen Bewertung der jeweiligen Sicherheit. Auch eine Reihe von Universitäten[15] bieten kostenlose XMPP-Accounts für ihre Mitarbeiter und Studierenden an.

Wie bei E-Mail ist die Verschlüsselung, wie Sie sehen, bei dieser Vorgehensweise nicht von vornherein eingebaut. Die Zustellung einer Nachricht erfolgt erst einmal im Klartext. 2014 haben sich jedoch die Betreiber der größten XMPP-Server darauf geeinigt, dass zwischen ihren Systemen stets eine Transportverschlüsselung mittels TLS vorgenommen wird.

Die Verschlüsselung von XMPP-Nachrichten kann, Sie haben es sich vielleicht schon gedacht, ebenfalls analog zur E-Mail erfolgen. Jabber unterstützt wie E-Mail die Transportverschlüsselung zwischen Client und Server, beziehungsweise zwischen Server und Server mittels TLS. Eine Ende-zu-Ende-Verschlüsselung kann theoretisch ebenfalls mit PGP erfolgen. Allerdings sind IM-Clients, die PGP nativ beherrschen oder bei denen sich diese Funktionalität durch Add-ons nachrüsten lässt, dünn gesät. Der Hauptgrund hierfür ist wohl, dass der dafür verantwortliche Standard (XEP-0027) seit 2014 nicht mehr weiterentwickelt wird. Die XMPP Foundation[16] empfiehlt ausdrücklich, keine Funktionalitäten mehr auf diesem Entwurf aufzubauen.

Für die zuverlässige Verschlüsselung von Instant Messaging hat sich stattdessen überwiegend das sogenannte *Off-the-Record*-Messaging-Protokoll (OTR) durchgesetzt. OTR lässt sich nicht nur mit XMPP verwenden. Solange Ihr Client diesen Mechanismus unterstützt, können Sie ihn zur Verschlüsselung eines beliebigen IM-Protokolls (zum Beispiel auch AIM/ICQ) verwenden.

5.2.3. Dieses Gespräch hat nicht stattgefunden – Off-the-Record-Messaging (OTR)

Alle weiter oben genannten Formen des Chattens sind wie Gespräche, die Sie mit einem Freund in einer vollen U-Bahn führen. Meistens haben Sie zwar keinen Grund anzunehmen, dass jemand Sie speziell abhört – wenn ein Lauscher sich allerdings genau das in den Kopf gesetzt hat, ist es für ihn nicht besonders schwer.

Was Sie in diesem Falle benötigen, ist also das elektronische Äquivalent zu einem geflüsterten Gespräch unter Freunden. Es gibt keine Zeugen und keine Möglichkeit, hinterher nachzuweisen, was gesprochen wurde (falls sich herausstellt, dass der Freund doch kein so guter Freund ist).

Ein Gespräch, das inoffiziell oder »nicht fürs Protokoll« geführt wird, wird auf Englisch als »off the record« bezeichnet. Die entsprechende Form des Chats heißt deswegen *Off-the-Record-Messaging* oder *OTR*.

Bei OTR ist der Inhalt nach Ende des Chats nicht mehr zu rekonstruieren. Dazu ist es notwendig, den symmetrischen Schlüssel, der zur Codierung der einzelnen Nachrichten verwendet wird, nach Ende der Unterhaltung zu zerstören.

Damit kennen Sie nun schon die erste Voraussetzung, die erfüllt sein muss, damit ein Gespräch OTR ist: *Perfect Forward Secrecy*, also perfekte Geheimhaltung »in die Zukunft«. Das bedeutet, dass eine Entschlüsselung im Nachhinein verhindert wird, auch wenn private Schlüssel der Kommunikationsteilnehmer gestohlen werden.

Die restlichen Voraussetzungen, die für OTR erfüllt sein müssen, sind:

- Ende-zu-Ende-Verschlüsselung
- Authentifizierung der Gesprächsteilnehmer
- Abstreitbarkeit des Gesprächs und der Gesprächsinhalte

Ein wesentlicher Nachteil von OTR ist, dass es nur zur synchronen Kommunikation geeignet ist. Das bedeutet, dass beide Gesprächspartner gleichzeitig online sein müssen. Bei Instant Messaging ohne OTR werden dagegen, wenn nur ein Gesprächspartner online ist (oder Empfang hat), dem anderen die »verpassten« Nachrichten zugestellt, sobald er ebenfalls wieder online ist (Empfang hat). Mit OTR ist dies nicht möglich – verpasste Nachrichten sind verloren.

5.2.3.1 OTR mit Pidgin unter Linux oder Windows

Pidgin ist ein IM-Client für Linux und Windows, der eine Vielzahl von Messaging-Protokollen benutzt. Wenn Sie ihn mit einem Protokoll verwenden, das OTR unterstützt, können Sie vertrauliche und im Nachhinein abstreitbare Unterhaltungen mit anderen OTR-Nutzern führen. Konkret zeigen wir dies am Beispiel von XMPP.

Um OTR in Pidgin zu verwenden, können Sie das gleichnamige Plug-in verwenden. Dieses müssen Sie nicht extra herunterladen, sondern können es bequem von Pidgin aus installieren. Gehen Sie dazu im Menü Tools auf den Menüpunkt Plug-ins.

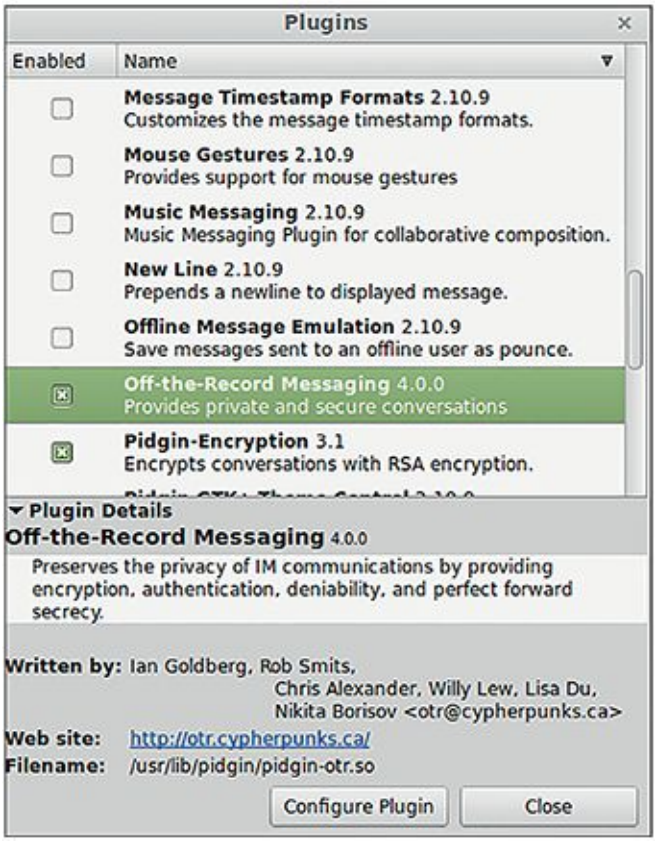


Abb. 5.1 Details des OTR-Plug-ins für Pidgin

Wenn Sie das Plug-in installiert haben und dann markieren, öffnet sich ein Menü, in dem Sie es konfigurieren können (Abbildung 5.1). Dort können Sie auch Ihr Schlüsselpaar generieren. Klicken Sie also bitte auf CONFIGURE PLUGIN.

Es öffnet sich daraufhin ein Fenster, in dem Sie sehen, ob Sie bereits im Besitz eines Schlüsselpaares sind (wenn Sie OTR gerade erst installiert haben, wird dies nicht der Fall sein), und weitere Einstellungen festlegen können (Abbildung 5.2).

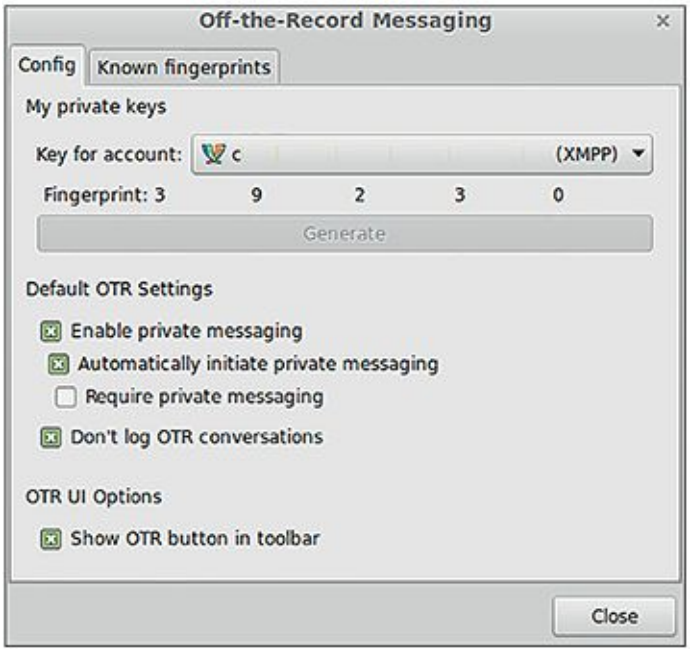


Abb. 5.2 Einstellungen des OTR-Plug-ins für Pidgin

Mit einem Klick auf das Feld NOT PRIVATE öffnet sich ein Kontextmenü, in dem Sie dann START A PRIVATE CONVERSATION auswählen können (siehe Abbildung 5.3).

Abb. 5.3 Anzeige des OTR-Konversationsstatus in Pidgin

Wenn der Gesprächspartner ebenfalls OTR nutzt und Ihre Anforderung nach einer OTR-Konversation annimmt, wird daraufhin eine solche gestartet. Darüber werden Sie durch eine Meldung im Chat-Fenster informiert. Wenn Sie Ihren Gesprächspartner noch nicht authentifiziert haben, ändert sich die Anzeige im Feld NOT PRIVATE daraufhin zu UNVERIFIED. Die Authentifizierung kann auf drei verschiedene Arten erfolgen. Diese werden Ihnen zur Auswahl angeboten, wenn Sie auf UNVERIFIED und dann auf AUTHENTICATE BUDDY klicken:

- *Frage und Antwort* (question and answer): Pidgin stellt Ihrem Gesprächspartner eine Frage, die Sie eingegeben haben und deren Antwort im Idealfall nur Sie beide kennen. Wenn er die Frage richtig beantwortet, ist seine Identität damit authentifiziert.

- *Geteiltes Geheimnis* (shared secret): Das gleiche Prinzip, nur dass die Frage wegfällt und Sie und Ihr Gesprächspartner einfach die gleiche Zeichenkette eingeben müssen – das »Geheimnis«, das nur Sie beide kennen (und das Sie beispielsweise vorher persönlich oder telefonisch vereinbart haben oder schon von vorherigen Konversationen kennen).
- *Manuelle Fingerabdruck-Verifikation* (manual fingerprint verification): Hierbei müssen Sie beide jeweils eine Kette von Zahlen und Buchstaben mit dem anderen abgleichen, den Fingerabdruck des Schlüssels des anderen. Dies sollte durch einen unabhängigen, sicheren Kommunikationskanal erfolgen, beispielsweise telefonisch oder per verschlüsselter E-Mail.

Wenn dieser Schritt geschafft ist, wechselt die Anzeige zu PRIVATE – Sie haben jetzt eine vertrauliche und im Nachhinein abstreitbare Unterhaltung (siehe Abbildung 5.4).

Abb. 5.4 Private Konversation mit OTR in Pidgin

Eine Alternative zu Pidgin unter Windows, wenn Sie OTR benutzen wollen, ist der Client Miranda[17], den wir weiter oben schon kurz angesprochen haben. Hier sollen die Benutzerzahlen in letzter Zeit aber abgenommen haben, sodass fraglich ist, wie lange diese Software noch weiterentwickelt wird.

5.2.3.2 OTR mit Adium unter OS X

Adium ist ein enger Verwandter von Pidgin und daher in Ausstattung und Handhabung recht ähnlich. Im Gegensatz zu Pidgin muss aber OTR in Adium nicht separat durch ein Add-on aktiviert werden, sondern ist ohne zusätzlichen Aufwand einsatzfähig.

Die Konfiguration für OTR finden Sie in den Einstellungen von Adium (DATEI > EINSTELLUNGEN, siehe auch Abbildung 5.5) unter dem Reiter ERWEITERT.

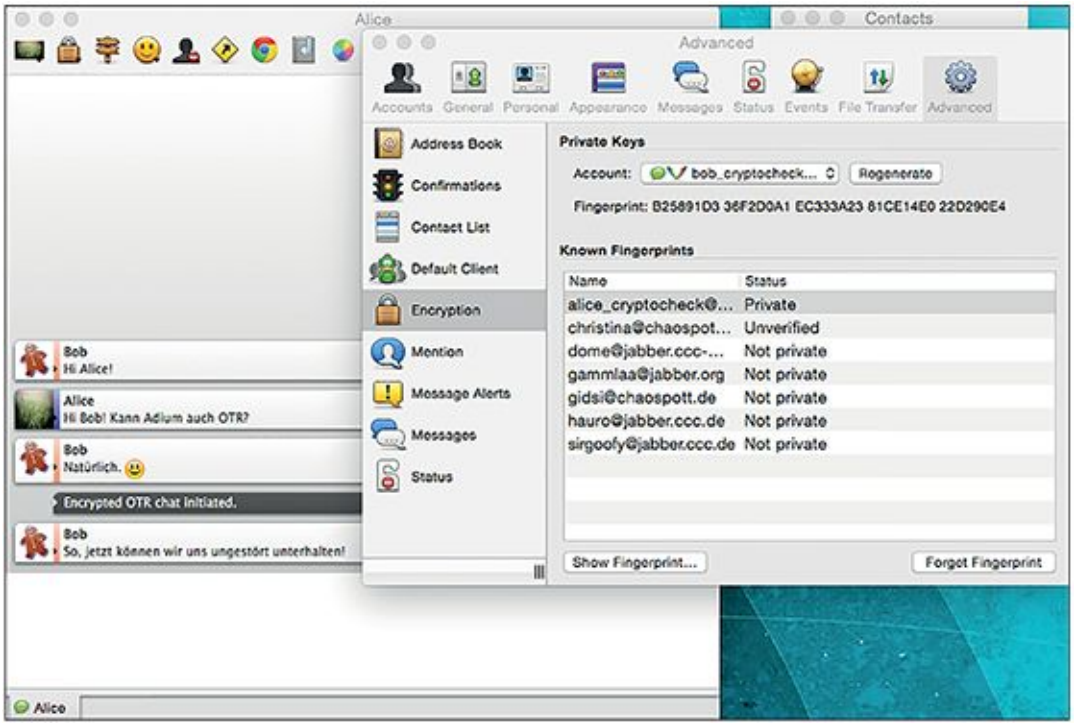


Abb. 5.5Konfiguration von Adium

Dort können Sie Ihren privaten Schlüssel generieren lassen oder diesen neu erstellen, wenn Sie schon einen haben. Zudem werden Ihnen hier die öffentlichen Schlüssel, die Sie bereits von Ihren Chatpartnern erhalten haben, und deren Status angezeigt.

Wenn Sie jetzt eine Konversation mit einem Chatpartner starten, der bereits OTR einsetzt, sollte automatisch eine verschlüsselte Verbindung hergestellt werden. Falls das nicht passiert, können Sie es manuell über das Schloss-Symbol in der Menüleiste des Chatfensters veranlassen (Abbildung 5.6).

Abb. 5.6 OTR-Konversation in Adium manuell starten

Falls Sie hiermit zum ersten Mal eine OTR-Session zu Ihrem Gegenüber aufbauen, wird Ihnen und dem Kontakt nun ein Dialog zur Verifizierung des öffentlichen Schlüssels (also Authentifizierung des Gesprächspartners) angezeigt. Falls das nicht automatisch geschieht, können Sie es über das Schloss-Symbol und den Menüpunkt VERIFIZIEREN nachholen (Abbildung 5.7).

Abb. 5.7 Verifikation des öffentlichen Schlüssels des Gesprächspartners in Adium

Im Gegensatz zu Pidgin, das auch Verifikation über Frage und Antwort oder ein geteiltes Geheimnis anbietet (siehe oben), unterstützt Adium bisher nur die manuelle Verifikation des Fingerabdrucks des Schlüssels. Der Vertrauensstatus eines Chatpartners wird Ihnen übrigens nicht (wie bei Pidgin) direkt im Chatfenster angezeigt – Sie können ihn stattdessen über den Konfigurationsdialog von OTR und die dortige Auflistung der bekannten Schlüssel prüfen.

Wenn der Gesprächspartner nun ebenfalls OTR verwendet und seinerseits die verschlüsselte Verbindung bestätigt, haben Sie nun die Möglichkeit, sich vertraulich und abstreitbar mit ihm zu unterhalten.

Wenn Sie möchten, können Sie auch veranlassen, dass OTR *immer* initiiert wird, wenn der Chatpartner das Protokoll ebenfalls unterstützt. Dies lässt sich in den Verschlüsselungsoptionen (siehe Abbildung 5.8) einstellen.

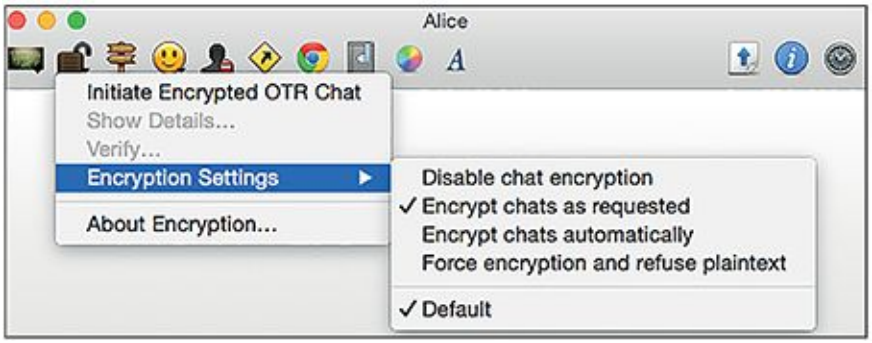


Abb. 5.8 Verschlüsselungsoptionen in Adium

5.2.4. Die Oma in Australien – Skype, Hangouts und sichere Alternativen

In der 80er-Jahren war Videotelefonie noch so futuristisch, dass kaum ein Science-Fiction-Film ohne sie auskam. Man wollte schließlich zeigen, dass das herkömmliche Telefonieren und die damit verbundenen Einschränkungen der Vergangenheit angehörten.

Mittlerweile hat die Videotelefonie sich in nahezu allen Schichten der Gesellschaft, mit Skype als einem der Vorreiter, durchgesetzt. Man könnte sogar sagen, dass Skype die Killerapplikation ist, die Heerscharen von Großeltern dazu bewogen hat, sich endlich mal mit »diesem Internet« zu beschäftigen.

Aber ist Skype auch sicher? Für die Oma, die sich abends von ihrem Enkel Bob erzählen lassen will, wie die Mathearbeit ausgefallen ist, ist diese Frage weniger wichtig als die einfache Bedienbarkeit des Programms auf ihrem iPad. Aber es gibt durchaus freie, sichere und bedienbare Alternativen zu Skype – dazu müssen Sie weder Informatik studiert haben noch benötigen Sie die Frustrationstoleranz eines Zen-Mönchs.

Aber erst mal zu der Antwort auf die oben stehende Frage: Skype hat einige Features, die es sicher machen könnten, wenn sie denn entsprechend eingesetzt werden würden. Hybride

Verschlüsselung (und zwar AES mit 256 bit Schlüssellänge) ist Teil des Skype-Protokolls und wird immer dann genutzt, wenn ein Skype-Client mit einem anderen Skype-Client kommuniziert. Wenn das Telefonat vom Skype-Client ins Fest- oder Handynetz, also ohne einen Skype-Client auf der Empfängerseite, erfolgt, passiert das nicht.

Der Skype-Server stellt dem anrufenden Skype-Client (also Omas Computer) seinen Public Key zur Verfügung. Der Client erstellt mit einem Zufallszahlengenerator einen Sitzungsschlüssel (Session Key), also einen Schlüssel zur symmetrischen Verschlüsselung, der nur für die eine Sitzung gilt. Diesen überträgt er mit dem Public Key des Servers verschlüsselt an den Server. Der Server überträgt ihn wiederum verschlüsselt an den Client, der angerufen wird (also Enkel Bob). Das geht ebenfalls mit asymmetrischer Verschlüsselung, da der Server nicht nur seinen Public Key an die Clients weitergibt, sondern auch die Public Keys der Clients gespeichert hat. Oma und Bob können jetzt eine mit dem Session Key symmetrisch verschlüsselte Sitzung starten. Warum das nicht ganz sicher ist (beispielsweise öffnet es die Türen für eine Man-in-the-Middle-Attacke), werden Sie weiter unten sehen.

Es gibt auch hier schon gewisse Sicherheitslücken, zum Beispiel hängt die Sicherheit der Kommunikation von der Qualität des Zufallszahlengenerators von Omas Computer ab, die wiederum vom Betriebssystem abhängt – im Großen und Ganzen kann man aber sagen, dass die Verschlüsselung des Nachrichteninhalts bis hierhin ganz anständig abläuft.

Die Metadaten sind allerdings unverschlüsselt – das heißt, wer mit wem wann und wie lange telefoniert hat. Warum das problematisch ist, haben Sie in Kapitel 1 schon gesehen. Außerdem legt Skype Ihre Nachrichten-Vorgeschichte in einer »History«-Datei auf Ihrem Computer ab – unverschlüsselt natürlich, sodass auch diese in falsche Hände geraten kann. In den Privatsphäre-Einstellungen können Sie bestimmen, dass keine History angelegt wird. Im weiteren Sinne auch zu den Metadaten gehört die IP-Adresse Ihres Computers, die ein Angreifer relativ leicht herausfinden kann, wenn er Ihren Skype-Namen kennt. Auch dies mag für die Oma erst einmal kein großes Problem darstellen – sehr wohl aber, wenn beispielsweise ein chinesischer Dissident von seiner Regierung lokalisiert werden kann, weil seine IP-Adresse bekannt wird. Wenn man sich vorstellt, dass ein Angreifer Omas Metadaten über mehrere Wochen beobachtet und die abendlichen Anrufe beim Enkel für mehrere Tage ausbleiben, wird diese Sicherheitslücke auch in ihrem Fall interessant: vielleicht besucht sie den Enkel gerade, oder sie liegt im Krankenhaus – eine glänzende Gelegenheit für einen Einbruch!

Neben den Metadaten hat Skype allerdings auch und vor allem bei Gesprächsinhalten eine eklatante Sicherheitslücke, und die wurde absichtlich eingeführt: Als Microsoft 2011 die bis dahin unabhängige, 2003 gegründete Firma Skype gekauft hat, hat es eine Hintertür eingeführt, die es Regierungsorganisationen erlauben sollte, Skype-Gespräche abzuhören. Bisher ist bekannt, dass die Regierungen der USA, Russlands und Chinas dazu in der Lage sind. Die englische Zeitung The Guardian berichtete, dass Skype dieses Abhören sogar schon vor dem Kauf durch Microsoft 2011 ermöglicht haben soll.

Wie funktioniert diese Hintertür? Da Skype den Quellcode seiner Software nicht offenlegt, ist das bis heute nicht ganz geklärt. Möglich wäre zum Beispiel eine Man-in-the-Middle-Attacke – da jegliche Kommunikation über den Skype-Server erfolgt, könnte dort ein verschlüsseltes Videotelefonat entschlüsselt, abgehört, neu verschlüsselt und an den Empfänger weitergeschickt werden.

Neben allen Sicherheitsbedenken gibt es bei der Skype-Telefonie auch noch das Problem der sogenannten Supernodes: Der Skype-Server pickt sich unter allen angemeldeten Benutzern einige wenige heraus, die er als Supernodes verwendet – das heißt, über deren Computer Datenverkehr von anderen Benutzern geleitet wird, auch wenn der betreffende Nutzer im Moment gar nicht per Skype telefoniert. Das verursacht unnötigen Verkehr für den untätigen Nutzer, der im Zweifelsfall auf seine Rechnung geht.

So weit also zur (fehlenden) Sicherheit der Videotelefonie mit Skype. Und wie sieht es mit der Sicherheit der Chatfunktion aus, die Skype bereitstellt? Instant Messages werden nach eigenen Angaben der Firma mittels TLS verschlüsselt. Diese Verschlüsselungsmethode haben Sie bereits im E-Mail-Kapitel kennengelernt. Dummerweise stellte sich aber heraus (und wurde 2013 auf der Nachrichtenseite Heise Online in der Rubrik Security berichtet), dass Microsoft in der Lage ist, Instant Messages der Benutzer nach URLs zu filtern: Benutzern fiel auf, dass eine URL, die sie per Chat verschickt hatten, kurze Zeit später von einem Microsoft-Bot besucht wurde. Das bedeutet, dass Microsoft in der Lage ist, Chatnachrichten zu entschlüsseln, und Chat per Skype somit definitiv *nicht* sicher gegenüber Lauschangriffen ist.

Das ist auch logisch nachzuvollziehen, denn TLS ist ja »nur« eine Transportverschlüsselung zwischen Client und Server. Das heißt, dass Mitteilungen immer kurzzeitig unverschlüsselt auf dem Server zur Verfügung stehen, bevor sie wieder durch einen verschlüsselten Transportkanal an den Gesprächspartner weitergeleitet werden. Auf dem Server ist es daher

leicht, die einzelnen Nachrichten zu analysieren oder gegebenenfalls sogar zu manipulieren. Das kann zu Werbe- oder auch zu Überwachungszwecken ausgenutzt werden.

Ähnlich verhält es sich auch mit *Hangouts*, der IM- und Videotelefonie-Lösung von Google. Dieser Dienst bietet erstaunlichen Komfort, einen großen Funktionsumfang, ist für die meisten Endgeräte verfügbar und eng mit anderen Google-Angeboten verzahnt, sodass er mittlerweile auch im Unternehmensbereich angewandt wird. Allerdings ist auch bei Hangouts derzeit nur eine Transportverschlüsselung vorgesehen. Eine echte Ende-zu-Ende-Verschlüsselung, die die Analyse der Gesprächsinhalte für Werbezwecke verhindern würde, gibt es derzeit nicht.

Der wenig beachtete arme Verwandte von Skype war lange Zeit die Software *Jitsi* (Abbildung 5.9). Deren Vorläufer SIP Communicator wurde schon im Jahr 2003 vom Straßburger Studenten Emil Ivov entwickelt. Nach und nach begeisterten sich jedoch immer mehr Einzelpersonen und Institutionen, beispielsweise die Universität Straßburg, für das Projekt, sodass immer wieder substanzielle Verbesserungen vorgenommen wurden – auch an der Benutzerfreundlichkeit!

Abb. 5.9 Kontaktliste von Jitsi

Jitsi versteht, wie Adium oder Pigdin, eine Vielzahl von IM-Protokollen, ist also auch für textbasierte Chats geeignet (siehe Abbildung 5.10).

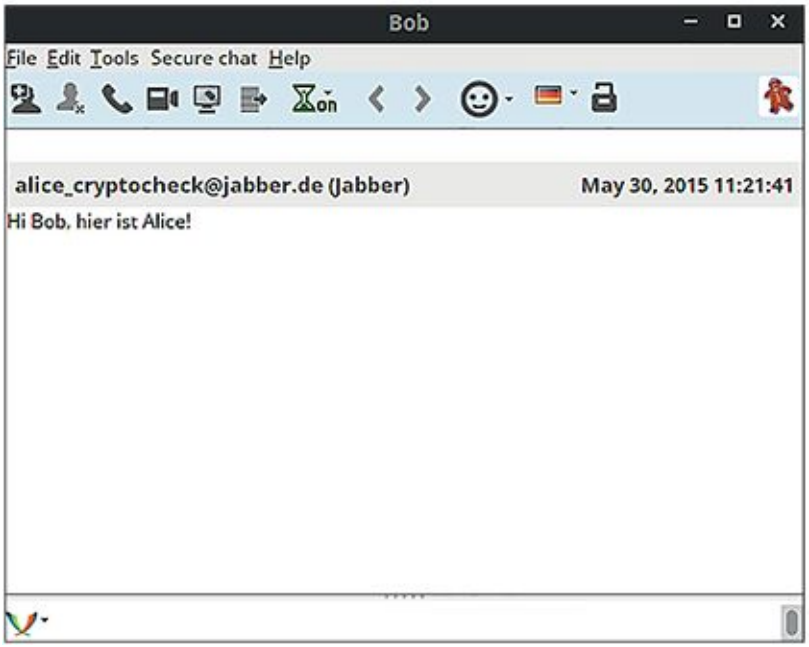


Abb. 5.10 Einfacher, unverschlüsselter Textchat in Jitsi

Die Software ist in Java geschrieben, was es prinzipiell ermöglicht, sie auf jeder Plattform laufen zu lassen. Im Wesentlichen werden also Windows, OS X und Linux unterstützt.

Zur Verschlüsselung von Textnachrichten steht das weiter oben beschriebene OTR-Protokoll zur Verfügung, und es werden zur Authentifizierung von Gesprächspartnern die gleichen Mechanismen angeboten wie in Pidgin (Abbildungen 5.11, 5.12 und 5.13).

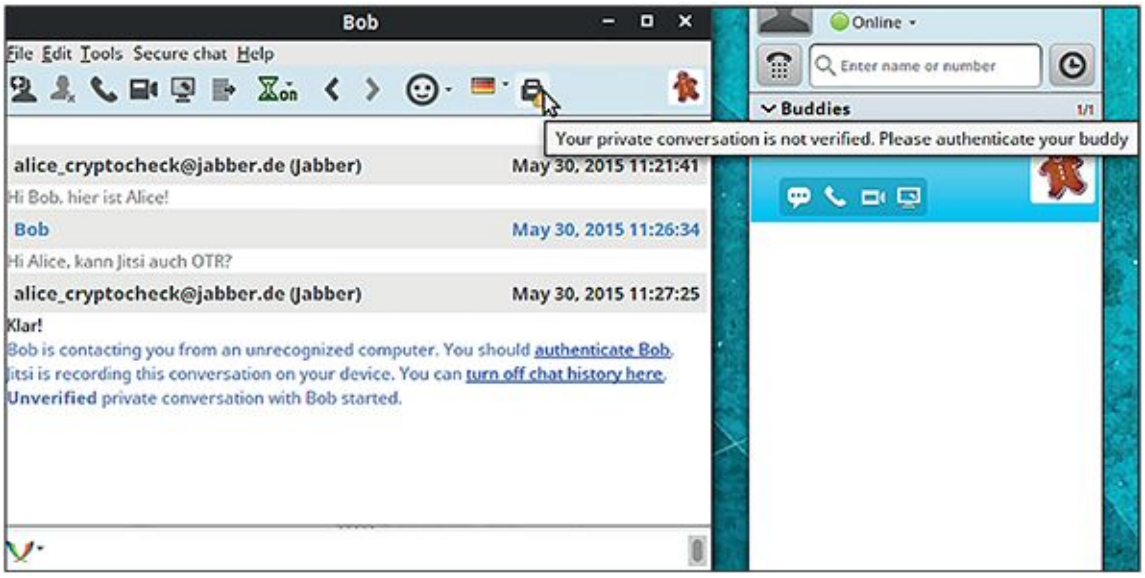


Abb. 5.11 OTR-Chat in Jitsi, Gesprächspartner noch nicht verifiziert

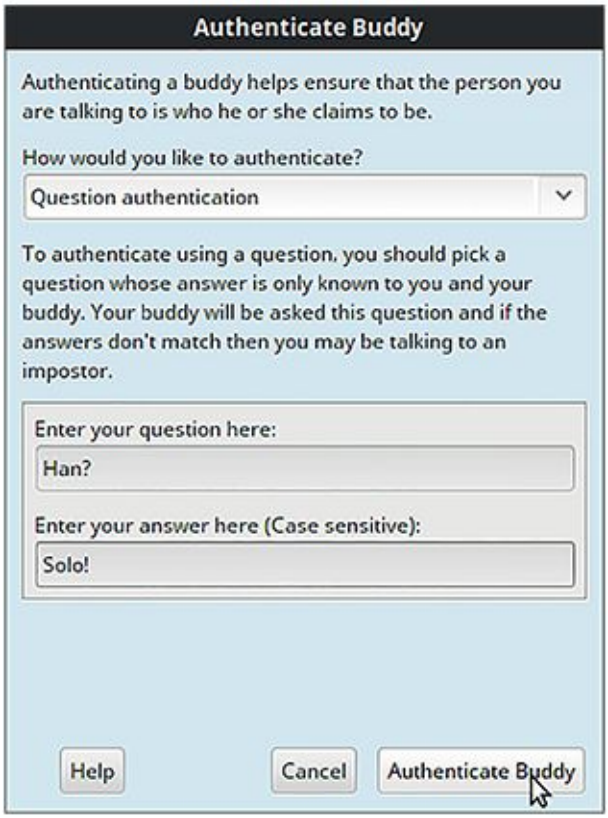


Abb. 5.12 Verifikation des Chatpartners in Jitsi mittels Frage und Antwort

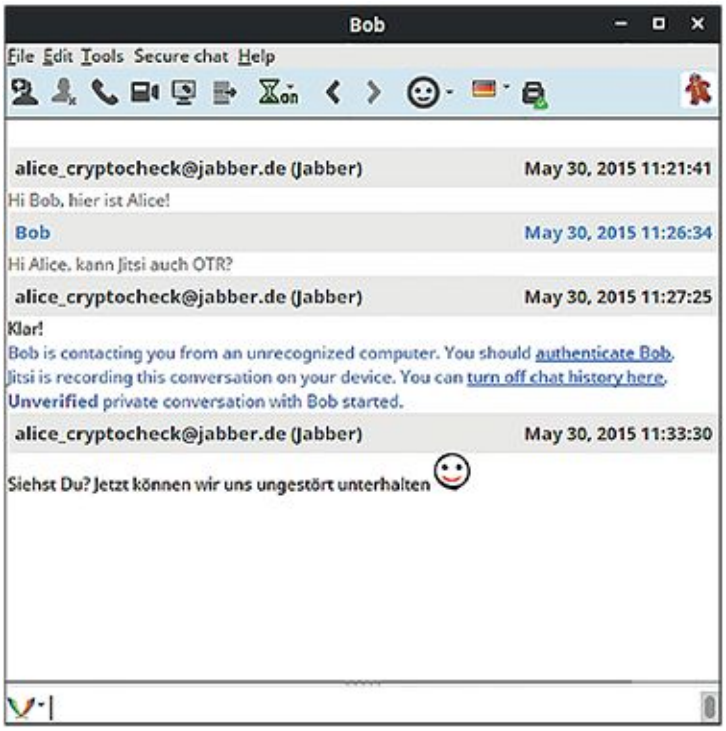


Abb. 5.13 Vertrauliche OTR-Konversation nach Authentifizierung des Chatpartners in Jitsi

Eine Besonderheit von Jitsi ist die Verwendung der XMPP-Erweiterung Jingle, die wir weiter oben schon kurz angesprochen hatten. Sie ermöglicht es Jitsi, Audio- und Videochats zwischen zwei Gesprächspartnern zu vermitteln, was erstaunlich einfach und in guter Qualität funktioniert. Einen Anruf initiieren Sie mit einem Klick auf das Telefonsymbol in der Kopfleiste (Abbildung 5.14).

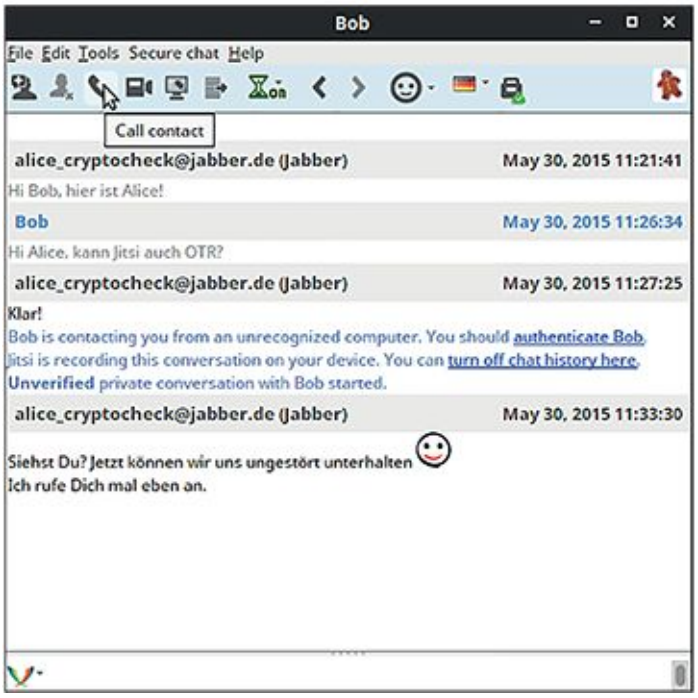


Abb. 5.14 Videoanruf zu Kontakt in Jitsi starten

Damit nicht genug: Jitsi unterstützt auch noch das *Z Real-time Transportation Protocol* (ZRTP)[18], mit dem sich Audio- und Videoanrufe sicher Ende zu Ende verschlüsseln lassen.

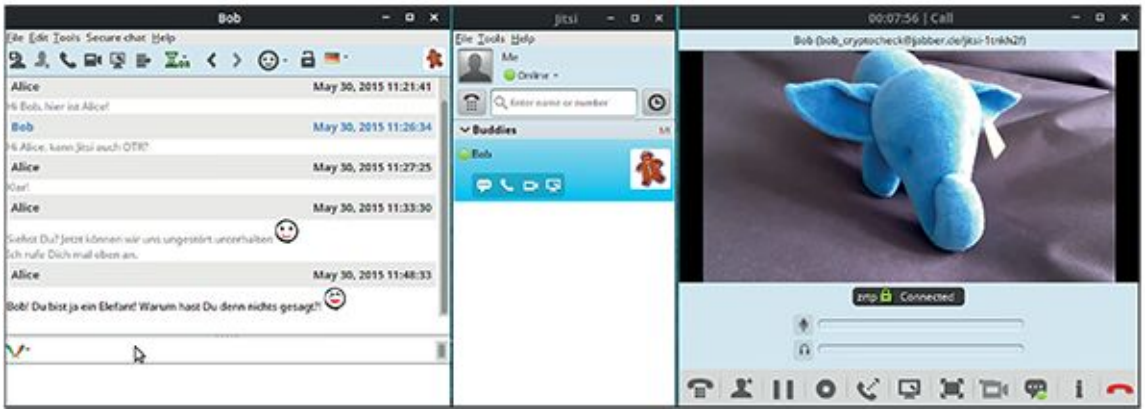


Abb. 5.15 Videoanruf in Jitsi

Analog zu OTR existiert auch für ZRTP einen Mechanismus, mit dem sich die Gesprächspartner gegenseitig verifizieren und der so vor unerwünschten Mithörern schützen soll. Beiden Teilnehmern wird ein vierstelliger Code angezeigt, den sie sich gegenseitig am Telefon vorlesen (Abbildung 5.16). Stimmen die Zeichen überein, kann die Leitung als sicher eingestuft werden, und das Schloss-Symbol wechselt seine Farbe von Gelb zu Grün.

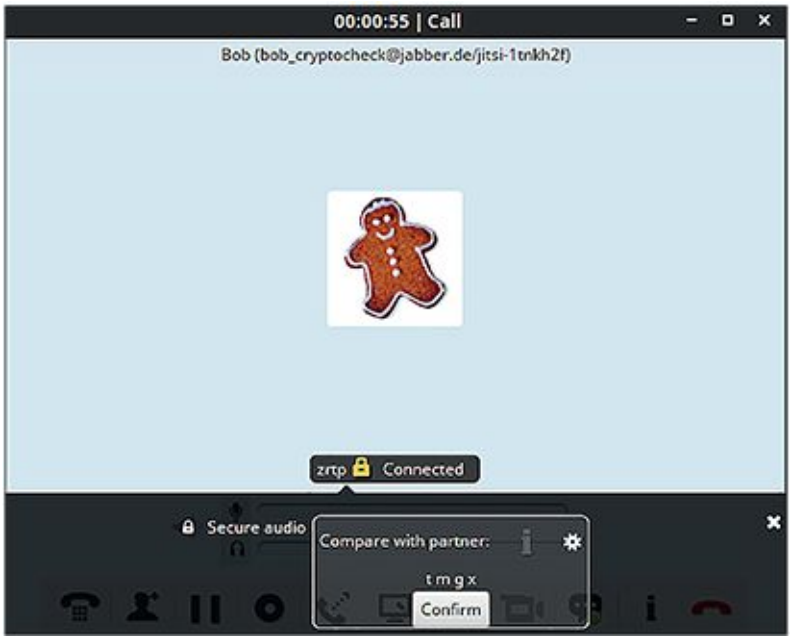


Abb. 5.16 Authentifizierung des Gesprächspartners für einen Videoanruf in Jitsi

5.3 Problemzone Smartphone (Android, iOS)

Wie beim E-Mailen ist auch beim Instant Messaging die Kommunikation zwischen zwei Smartphones tendenziell als unsicherer anzusehen als zwischen zwei Laptop- oder Desktop-Computern. Was Sie erwarten können und worauf Sie achten sollten, wenn Sie trotzdem mobil sicher kommunizieren möchten, erfahren Sie in diesem Abschnitt.

5.3.1. Die gute alte SMS

SMS werden wie Mobilfunkanrufe über ein Netz, das dem GSM-Standard entspricht, übermittelt. Sie werden nicht im Klartext übertragen, sondern je nach Land mit unterschiedlichen Algorithmen verschlüsselt – in Deutschland ist dies zurzeit A5/3. Sein Vorgänger, A5/1, galt lange Zeit als sicherer als die in anderen Ländern eingesetzte A5/2-Verschlüsselung. Allerdings wurde sie schon 2009 vom deutschen Informatiker Karsten Nohl geknackt. Das jetzige A5/3-Verfahren wurde ebenfalls von einer Forschergruppe im Jahr 2010 gebrochen. Allerdings ist hier nicht bekannt, ob ein derartiger Angriff auch in der Realität erfolgreich sein könnte. Die Telekom verkündete jedenfalls noch 2013, dass bis Ende des Jahres die Verschlüsselung flächendeckend auf A5/3 umgestellt werde.

SMS und auch Telefonie über das GSM-Netz sind allerdings durch Man-in-the-Middle-Attacken verwundbar. Für einen solchen Angriff werden unter anderem sogenannte *IMSI-Catcher* verwendet. Diese koffergroßen Geräte verhalten sich gegenüber dem Mobilfunknetz wie ein Endgerät, also zum Beispiel ein Telefon. Für die Handys in der Umgebung geben sie sich allerdings als Basisstation aus. Dazu machen sie sich eine Eigenheit des GSM-Protokolls zunutze: Mobiltelefone verbinden sich immer mit der Basisstation, die den besten Empfang bietet. Ein Mobiltelefon muss sich übrigens stets gegenüber dem Mobilfunknetz authentifizieren, das GSM-Netz aber nicht gegenüber dem Telefon. Steht ein IMSI-Catcher nun nah genug an einem Telefon, so kann er diesem vorgaukeln, eine Basisstation des Netzbetreibers zu sein. So zwingt er das Telefon dazu, eine unverschlüsselte Verbindung zu ihm aufzubauen. Gleichzeitig baut er für das Telefon eine Verbindung zur eigentlichen Basisstation auf. Alle Daten, also Anrufe und SMS, die nicht zusätzlich Ende zu Ende verschlüsselt wurden, fließen nun von der richtigen Basisstation über den IMSI-Catcher zum Telefon und zurück. So können unterwegs Telefonate mitgehört, SMS gelesen[19] und sogar verändert werden. Mit einem Preis um 250.000 Euro (Tendenz fallend) sind kommerzielle IMSI-Catcher mittlerweile nicht ausschließlich für Geheimdienste oder Polizeibehörden, sondern auch für den ambitionierten Kriminellen durchaus erschwinglich. Sogar ein Selbstbau (Kosten von etwa 1500 Euro) wurde bereits vor einigen Jahren von Chris Paget auf der Sicherheitskonferenz Defcon[20] vorgestellt[21]. Die Nachfolger von GSM (2G), UMTS und LTE (3G und 4G), sind sicherer als ihr Vorgänger, weil auch eine Authentifizierung des Netzes gegenüber dem Telefon vorgesehen ist. Hier gibt es aber beispielsweise die Möglichkeit, ein 3G-Netz so zu stören, dass das Telefon in 2G zurückfällt und wieder gegenüber dem oben beschriebenen Angriff anfällig wird.

Sie sollten eine SMS also sicherheitshalber wie eine unverschlüsselte E-Mail oder, den Vergleich kennen Sie ja schon zu genüge, wie eine Postkarte behandeln, also nicht davon ausgehen, dass irgendetwas, das Sie per SMS mitteilen, sicher vor unbefugtem Mitlesen ist.

Da mittlerweile ein großer Teil der SMS nicht mehr über altmodische Handys ohne mobiles Internet, sondern über Smartphones verschickt wird, gibt es eine große Auswahl an alternativen Messengern, von denen einige sicherer sind als die SMS – einige aber auch nicht.

5.3.2. WhatsApp – die Ablösung für SMS

Die erste wirklich weit verbreitete Alternative für SMS war WhatsApp, das ab 2009 entwickelt wurde. Anders als bei SMS werden die Nachrichtendaten über das mobile Internet und nicht über Mobilfunk übertragen, sodass WhatsApp sich erst durchsetzen konnte, als Smartphones weitere Verbreitung fanden.

WhatsApp benutzt zur Nachrichtenübermittlung eine angepasste Version des XMPP-Protokolls, das Sie schon weiter oben kennengelernt haben.

Nach Installation des WhatsApp-Clients auf dem Smartphone fordert WhatsApp erst einmal Zugriff auf das Adressbuch, sodass andere WhatsApp-Benutzer identifiziert werden können. Anders als bei beispielsweise TextSecure, das wir weiter unten vorstellen, ist ein Messaging mit Leuten, die selbst kein WhatsApp installiert haben, nicht möglich – trotzdem erhält WhatsApp aber auch auf die zugehörigen Adresseinträge im Telefonbuch des Nutzers Zugriff.

Die WhatsApp-Installation auf einem Smartphone wird automatisch mit der entsprechenden Mobilfunknummer verknüpft, die später (statt beispielsweise eines eindeutigen Benutzernamens) zur Identifikation eines Benutzers dient.

Im Februar 2014 wurde WhatsApp von Facebook gekauft. Da Facebook noch mehr als WhatsApp notorisch war für das Sammeln und Verwerten von Nutzerdaten, wurden zu diesem Zeitpunkt auch in den Mainstream-Medien Bedenken über den Datenschutz bei WhatsApp laut, und viele Nutzer begannen erstmals, sich Gedanken über mögliche Messaging-Alternativen zu machen (siehe weiter unten in diesem Kapitel).

Kommunikation per WhatsApp war ursprünglich überhaupt nicht verschlüsselt. Mitte 2012 verkündete die Firma jedoch, dass die Nachrichten künftig verschlüsselt würden. Es sprach sich schnell herum, dass der Nutzer-Login leicht zu knacken war: Der Benutzername entsprach stets der Mobilfunknummer, und Passwörter hingen vollständig von der IMEI-Nummer (eine Art Seriennummer eines Handys) oder der MAC-Adresse des Smartphones im Netzwerk ab. Auf Sicherheitskonferenzen wurde es ein beliebter Sport, immer neue Methoden vorzuführen, mit denen man unbefugt Daten der WhatsApp-Nutzer sammeln konnte – beispielsweise auch Profile über das Onlineverhalten von Nutzern.

Im November 2014, nachdem es schon viele Nutzer an Threema verloren hatte, zog WhatsApp jedoch nach und ging eine Partnerschaft mit Open Whisper Systems ein (Hersteller von TextSecure), die beauftragt wurden, eine Ende-zu-Ende-Verschlüsselung für WhatsApp zu

entwickeln. Diese wurde bisher für Android-zu-Android-Nachrichten umgesetzt. Eine Verschlüsselung kann jedoch, wie Sie wissen, nicht sicherstellen, dass Ihr Gesprächspartner auch der ist, für den Sie ihn halten: Dazu benötigen Sie eine gute Authentifizierungsmethode. Eine solche ist auch im neuen verschlüsselten WhatsApp noch nicht implementiert – Sie haben also keine Sicherheit darüber, dass Ihre Daten nicht (natürlich brav verschlüsselt) an einen Lauscher übermittelt werden und erst von diesem weiter an Ihren Gesprächspartner (Man-in-the-Middle-Attacke).

Zudem sind die Metadaten, die bei WhatsApp (wie auch bei praktisch allen anderen, auch den sicheren, Messaging-Apps) unverschlüsselt übermittelt werden, für Facebook hochinteressant – wer mit wem wann und wie lange kommuniziert. Die Geschäftsbedingungen von WhatsApp und Facebook schließen eine Nutzung dieser Daten zu Werbezwecken nicht aus – ein Geschäft, das Facebook sich kaum entgehen lassen wird.

5.3.3. Threema – kommerziell, aber sicher?

Als WhatsApp, das bis dahin eine eigenständige Firma war, 2014 von Facebook übernommen wurde, ging eine ungewohnte Welle der Besorgnis über Datenschutzfragen durch die Medien. Das führte dazu, dass nur wenige Wochen später der alternative Messaging-Dienst Threema siebenmal mehr Nutzer verzeichnen konnte als zuvor.

Threema ist ein in der Schweiz beheimateter Dienst der kleinen Firma Kasper Systems und bietet Ende-zu-Ende-Verschlüsselung an. Der Name Threema, sagt der Macher Manuel Kasper auf threema.ch, leitet sich von dem etwas unhandlichen Akronym EEEMA für »End-to-End-Encrypting Messaging Application« ab.

Wie WhatsApp ist auch Threema eine kommerzielle Software. Von den Benutzern wird allerdings, im Gegensatz zu WhatsApps jährlichem Gebührenmodell, nur eine einmalige Gebühr für die Installation des Clients auf dem Smartphone verlangt. Diese liegt je nach Betriebssystem zurzeit (Stand Juli 2015) bei unter zwei Euro. Threema generiert also auf diese Art weniger regelmäßige Einnahmen als WhatsApp, auch wenn man davon ausgeht, dass ein bereits registrierter Threema-Nutzer gelegentlich – vielleicht alle zwei bis drei Jahre – die Gebühr erneut zahlt, um Threema auf einem neuen Gerät einzurichten (obwohl auch diese erneute Gebühr bei der Einrichtung eines neuen Telefons vermieden werden kann). Auch Werbeeinnahmen kommen nicht zustande, weil Threema keine Werbeplätze in seiner App

verkauft. Es bleibt abzuwarten, ob die Macher doch eines Tages in das Werbegeschäft einsteigen oder sonstige Finanzierungsquellen von Benutzern oder Entwicklern erschließen – zum jetzigen Zeitpunkt zeichnet sich das allerdings nicht ab.

Seit März 2015 können Entwickler sich bei Threema für einen sogenannten *API*-Zugang kostenlos registrieren – das bedeutet, dass sie ihre eigene Software für die Nachrichtenverschlüsselung entwickeln können und nur das Threema-Protokoll für den Versand benutzen. Es ist also gut möglich, dass in Zukunft eine größere Auswahl von Apps zur Verfügung steht, die auf der Threema-Infrastruktur aufbauen.

Threema bietet, im Gegensatz zu WhatsApp, nicht nur eine Ende-zu-Ende-Verschlüsselung, sondern auch ein einfaches und praxistaugliches Verfahren zur Authentifizierung von Gesprächspartnern. Einziger Nachteil: Man muss seiner Alice oder seinem Bob dazu einmal von Angesicht zu Angesicht gegenübergestanden haben. Die Authentifizierung funktioniert nämlich so, dass man am Smartphone seines Gegenübers mit dem eigenen Smartphone einen QR-Code einscannt. Da man dabei unmittelbar, also durch Gesichtskontrolle, feststellt, dass der Besitzer des Barcodes der ist, der er zu sein vorgibt, wird die Identität des Threema-Users durch dieses Verfahren bestätigt. Eine solche Authentifizierung verhindert Man-in-the-Middle-Attacken.

Das Einscannen des QR-Codes des Gegenübers führt dazu, dass innerhalb der App dieser dann mit der höchsten Sicherheitsstufe markiert wird, also in Threemas Ampelsystem ein grünes Lämpchen bekommt. Wenn Sie nur den öffentlichen Schlüssel Ihres Kommunikationspartners vom Threema-Server herunterladen, wird der Gesprächspartner in Rot markiert, also als nicht authentifiziert. Es gibt noch eine mittlere (gelbe) Authentifizierungsstufe: Diese greift, wenn Threema die E-Mail-Adresse oder die Telefonnummer des Gesprächspartners (die ebenfalls als Hash[22] auf dem Threema-Server gespeichert sind) in Ihrem persönlichen Adressbuch auf dem Smartphone gefunden hat.

Um den Barcode Ihres Gegenübers einzuscannen, öffnen Sie zunächst den entsprechenden Kontakt in der Kontaktliste. In der Kopfzeile sehen Sie nun den Namen des Kontakts und darunter das Ampelsymbol (das in diesem Moment noch rot ist). Falls Sie schon Nachrichten mit diesem Kontakt ausgetauscht haben, sehen Sie diese darunter aufgelistet. Tippen Sie jetzt auf den Namen des Nutzers. Es öffnet sich nun eine Detailseite (siehe Abbildung 5.17).

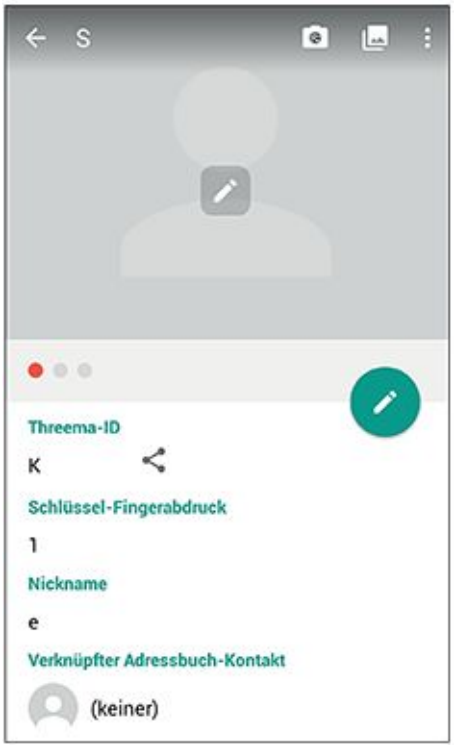


Abb. 5.17 Details eines Kontakts in Threema

Auf dieser Seite finden Sie in der Kopfzeile rechts ein Kamera-Symbol. Wenn Sie dieses antippen, wird die Barcode-App Ihres Smartphones geöffnet.

Wenn Ihr Gegenüber Ihnen nun seinen Barcode auf seinem eigenen Display anzeigt, können Sie ihn einscannen. Die Ampelfarbe des Kontakts sollte nun auf Grün umspringen.

Ihr Gesprächspartner möchte nun sicher auch Ihren Barcode einscannen – öffnen Sie dazu im Hauptbildschirm von Threema (der Liste der Kontakte) durch Antippen des Symbols ganz links oben das Menü. Im oberen Teil des Bildschirms wird nun Ihr Barcode eingeblendet (siehe Abbildung 5.18).

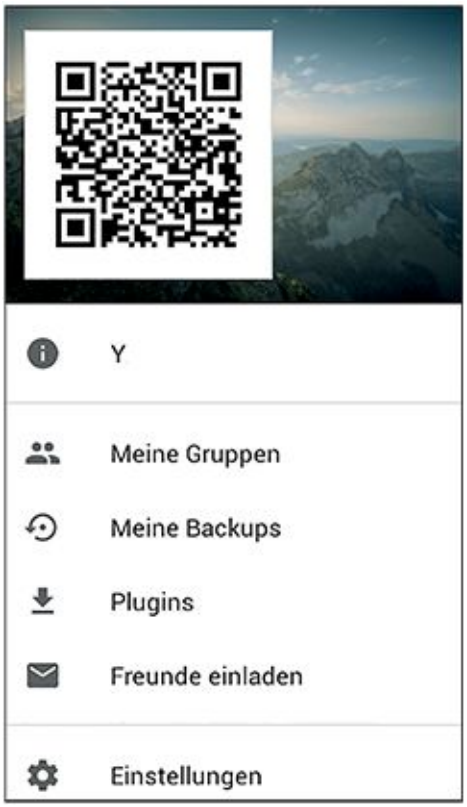


Abb. 5.18 Eigenen Barcode anzeigen in Threema

Da Threema eine kommerzielle Software ist – der Quellcode also sozusagen das Geschäftsgeheimnis der kleinen Schweizer Firma Kasper Systems darstellt – ist die Software nicht Open Source. Wenn ein Nutzer mit Fachkenntnissen sich also selbst davon überzeugen will, dass der Quellcode seiner Messaging-App keine offenen Sicherheitslücken enthält, wird er bei Threema enttäuscht werden. Auch unabhängige, externe Sicherheitsaudits sind bisher nicht durchgeführt worden – nach Ansicht von Kasper Systems würden sich diese finanziell nicht lohnen. Es wird auf der Webseite aber auf eine Softwarebibliothek verwiesen, die Networking and Cryptography library (NaCl), mit der getestet werden kann, ob eine vertrauenswürdige Ende-zu-Ende-Verschlüsselung mittels Threema stattfindet. Es handelt sich dabei um Programme in der Sprache C, und um die Bibliothek anzuwenden, muss man zumindest wissen, wie ein C-Programm kompiliert, also vom Quelltext in Maschinencode übersetzt wird – für den Anwender, der einfach nur wissen will, ob er der Verschlüsselung von Threema vertrauen kann, ist es also eher keine Option, diesen Test selbst durchzuführen.

Eine weitere Einschränkung der Sicherheit von Threema (aber auch der Sicherheit der meisten anderen Messenger): Metadaten werden nicht verschlüsselt. Eine weitere Einschränkung:

Jegliche Kommunikation läuft über einen zentralen Server in der Schweiz, der somit auch einen zentralen Angriffspunkt für eine mögliche Überwachung der Kommunikation darstellt.
Threema ist für Android und iOS verfügbar.

5.3.4. TextSecure und Signal – die Open-Source-Lösung

Open Whisper Systems, das Team um den Entwickler Moxie Marlinspike, hat eine App entwickelt, die ähnlich wie Threema Ende-zu-Ende-Verschlüsselung und Authentifizierung des Gesprächspartners bietet, aber zusätzlich auch noch quelloffen ist. Ursprünglich war das Ziel dieses 2009 begonnenen Projekts, die Kommunikation über SMS sicher zu machen – mittlerweile ist man aber dazu übergegangen, die sichere Kommunikation per Datenverbindung zu bevorzugen. SMS werden somit nicht mehr verschlüsselt, da dies technisch zu aufwendig geworden ist. Es gibt eine Software namens SMSSecure zur Verschlüsselung von SMS, die auf der ursprünglichen TextSecure-App basiert, mit dieser allerdings nicht mehr kompatibel ist.
Neben Ende-zu-Ende-Verschlüsselung (inklusive Perfect Forward Secrecy) verschlüsselt TextSecure auch die auf dem Smartphone gespeicherten Nachrichten. Wie bei anderen Messaging-Apps sind allerdings auch bei TextSecure Metadaten von der Verschlüsselung ausgenommen.
Bei Open Whisper Systems handelt es sich nicht um eine gewinnorientierte Firma, sondern um den Open-Source-Ableger des 2010 gegründeten Unternehmens Whisper Systems. Das ursprüngliche Whisper Systems wurde 2011 von Twitter gekauft. Obwohl Open Whisper Systems somit eher eine Open-Source-Community ist, gibt es neben den ehrenamtlichen Mitarbeitern an den Open-Source-Projekten auch einen kleinen Entwicklerstamm, der hauptberuflich an der Entwicklung von TextSecure arbeitet, darunter auch der ursprüngliche Gründer Moxie Marlinspike.
Whisper Systems hatte außerdem die sichere Skype-Alternative *Redphone* entwickelt, die mittlerweile ebenfalls als quelloffenes Projekt von Open Whisper Systems weiterentwickelt wird.
Wie funktioniert TextSecure nun praktisch? Wenn Sie das Programm aus dem App-Store installiert und sich mit Ihrer Telefonnummer registriert haben, werden Sie gefragt, ob Sie alle Ihre SMS-Nachrichten in die App importieren möchten – ursprünglich war TextSecure ja eine

App für den SMS-Versand. Bestätigen Sie ruhig diesen Import, sodass die SMS in der verschlüsselten Datenbank von TextSecure gespeichert werden.

Im Anschluss an den Importvorgang werden Sie gefragt, ob Sie TextSecure zu Ihrer Standard-SMS-App machen wollen. Wenn Sie hier bestätigen, werden zukünftige SMS ebenfalls in der verschlüsselten Datenbank gespeichert. Das bedeutet allerdings nicht, dass SMS dadurch während des Transports oder auf dem Smartphone Ihres Gegenübers auf magische Weise sicher geworden sind – versuchen Sie daher trotzdem mal, die Gesprächspartner, die noch auf altmodischen SMS bestehen, vom Umsteigen zu überzeugen.

Um die Verschlüsselung der Nachrichtendatenbank vollständig zu machen, sollten Sie noch ein Passwort einstellen. Wählen Sie dazu im Menü (siehe Abbildung 5.19 und 5.20) zuerst Einstellungen und im folgenden Menü ANWENDUNGSSCHUTZ.

Abb. 5.19 TextSecure-Menü

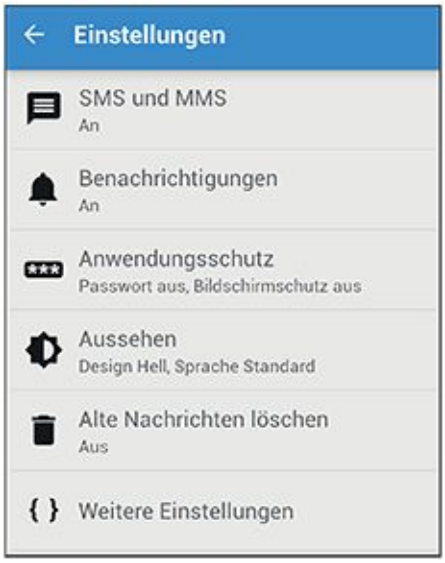


Abb. 5.20 TextSecure-Einstellungen

Dort müssen Sie das standardmäßig ausgeschaltete Häkchen für PASSWORT AKTIVIEREN einschalten und Ihr gewünschtes Passwort eingeben (siehe Abbildung 5.21). Zudem können Sie wählen, ob die App das Passwort nach einem gewissen Zeitintervall »vergessen« soll.

Abb. 5.21 Passwort aktivieren in TextSecure

Der Versand neuer Nachrichten an Kontakte in Ihrem Adressbuch funktioniert ganz intuitiv – gehen Sie dazu einfach auf die Kontaktliste und tippen den Kontakt an, dem Sie schreiben möchten. Zur Sicherheit erinnern wir Sie noch einmal daran: Wenn der Gesprächspartner nicht selber TextSecure (oder Signal, siehe unten) nutzt, wird die Nachricht als unsichere SMS verschickt.

Wie Sie wissen, ist mit dem nun eingerichteten verschlüsselten Versand von Nachrichten zwischen Ihnen und Ihrem ebenfalls TextSecure benutzenden Gesprächspartner noch nicht sichergestellt, dass niemand die Nachrichten mitliest – ein Angreifer könnte sich ja als Ihr Gesprächspartner ausgeben (Man-in-the-Middle-Attacke). Hierzu müssen Sie, wie oben schon bei Threema beschrieben, die öffentlichen Schlüssel verifizieren. Am einfachsten funktioniert das, wie bei Threema, durch Einscannen eines QR-Codes. Hierzu wählen Sie innerhalb eines Chats mit Ihrem Gesprächspartner das Schloss-Symbol im oberen Bereich des Fensters aus. Im darunterliegenden Menü tippen Sie einfach »Empfänger überprüfen« an. Daraufhin erscheint ein Fenster mit dem Fingerprint Ihres öffentlichen Schlüssels und dem Ihres Gegenübers. Hier haben Sie wiederum durch Antippen des Barcode-Symbols in der oberen rechten Ecke die Möglichkeit, die Schlüssel gegenseitig per QR-Code zu verifizieren (Abbildung 5.22).

Abb. 5.22 Eigenen Schlüssel als Barcode zum Einscannen anzeigen lassen in TextSecure

Bis hierhin haben wir die Vorgehensweise für Android-Nutzer beschrieben. iPhone- und iPad-Nutzern steht jedoch die kompatible iOS-App *Signal*[23] (Abbildung 5.23) zur Verfügung, die von den gleichen Entwicklern wie TextSecure stammt und eine ganz ähnliche Benutzeroberfläche aufweist.

Abb. 5.23 Mit TextSecure kompatible App Signal für iOS

5.3.5. IM und Chat: auf dem Laufenden bleiben

Da der Messenger-Markt ständig in Bewegung ist, gibt es bei Erscheinen dieses Buches vielleicht schon wieder einen neuen vielversprechenden Messenger, oder die Entwicklung von einem der hier vorgestellten ist eingestellt worden. Die Electronic Frontier Foundation (EFF) hat auf ihren Seiten einen sehr schön übersichtlichen grafischen Vergleich von verschiedenen Messengern, genannt *Secure Messaging Scorecard*[24],in der diese nach sieben Kriterien bewertet werden (siehe auch Abbildung 5.24):

- Transportverschlüsselung
- Verschlüsselung, die Sicherheit gegen Mitlesen des Providers bietet
- Authentifizierung der Identität der Gesprächspartner
- Perfect Forward Secrecy (können zurückliegende Gespräche im Nachhinein gelesen werden, wenn ein Schlüssel gestohlen wird?)
- Quelloffener Code
- Anständige Dokumentation der Sicherheitsarchitektur
- Externe Sicherheitsaudits des Quellcodes

Abb. 5.24 Auszug aus der Secure Messaging Scorecard der EFF

Hier lohnt es sich, vor Installation eines neuen Messengers einen Blick zu riskieren.

[1] eine Sehnenscheidenentzündung durch exzessives Schreiben von SMS-Nachrichten

[2] IRC existiert übrigens noch immer und erfreut sich weiterhin reger Beliebtheit bei diversen Subkulturen.

[3] www.spin.de

[4] www.knuddels.de

[5] www.icq.com

[6] www.aol.de

[7] https://mail.ru

[8] www.miranda-im.de

[9] https://userbase.kde.org/Kopete/de

[10] https://jitsi.org/Documentation/UserDocumentation

[11] https://developer.pidgin.im/wiki/Using\%20Pidgin

[12] https://adium.im/help/pgs/AdiumDocumentation.html

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

[14] http://web.jabber.ccc.de/

[15] http://j-u-n-e.org/wiki/JUNe/Mitglieder

[16] http://xmpp.org/

[17] www.miranda-im.org

[18] Das »Z« im Namen ist eine Anspielung auf den Erfinder des Protokolls, Phil Zimmermann, der auch der Schöpfer des PGP-Standards ist.

[19] was zum Beispiel beim Mobil-TAN-Verfahrenfür Ihr Onlinebanking sehr pikant sein kann

[20] https://www.defcon.org

[21] https://www.youtube.com/watch?v=fQSu9cBaojc

[22] zu Hash-Funktionen siehe Kapitel 2

[23] https://itunes.apple.com/de/app/signal-private-messenger/id874139669

[24] https://www.eff.org/de/node/82654

Kapitel 6 Blick über den Tellerrand

Herzlichen Glückwunsch! Wenn Sie bis hierhin durchgehalten haben, kennen Sie nun die Grundlagen der digitalen Kryptografie und wissen, wie Sie potenziellen Angreifern, die Ihre Kommunikation abhören wollen, in die Suppe spucken. Sie wissen aber auch, dass sichere Kommunikation und Datensicherheit ein sehr weites Feld sind, das ständigem Wandel unterliegt, und für das es keine Patentrezepte gibt.

In diesem Kapitel wollen wir daher ein paar Aspekte zu Verschlüsselung und Datensicherheit genauer beleuchten. Die Unterkapitel haben keine bestimmte Reihenfolge – vielleicht interessieren Sie manche Themen gar nicht und manche umso mehr, picken Sie sich also ruhig erst einmal nur ein oder zwei heraus.

6.1 Metadaten – Ihr Smartphone weiß, was Sie letzten Sommer getan haben

Wenn Sie den einen oder anderen Artikel zur sogenannten NSA-Affäre gelesen haben, ist Ihnen wahrscheinlich bewusst, dass viele westliche Geheimdienste auch *Metadaten* nahezu vollumfänglich sammeln und speichern.

Hinweis

Metadaten

Metadaten sind »Daten über Daten«. Sie dienen dazu, sogenannte Nutzdaten, also beispielsweise den Text einer E-Mail, ein Bild auf Ihrer Digitalkamera oder ein E-Book, näher zu beschreiben. Metadaten können neben zusätzlicher Beschreibung der Nutzdaten aber auch Steuerinformationen beinhalten. Der sogenannte Header einer E-Mail enthält beispielsweise sowohl Informationen, die den Inhalt beschreiben (z. B. Absender, Betreff und Zeitstempel), als auch solche, die für die Übermittlung der Nachricht wichtig sind (z. B. E-Mail-Adresse des Empfängers).

Auch in der analogen Kommunikation existieren Metadaten. Empfänger und Absender eines Briefes und sogar die Briefmarke sind im Grunde nur Steuerinformationen für den Postdienst, die wichtig dafür sind, dass der Brief beim Empfänger ankommt.

Das Problem mit Metadaten: Sie sind unerlässlich, damit Kommunikation überhaupt stattfinden kann und fallen daher auch bei jeglicher Art von Kommunikation an. Gleichzeitig können sie aber in vielen Fällen nicht verschlüsselt werden, da sie auf dem Weg lesbar bleiben müssen. Ein Postbote könnte ja auch einen Brief nicht zustellen, dessen Adressat und Absender nur verschlüsselt auf dem Umschlag stehen.

Metadaten Ihrer E-Mails sind unter anderem Absender, Empfänger, Datum, Uhrzeit und Betreff. Auch Telefonanrufe erzeugen Metadaten. Diese sind beispielsweise die Rufnummer des Anrufers, die gewählte Rufnummer sowie Dauer und Uhrzeit des Telefonats.

Sie können sich vorstellen, dass allein schon durch die Auswertung der Metadaten Ihres E-Mail-Verkehrs und Ihrer Telefonate ein ziemlich genaues Bild Ihrer Gewohnheiten und sozialen Kontakte entstehen kann. Mailadressen und Telefonnummern, die oft kontaktiert werden, sind wahrscheinlich Freunde und Familie. Eine Telefonnummer, die oft nach zehn Uhr abends angerufen wird, ist wahrscheinlich der Partner oder die Partnerin. Wenn häufig die Nummer eines Arztes oder Krankenhauses angerufen wird, liegt wohl ein gesundheitliches Problem vor, und wenn über mehrere Tage oder Wochen hinweg die Nummer einer psychologischen Beratungsstelle oder eines Psychiaters angerufen wird, dann würden Sie als Arbeitgeber diese Person lieber nicht einstellen, oder?

Forscher der US-amerikanischen Universität Stanford, Jonathan Mayer und Patrick Mutchler, haben eine Studie zu Metadaten durchgeführt. Das Ziel war, genauer zu beleuchten, welche Arten von sensiblen Informationen man über Personen herausfinden kann, wenn man nur Zugriff auf Metadaten, nicht auf die Inhalte der Kommunikation hat. Zu diesem Zweck boten sie die App MetaPhone kostenlos zum Download an. Freiwillige, die diese App herunterluden, stellten ihre Metadaten über mehrere Monate zur Auswertung zur Verfügung. Die Forscher verzichteten darauf, zusätzlich Daten über die Aufenthaltsorte der Teilnehmer auszuwerten, was technisch aber möglich gewesen wäre.

Die Auswertung zeigte, dass ein großer Teil der Teilnehmer während der Laufzeit der Studie Empfänger kontaktierte, bei denen möglicherweise schon der Anruf an sich eine sensible Information darstellt: Ärzte und Krankenhäuser, Banken und Kreditinstitute, Apotheken, Rechtsanwälte, Personalvermittler und kirchliche Einrichtungen beziehungsweise Einrichtungen anderer Religionen. Sieben Prozent der Teilnehmer kontaktierten zudem Waffenhändler oder -werkstätten (eine US-amerikanische Eigentümlichkeit, die bei einer

deutschen Studie wohl nicht vorgekommen wäre), und zwei Prozent der Teilnehmer kontaktierten »Adult Establishments«, also Bordelle oder Nachtclubs. Die Anrufe bei medizinischen Einrichtungen konnten die Forscher weiter nach Fachrichtung aufschlüsseln. Beispielsweise gingen immerhin jeweils ein Prozent der Anrufe an suchtmedizinische Zentren und ein Prozent an schönheitschirurgische Praxen oder Kliniken. Eine weitere Aufschlüsselung der anderen Kategorien zeigte zum Beispiel Anrufe bei den Anonymen Alkoholikern, bei Scheidungsanwälten und Behandlungszentren für Geschlechtskrankheiten.

Im nächsten Schritt betrachteten die Forscher nicht mehr nur einzelne Anrufe, sondern setzten die Anrufe miteinander in Beziehung, um aus dem Muster weitere Schlüsse zu ziehen. Hier wurden zum Beispiel bei einem Teilnehmer lange Telefonate mit Kardiologen an einem großen Krankenhaus aufgezeichnet, ein kurzes Gespräch mit einem Labor, eingehende Anrufe einer Apotheke und mehrere kurze Anrufe bei der Hotline eines medizintechnischen Geräts zur Überwachung von Herzrhythmusstörungen. Ein anderer Teilnehmer kontaktierte innerhalb von drei Wochen einen Baumarkt, mehrere Schlüsseldienste, einen Händler für hydroponische Bewässerungssysteme und einen Headshop (ein Geschäft, das Zubehör für den Konsum von Cannabis verkauft). Die Metadaten des ersten Teilnehmers wären sicher hochinteressant für einen potenziellen Arbeitgeber oder eine Versicherungsgesellschaft, bei der der Teilnehmer versucht, eine Lebensversicherung abzuschließen. Für die Metadaten des zweiten Teilnehmers dürfte sich sogar die Polizei interessieren.

All dies wurde, wie gesagt, aus Metadaten geschlossen, bei denen die Daten zum Aufenthaltsort des Teilnehmers ausdrücklich nicht berücksichtigt wurden. Noch sensibler wird die Datenlage also, wenn wir geografische Informationen dazunehmen. Zwei Politiker, der Grünen-Abgeordnete Malte Spitz(http://www.zeit.de/digital/datenschutz/2011-02/vorratsdaten-malte-spitz) und der Schweizer Nationalrat Balthasar Glättli(http://www.nzz.ch/aktuell/digital/vorratsdaten-veroeffentlicht-nationalrat-balthasar-glaettli-1.18291061), haben der Öffentlichkeit die bei der jeweiligen Telefongesellschaft gespeicherten Vorratsdaten zur Verfügung gestellt: Malte Spitz für sechs Monate im Jahr 2009, Balthasar Glättli für sechs Monate im Jahr 2013 (veröffentlicht 2014). Journalisten der ZEIT beziehungsweise Mitarbeiter der Agentur Open Data City erstellten daraus detaillierte Profile, die zeigen, wo sich die Politiker an welchem Tag zu welcher Uhrzeit aufgehalten haben, mit

wem sie wann und wie lange kommunizierten, wie lange sie mit dem Internet verbunden waren und so weiter.

Der Anwalt Ton Siedsma, der für die Bürgerrechtsorganisation Bits of Freedom arbeitet, hat seine Metadaten zwar nur für eine Woche veröffentlicht (https://netzpolitik.org/2014/metadaten-wie-dein-unschuldiges-smartphone-fast-dein-ganzes-leben-an-den-geheimdienst-uebermittelt/), aber in noch größerem Detail, als es die Vorratsdatenspeicherung der Telefongesellschaft hergeben würde. Die Auswertung zeigte, dass nur aus den Metadaten sein ungefähres Alter, sein Beruf, sein Beziehungsstatus und die Identität seiner Freundin ermittelt werden konnten. Der Weg, den er beim Pendeln zurücklegte, wurde offengelegt, und es konnten Schlussfolgerungen über seine Arbeitsbedingungen, über sensible Inhalte seiner Arbeit sowie über den Studienfortschritt seiner Schwester gezogen werden, über seine Hobbies und Interessen, seine Sympathien für eine bestimmte politische Partei und seine Religionszugehörigkeit. Außerdem konnten detaillierte Netzwerkdiagramme über seine privaten und beruflichen Kontakte erstellt werden. Man kann sich leicht vorstellen, dass diese Analyse noch viel aufschlussreicher werden könnte, wenn wiederum auch die Metadaten dieser Kontaktpersonen analysiert werden würden.

Die am NSA-Untersuchungsausschuss beteiligte Politikwissenschaftlerin Anne Roth berichtete der englischen Zeitung The Guardian, wie ihr Mann, ein Soziologe, im Jahr 2007 unter Terrorverdacht verhaftet wurde (http://www.theguardian.com/world/2014/nov/09/berlins-digital-exiles-tech-activists-escape-nsa). Grundlage des Verdachts waren ihrer Auffassung nach Schlüsselwörter, die er in wissenschaftlichen Aufsätzen verwendet hatte, wie zum Beispiel marxistisch-leninistisch, sowie Metadaten wie die Personen, die er anrief, die Tatsache, dass er seine E-Mails verschlüsselte, und dass er gelegentlich ohne eingeschaltetes Handy aus dem Haus ging.

Und wie können Sie diese Metadaten-Lecks stopfen? Um gar keine Metadaten mehr zu hinterlassen, müssten Sie die Funktionalität Ihres Smartphones wahrscheinlich so weit einschränken, dass Sie genauso gut wieder eine Telefonzelle benutzen könnten. Die Erzeugung von Metadaten lässt sich leider nicht vollständig vermeiden – es sei denn, Sie sind bereit, dafür einen hohen Aufwand zu treiben und soziale Kontakte aufzugeben oder einzuschränken. Realistischer ist es daher, sich der Existenz dieser Daten bewusst zu sein und möglichst wenige dieser digitalen Spuren zu hinterlassen. Sie sollten dazu folgende Punkte beachten:

- E-Mail-Betreffzeilen bleiben auch bei verschlüsselten Mails klar lesbar. Geben Sie daher keine sensiblen Informationen (zum Beispiel Kundennummern) im Betreff einer E-Mail preis.
- Schalten Sie in Ihrem Google-Konto die Aufzeichnung von Suchverläufen und Aufenthaltsorten aus.
- Verzichten Sie auch bei Twitter, Facebook oder anderen sozialen Netzwerken darauf, Ihren Aufenthaltsort bekannt zu geben.
- Nutzen Sie Werbe- und Skriptblocker in Ihrem Browser (siehe auch Kapitel 3).
- Ändern Sie die Konfiguration Ihres Browsers so, dass Plug-ins nicht mehr automatisch, sondern nur auf Ihren ausdrücklichen Wunsch hin ausgeführt werden (siehe auch Kapitel 3).
- Geben Sie in Webformularen nur Pflichtinformationen an.

6.2 Der Laptop im Hofbräuhaus – kleine Übersicht über Festplattenverschlüsselung

Sie wissen ja wahrscheinlich aus dem Geschichtsunterricht (oder aus spätabendlichen Dokumentationen auf NTV), dass manchmal erst berittene Horden einfallen müssen, bis jemand eine Chinesische Mauer baut. Manchmal muss auch erst ein Zeppelin explodieren, bis Leute einsehen, dass es eine schlechte Idee ist, Luftschiffe mit feuergefährlichem Gas zu füllen, und manchmal muss man sich selbst einmal richtig in Schwierigkeiten bringen, bevor man seinen Daten ein Vorhängeschloss verpasst.

Um die Privatsphäre der Autoren dieses Buchs zu schützen[1], tun wir einfach mal so, als wäre die folgende Geschichte nicht einem von uns passiert, sondern jemand ganz anderem. Vielleicht (aber wir hoffen es nicht) finden Sie sich auch selbst in der Geschichte wieder:

Die betreffende Person (nennen wir sie mal ganz unbayerisch Erik) besitzt einen Laptop, auf dem ein Haufen sensibler Informationen gespeichert sind. Eriks Notebook, auf dem Windows installiert ist, hat eine Passwort-Zugangssperre, die allerdings einem entschlossenen Angreifer nicht viel entgegenzusetzen hat: Es gibt mehrere Möglichkeiten, das Passwort zurücksetzen zu lassen, um vergessliche Nutzer nicht zu vergrämen. Außerdem ist ein Laptop, der in den Besitz eines Angreifers geraten ist, natürlich der Gefahr eines Brute-Force-Angriffs ausgesetzt. (siehe hierzu auch Kapitel 2).

An einem regnerischen Frühlingsabend beschließt Erik, mit zwei Freunden ins Hofbräuhaus zu gehen. Das Hofbräuhaus hat 3500 Sitzplätze, und die Leute, oft aus ganz verschiedenen Ländern, sitzen an langen Tischen. Erik und seine Freunde sind froh, in dem überfüllten Gasthaus noch einen Tisch mit drei freien Plätzen ergattert zu haben. Er verstaut seinen Rucksack zugunsten der Bequemlichkeit unter seiner Sitzbank und ordert voller Vorfreude die erste Maß des Tages. Im weiteren Verlauf des Abends wird die zwischenmenschliche Kommunikation der anwesenden Gäste kontinuierlich durch reichlich Bier geölt, sodass nach 20 Uhr ein Lärmpegel wie auf der Landebahn Nordwest des Frankfurter Flughafens herrscht. Zufällig finden Erik und seine Freunde sich an einem Tisch mit vier zunächst schweigsamen Finnen wieder, die nach zwei Maß Bier jedoch zunehmend auftauen und schließlich laut, aber melodisch, finnische Volkslieder anstimmen. Man tauscht sich darüber aus, was einem an München gefällt (die Fußballmannschaft) und was nicht (die Fußballmannschaft). Nach zwei weiteren Maß schließt man Freundschaft mit dem Nebentisch, an dem englische Schülerinnen und Schüler auf Abschlussfahrt sitzen. Brüllend tauscht man Vornamen aus und trinkt auf die Völkerverständigung, während die Blaskapelle spielt.

Ein paar Salzbrezen und eine weitere Runde Bier später hört die Blaskapelle plötzlich auf zu spielen. Die in Dirndl gewandeten Kellnerinnen fangen an, Bierkrüge abzuräumen; kein Bier mehr nach halb zwölf. Wohin jetzt mit den neugewonnenen Freunden? Ein stämmiger Australier schlägt vor, in einem Irish Pub weiterzutrinken. Oder doch besser noch in einen Club? Vorschläge werden gemacht und wieder verworfen. Währenddessen geht das Neonlicht an, und die Kellnerinnen werden letzten zurückgebliebenen Gästen gegenüber langsam unwirscher.

Schließlich geht man gemeinsam, nicht mehr ganz schnurgerade, in Richtung Ausgang. Die Gruppe teilt sich, einige gehen nach Hause, Erik geht mit anderen weiter in den Irish Pub. Nach dem einen oder anderen Guinness wird aber auch er müde, und er geht zurück in die Wohnung, die er sich für den Aufenthalt mit den anderen Freunden teilt. Als er seinen Rucksack in die Ecke werfen und auf der Luftmatratze unter die Decke kriechen will, fällt ihm auf: Wo ist der Rucksack?

In dem Rucksack waren nicht nur Stadtplan und Rückflugticket, sondern auch und vor allem der Laptop! Vor Schreck muss er sich erst mal setzen. Ein eiliger Anruf im Hofbräuhaus endet nur am Anrufbeantworter. So beschließt er, sich erst einmal schlafen zu legen. Am nächsten

Morgen begibt er sich um kurz nach acht, auf leeren Magen und mit Kreislaufproblemen, mit der U-Bahn zurück in die Innenstadt, um als Allererstes bei Öffnung des Hofbräuhauses nach dem Verbleib seines Rucksacks zu fragen.

Die Geschichte geht gut aus – zufällig, denn jeder der Gäste am vorigen Abend hätte den Rucksack unauffällig über die Schulter werfen und mitsamt des Laptops zurück nach Schwabing, Dortmund oder Atlanta nehmen können. Auf dem Laptop hätten wichtige Unterlagen, ärztliche Befunde, Bankdaten oder Nacktfotos sein können. Die Zugangssperre des Laptops ist, wie oben schon erwähnt, oft leicht auszuhebeln. Selbst wenn einem unehrlichen Finder das Knacken des Passwortes nicht gelingen sollte, so könnte er oder sie ohne Weiteres ein sogenanntes Live-Betriebssystem booten (von DVD oder USB-Stick) und auf diesem Wege auf der Festplatte gespeicherte Daten auslesen. Mit etwas Glück gelingt ihm das sogar bei bereits gelöschten Informationen (siehe auch Kapitel 1). Schließlich könnte besagter Angreifer auch einfach die Platte ausbauen und die Daten mithilfe eines anderen Computers auslesen.

Was tun gegen solche Gefahren? Eine Lösung ist die Festplattenverschlüsselung. Eine Festplatte lässt sich auf verschiedene Arten schützen, und einige dieser Möglichkeiten wollen wir im Folgenden mit Ihnen durchgehen. Die meisten davon lassen sich übrigens nicht nur auf Festplatten oder SSDs, sondern auch auf anderen Datenträgern wie beispielsweise USB-Sticks und SD-Karten anwenden. Die Verschlüsselung von Speichermedien kann auf verschiedenen Ebenen erfolgen, die sich teilweise sogar miteinander kombinieren lassen.

6.2.1. Dateiverschlüsselung

Die Verschlüsselung auf Dateiebene ist eine der einfachsten Möglichkeiten, Ihre Daten zu schützen. Einzelne wichtige Dateien können so vor unautorisiertem Zugriff bewahrt werden.

Viele gängige Anwendungen bieten mittlerweile solch eine Chiffrierung ihrer Daten an. So kann zum Beispiel ein Bank- oder Steuerprogramm selbst seine Daten gegen unberechtigten Zugriff schützen. Hierbei kommt oft das symmetrische Verschlüsselungsverfahren AES zum Einsatz. Auch mit GPG, das Sie bereits aus dem E-Mail-Kapitel kennen, lassen sich einzelne Dateien asymmetrisch verschlüsseln.

Dateiverschlüsselung

Vorteile:

- einfach anzuwenden

- in vielen Programmen des täglichen Lebens bereits direkt benutzbar, z. B.
  OpenOffice, LibreOffice (Office Suite für Windows, Linux und OS X)
  Microsoft Office (Office Suite für Windows und OS X)
  OutBank (Onlinebanking für OS X)
  Starmoney (Onlinebanking für Windows)
  Elster (Elektronische Steuererklärung für Windows)

Nachteile:

- Viele einzelne Dateien zu verschlüsseln ist umständlich.
- Für alle Dateien immer dasselbe Passwort zu verwenden, ist gefährlich.
- Die Verschlüsselung einzelner Dateien kann die Aufmerksamkeit von Angreifern direkt auf diese Dateien lenken.
- Große Teile Ihrer Daten bleiben ungeschützt.
- Oft kann nicht beurteilt werden, wie proprietäre Programme Daten verschlüsseln, daher ist es fraglich, ob diese wirklich »sicher« sind.
- Bei proprietärer Software kann auch oft nicht beurteilt werden, ob vom Hersteller Hintertüren für Polizeibehörden oder Geheimdienste eingebaut wurden.
- Verlieren oder vergessen Sie den Schlüssel, sind Ihre Daten nicht mehr nutzbar.

6.2.2. Verschlüsselte Container

Es gibt Programme, die einen verschlüsselten Container erzeugen, in dem Dateien abgelegt werden können. Dieser liegt dann als große Datei auf Ihrer Festplatte und kann dann durch spezielle Programme wie ein virtueller USB-Stick in das System eingebunden und wieder ausgeworfen werden. Die jeweilige Software übernimmt dann die Ver- und Entschlüsselung der Daten »on the fly«, also während des Betriebs.

Die Software *TrueCrypt* lange Zeit das Mittel der Wahl auf diesem Gebiet und für alle großen Betriebssysteme verfügbar. Allerdings stellten die verantwortlichen Programmierer ihre Arbeit am 28. Mai 2014 offiziell ein.

Mittlerweile gibt es ein Nachfolgeprojekt zu TrueCrypt: die Software *VeraCrypt*, die für Windows, Linux und OS X unter https://veracrypt.codeplex.com heruntergeladen werden kann. VeraCrypt baut auf dem Quellcode von TrueCrypt auf und bietet auch eine Funktion, mit der alte TrueCrypt-Container geöffnet werden können. Die Funktionsweise ist im Großen und

Ganzen dieselbe: Es werden verschlüsselte Container eingerichtet, die wie ein virtueller Datenträger in das System eingebunden werden können. Eine unabhängige Überprüfung der Sicherheit des Quellcodes von VeraCrypt hat noch nicht stattgefunden (Stand Juli 2015). VeraCrypt ist aber Open Source, sodass der Beurteilung durch die Allgemeinheit beziehungsweise unabhängige Experten nichts im Wege steht.

TrueCrypt und sein Nachfolger VeraCrypt bringen noch ein nützliches Feature mit, das Ihnen aus der Patsche helfen kann, wenn Sie sich nicht nur gegen zufällige Mitleser nach Verlust Ihres Datenträgers schützen wollen, sondern jemand es speziell auf Sie abgesehen hat. Wie im vorigen Abschnitt schon kurz erwähnt, wirken eine einzelne oder ein paar verschlüsselte Dateien oder Container verdächtig, wenn es jemand auf Ihre Geheimnisse abgesehen hat. Wenn derjenige Zugriff auf Ihre Person hat, können Sie möglicherweise sogar erpresst oder sonstwie gezwungen werden (beispielsweise, indem Ihnen an der Grenze die Einreise in ein Land verweigert wird), das Passwort preiszugeben. In dieser Situation hilft es, wenn der Angreifer gar nicht weiß, dass es einen verschlüsselten Container gibt. Für solche Fälle bieten TrueCrypt und VeraCrypt die Einrichtung von *unsichtbaren Containern* (hidden containers) an, die innerhalb eines »normalen« verschlüsselten Containers liegen. Wenn Sie gezwungen werden, ein Passwort zu offenbaren, nennen Sie das Passwort des äußeren Containers (der zur Sicherheit ein paar Dateien mit halbwegs sensiblem Inhalt enthalten sollte). Der unsichtbare Container ist nicht zu unterscheiden von zufälligem Datensalat, der im Normalfall den leeren Speicherplatz innerhalb eines verschlüsselten Containers füllt.

Verschlüsselte Container

Vorteile:

- relativ einfach einzurichten
- Container sind auf USB-Stick transportabel und können an mit mehreren Rechnern verwendet werden.
- Je nach verwendeter Software sind Container unabhängig vom Betriebssystem verwendbar.
- einfache Anwendung
- auch für viele Dateien benutzbar, da nicht einzeln verschlüsselt werden muss
- Einrichtung unsichtbarer Container möglich

Nachteile:

- Oft wird Software für Crypto-Container nur für ein Betriebssystem hergestellt und ist nicht kompatibel mit anderen.
- Auch hier gilt: Bei proprietärer Software ist oft schwer einzuschätzen, wie sicher diese wirklich ist.
- Verlieren oder vergessen Sie den Schlüssel, sind Ihre Daten nicht mehr nutzbar.

6.2.3. Dateisystem- und Geräteverschlüsselung

Mittels geeigneter Software, die auch direkt in den Kern des Betriebssystems integriert sein kann, lassen sich auch ganze Partitionen und Geräte verschlüsseln.

Hintergrund

Partition

Als *Partition* bezeichnet man eine Unterteilung eines physikalischen Speichermediums in ein oder mehrere logische Speicherbereiche, die dann jeweils verschiedene *Dateisysteme* beherbergen können. Ein Dateisystem kümmert sich darum, wie einzelne Datenpakete auf dem Medium abgelegt werden. Das Betriebssystem nutzt standardisierte Schnittstellen, um Daten aus dem verwendeten Dateisystem abzurufen oder diese zu speichern.

Standarddateisysteme wie NTFS (Windows), HFS+ (OS X), Ext4 (Linux) sind normalerweise nicht in der Lage, die über sie verwalteten Daten selbst zu verschlüsseln. Allerdings existieren vor allem für Linux-Systeme freie und quelloffene Alternativen, die eine starke Verschlüsselung auf dieser Ebene erlauben. Ein weit verbreitetes Dateisystem zur verschlüsselten Ablage von Daten unter Linux ist beispielsweise EncFS.

Auch in den aktuellen Versionen von Windows und OS X gibt es Mechanismen (BitLocker, FileVault), die dem jeweiligen Standarddateisystem kryptografische Fähigkeiten »überstülpen« und so die Verschlüsselung einzelner Ordner oder eines kompletten Datenträgers erlauben.

Noch einen Schritt weiter gehen kryptografische Erweiterungen sogenannter *Device-Mapper*. Device-Mapper stellen eine Zwischenschicht zwischen dem Betriebssystem auf der einen Seite und der eigentlichen Festplatte (oder beispielsweise einem USB-Stick) auf der anderen Seite bereit und werden vor allem unter Linux-artigen Systemen eingesetzt. Ihre Hauptaufgabe ist die Abstraktion von Speichermedien gegenüber dem Betriebssystem. Sie erlauben es beispielsweise, mehrere kleinere Festplatten so zusammenzufassen, dass diese sich wie ein

einziges, großes Laufwerk verhalten. Durch besagte Erweiterungen, die in nahezu allen aktuellen Linux-Distributionen standardmäßig enthalten sind, lassen sich ganze Festplattenverbände einfach, sicher und transparent (also ohne dass das Betriebssystem etwas davon mitbekommt) verschlüsseln.

Dateisystem- und Geräteverschlüsselung

Vorteile:

- je nach verwendetem Crypto-Dateisystem sehr sicher
- sehr mächtig und für viele Szenarien geeignet
- je nach verwendetem Betriebssystem und verfügbarer Software einfach einzurichten und zu verwalten
- Alle modernen Versionen großer Betriebssysteme unterstützen verschlüsselte Dateisysteme oder vergleichbare Mechanismen.
- Vollverschlüsselung des gesamten Betriebssystems und Bootvorgang von verschlüsselter Festplatte in den meisten Fällen ohne großen Aufwand möglich

Nachteile:

- Vor allem bei proprietären Lösungen wie FileVault und BitLocker ist die Sicherheit schwer abzuschätzen, da der Quellcode nicht einsehbar ist (wie auch bei Datei- und Container-Verschlüsselung).
- Der Verlust der Passphrase führt zum Verlust sämtlicher Daten, hat also potenziell noch schwerere Konsequenzen als beispielsweise bei der Verschlüsselung einzelner Dateien.
- Derartig verschlüsselte portable Speichermedien lassen sich nicht ohne Weiteres mit unterschiedlichen Betriebssystemen nutzen.

6.2.4. Hardwareverschlüsselung

Analog zu den softwarebasierten Device-Mappern gibt es auch Hardware, die in der Lage ist, Speichermedien verschlüsselt zu betreiben. Spezielle USB-Sticks, Festplatten-Controller und Mainboards besitzen die Fähigkeit, dem Betriebssystem mitzuteilen (leider oft erst nach Installation zusätzlicher Software), dass das angeschlossene Speichermedium verschlüsselt ist und dass es erst nach der Eingabe des richtigen Passworts benutzt werden kann. Die eigentliche Ver- und Entschlüsselung übernimmt dann meistens ein speziell dafür

vorgesehener Hardwarebaustein. Viele moderne Mainboards mit diesen Fähigkeiten sind heute sogar in der Lage, noch vor dem Bootvorgang die erforderliche Passphrase abzufragen, um dann von der verschlüsselten Festplatte das Betriebssystem starten zu können. Auch die Freigabe eines Datenträgers durch Eingabe biometrischer Daten (zum Beispiel über einen Fingerabdruck-Scanner) oder durch Chipkarten ist so möglich. Viele dieser Lösungen finden allerdings nur im Unternehmensumfeld Anwendung und sind entsprechend teuer. Zudem ist die Schlüssellänge (siehe Kapitel 2) eines Fingerabdruckes oder Iris-Scans oft wesentlich kürzer als eine gut gewählte Passphrase. Werden diese Mechanismen jedoch zusätzlich zu einem Passwort eingesetzt, kann die Sicherheit durch eine solche *Multifaktor-Authentifizierung* signifikant erhöht werden.

Hardwareverschlüsselung

Vorteile:

- einfache Handhabung
- je nach verwendeter Technik sehr starke Verschlüsselung
- optional zusätzliche Sicherheit durch Multifaktor-Authentifizierung

Nachteile:

- Die verwendeten Bausteine sind in der Regel proprietär, sodass die Sicherheit nicht durch unabhängige Dritte überprüft werden kann.
- Oft ist zusätzliche Software erforderlich, um solche Hardware zu betreiben; zudem kann diese ebenfalls Sicherheitslücken aufweisen.
- Wird zusätzliche Software benötigt, kann sie oft nur unter Windows oder OS X verwendet werden, da sich die Hersteller die Entwicklung für andere Betriebssysteme sparen.
- Entsprechende Hardware guter Qualität ist oft um ein Vielfaches teurer als Standardhardware, daher lohnt sich die Anschaffung für Privatpersonen nur in Einzelfällen.

6.3 Exkurs Kryptografie im Alltag: Neuer Personalausweis und

Gesundheitskarte

Mittlerweile hat sich der Nutzen von digitaler Datenübermittlung und der dazu notwendigen Verschlüsselung so weit herumgesprochen, dass selbst so behäbige Institutionen wie Krankenkassen und der deutsche Staat sie für ihre Zwecke nutzen wollen. In diesem Zusammenhang stellen wir Ihnen daher hier den neuen Personalausweis (nPA) und die elektronische Gesundheitskarte (eGK) vor.

Wenn Sie im gleichen Alter oder älter als die Autoren dieses Buchs sind, ist es schon ein paar Jahre her, dass Sie an der Supermarktkasse nach Ihrem Personalausweis gefragt wurden, als Sie einen Kasten Bier für den Grillabend oder eine Flasche Rum für die Weihnachtsbäckerei gekauft haben. Wenn die Kassiererin anzweifelt, dass Sie das gesetzliche Mindestalter erreicht haben, ist das schmeichelhaft, aber lästig. Dass Sie die Zweifel beiseite räumen können, indem Sie Ihren Personalausweis (zärtlich »Perso« genannt) vorzeigen, ist nicht selbstverständlich.

Bis über den Ersten Weltkrieg hinaus gab es in Deutschland weder Personalausweisnoch Ausweispflicht. Eine »Kennkarte« als Vorläufer des heutigen Personalausweises wurde erst im Nationalsozialismus eingeführt und zugleich für bösartige Zwecke eingesetzt, denn die Pflicht, sich auf Aufforderung der Autoritäten mittels Kennkarte auszuweisen, bestand nur für Juden. Seit 1951 gab es einen Personalausweis in West- und ab 1953 auch in Ostdeutschland, noch in Form von Papierheftchen. Seit 1987 hat der Personalausweis Kartenformat und wird als »fälschungssicher« bezeichnet – eine eher unglückliche Namensgebung, da Dokumente immer genau so lange fälschungssicher sind, bis jemand sie zum ersten Mal fälscht.

Auch dieser Personalausweis, den die meisten von Ihnen wohl noch kennengelernt haben, wurde 2010 durch einen neuen ersetzt: den »*neuen Personalausweis*« (nPA). Der nPA hat die Größe einer Scheckkarte und ist somit kleiner als der vorige. Außerdem enthält er neben den Personaldaten und dem Foto auch die Möglichkeit, zwei Fingerabdrücke einzuspeichern. Alle diese Daten sind in einem in die Karte eingebetteten Transponder gespeichert. Dieser Transponder oder RFID-Chip ist ein Bauteil, das durch elektromagnetische Wellen ohne direkten Kontakt mit Lesegeräten kommunizieren kann. Andere Beispiele für den Einsatz von

RFID-Chips sind zum Beispiel Diebstahlsicherungen in Kaufhäusern und Supermärkten oder die Kennzeichnung von Haustieren, denen solche Chips unter der Haut eingepflanzt werden können.

Wenn Sie einen nPA beantragen, wird in jedem Fall Ihr Foto im RFID-Chip gespeichert (und natürlich auf den Personalausweis aufgedruckt). Zudem können Sie zwei Ihrer Fingerabdrücke speichern lassen – das ist aber freiwillig. Digital gespeichertes Foto und Fingerabdrücke bezeichnet man als *biometrische Daten*.

Ihr nPA bringt dann eine Reihe von Funktionen mit, die der alte Ausweis nicht hatte und die durch den RFID-Chip ermöglicht werden. Man unterscheidet *hoheitliche* und *nicht hoheitliche Funktionen*, je nachdem, wer Zugriff hat:

Nur staatliche Stellen (zum Beispiel Polizei, Standesamt, Zoll) dürfen auf Ihre biometrischen Daten zugreifen und Ihren nPA damit als biometrisches Personaldokument nutzen, also als Alternative zum elektronischen Reisepass.

Auf die elektronische Identifikationsfunktion (eID) und die damit verbundene Qualifizierte Elektronische Signatur (QES) dürfen dagegen private Unternehmen zugreifen, die ein entsprechendes Zertifikat beantragt haben, und auch solche Behörden, die nicht auf die biometrischen Daten zugreifen dürfen (zum Beispiel die Kfz-Zulassungsstelle). Ob Sie eID und QES auf Ihrem Personalausweis aktivieren lassen, bleibt aber Ihnen überlassen.

Mit Hilfe der eID können Sie im Internet Ihre Identität nachweisen. Zu diesem Zweck können folgende Angaben im Chip gespeichert werden:

- Vor- und Nachname (und, wenn vorhanden, Geburtsname, Künstlername, Doktorgrad)
- Geburtstag, Geburtsort
- Anschrift
- Alter (nicht in Jahren oder Monaten – nur das Erreichen einer Altersgrenze, beispielsweise zum Kauf von Zigaretten, kann abgeglichen werden)
- Wohnort
- pseudonyme Kartenkennung
- ausstellendes Land (also Deutschland)

Bei jedem Einsatz der eID-Funktion, beispielsweise beim Onlineshopping, können Sie selbst entscheiden, welche der oben aufgelisteten Angaben mit übertragen wird. Auf jeden Fall mit

übertragen wird lediglich eine Angabe zur Gültigkeit und, wenn vorhanden, ein Sperrvermerk. Eine Sperrung können Sie selbst veranlassen, sodass es einem Dieb hoffentlich nicht gelingt, mit Ihrem gestohlenen nPA in einem Onlineshop einzukaufen.

Jedes Unternehmen, das per Internet oder persönlich mit Lesegerät die oben aufgelisteten Angaben von Ihnen abfragen will, muss dazu ein Zertifikat bei der Bundesdruckerei oder der Deutschen Post beantragen. Ein solches Zertifikat wird nur unter der Voraussetzung ausgestellt, dass das Unternehmen ein sogenanntes »kreditorisches Risiko« trägt, also Nachteile davon hat, wenn Sie nicht zahlen oder nicht kreditwürdig sind. Das ist dann zum Beispiel der Fall, wenn ein Händler Waren an Sie auf Rechnung ausliefert – nicht, wenn er von Ihrer Kreditkarte abbucht oder nach Vorkasse liefert.

Um die eID-Funktion Ihres nPA im Internet nutzen zu können, brauchen Sie im Moment noch ein Lesegerät. Getüftelt wird aber schon an einem Smartphone, mit dem Sie den nPA ohne Lesegerät auslesen können. Wenn Sie ein Lesegerät haben, können Sie sich übrigens unter https://www.ausweisapp.bund.de/ausweisapp2/ anzeigen lassen, welche Daten auf Ihrem nPA gespeichert sind.

Die eID-Funktion hat noch eine Erweiterung: die *qualifizierte elektronische Signatur* (QES), die die gleiche rechtliche Beweiskraft hat wie Ihre eigenhändige Unterschrift.

Ein ähnliches Projekt wie der neue Personalausweis ist die *elektronische Gesundheitskarte* (eGK), deren Einführung in Deutschland gesetzlich vorgeschrieben wurde. Die eGK ersetzt die bisherige Versichertenkarte der gesetzlich Krankenversicherten, hat aber zusätzlich noch weitere Funktionen. Bestimmt sind auch Sie schon von Ihrer Krankenkasse aufgefordert worden, ein Foto für die eGK einzureichen. Wenn Sie der Aufforderung nachgekommen sind, haben Sie kurz darauf Ihre neue eGK in den Händen gehalten.

Zur Speicherung von Daten und zum Ausführen von Funktionen trägt die eGK einen Mikroprozessor anstatt des einfachen Speicherchips der alten Karte. Zusätzlich zu Ihrem Namen, Adresse, Geburtsdatum und Versicherungsstatus, die schon auf der alten Karte gespeichert waren, kommt bei der neuen Karte verpflichtend noch das

- elektronische Rezept (eRezept)

hinzu. Das eRezept soll das bisherige auf Papier ausgestellte Rezept ersetzen. Statt das altbekannte rosa Formular auszufüllen und per Hand zu unterschreiben, erstellt der Arzt dieses Rezept am Computer, speichert es auf der eGK und bringt mithilfe seines elektronischen

Arztausweises eine digitale Signatur an. Der Apotheker wiederum kann das Rezept nur mithilfe seines elektronischen Apothekerausweises lesen.

Weitere bisher nur geplante neue Funktionen (Stand Juli 2015), die (noch) freiwillig sein sollen, sind

- die elektronische Patientenakte (EPA) und
- der Notfalldatensatz.

Auf beides soll nur mittels eines elektronischen Heilberufeausweises (HBA)zugegriffen werden, den beispielsweise Ärzte und Apotheker besitzen.

Bund und gematik, die für die Entwicklung und Einführung der eGK zuständige Gesellschaft, versprechen den Krankenkassen, Ärzten und Ihnen und uns als Patienten eine Reihe von Vorteilen durch die neue Karte:

Den Versicherungen wird in Aussicht gestellt, dass der Missbrauch von Versichertenkarten verringert wird, da die eGK, im Gegensatz zur alten Karte, ein Foto des Versicherten trägt. Ausnahmen soll es nur für Kinder unter 15 Jahren geben und für bettlägerige Patienten, die sich nicht zum Fotografen begeben können. Lustigerweise ist aber im Prozedere der Kartenausgabe an die Versicherten gar kein Arbeitsschritt enthalten, mit dem sichergestellt wird, dass ein eingesandtes Foto tatsächlich den Versicherten zeigt. Wenn Sie also statt Ihres eigenen Porträts ein Bild von Angelina Jolie einsenden, mag das einem aufmerksamen Sachbearbeiter bei der Krankenkasse noch auffallen – ein Foto Ihrer Nachbarin wird aber mit Sicherheit nicht beanstandet werden. Aus diesem Grund warnen Juristen, dass der Zugriff auf die Daten eines Patienten bei der Krankenkasse (die Versichertenstammdaten) per eGK gar nicht rechtmäßig ist und gegen Datenschutzbestimmungen verstößt.

Ärzte sollen von der Einführung der eGK den Vorteil haben, dass keine veralteten Stammdaten mehr eingelesen werden, weil bei jedem Einlesen der neuen Karte die aktuellen Daten online von den Servern der jeweiligen Krankenkasse geladen werden. Das ist gleichzeitig ein Nachteil für die betreffenden Ärzte, da die Aktualisierung der Daten in den Praxen, nicht bei den Krankenkassen, erfolgen soll.

Zudem soll die Behandlung von Patienten einfacher werden, da durch die Nutzung einer elektronischen Patientenakte die Vorgeschichte und Befunde eines Patienten zentral verfügbar sind und nicht, möglicherweise lückenhaft, von mehreren Stellen angefordert werden müssen. Im Notfall oder am Wochenende sind diese Informationen zudem vielleicht überhaupt nicht zu

bekommen. Ganze Untersuchungen müssen in solchen Fällen doppelt oder mehrfach erfolgen – zu Lasten der Krankenkassen und Patienten. Die zentrale Speicherung von sensiblen Patientendaten ist aber gleichzeitig ein massives Sicherheitsrisiko, weil durch einen Angriff auf die Infrastruktur der eGK gleich Millionen von Patientenakten in die Hände des Angreifers geraten würden. (Es wird übrigens geschätzt, dass der Wert einer Patientenakte auf dem Schwarzmarkt zwischen 60 und 100 Euro liegen soll.)

Den Patienten soll ebenfalls die zentralisierte Verwaltung der medizinischen Vorgeschichte zugute kommen. Wenn beispielsweise Ihre alte Tante, die vom Hausarzt zwei verschiedene Blutdruck-Tabletten bekommt, vom Augenarzt ein weiteres Medikament verschrieben bekommt, das mit diesen unverträglich ist, fällt das heute nicht ohne Weiteres auf, wenn Ihre Tante nicht selbst darauf achtet. Wenn jeder Arzt jedoch alle aktuellen und früheren Medikamente angezeigt bekommt und auch Allergien mit gespeichert sind, können Zwischenfälle durch Medikamentenunverträglichkeiten verhindert werden. Allerdings gestattet die eGK keinen Zugriff, auch keinen reinen Lesezugriff, durch die Patienten selbst. Eine Kontrollmöglichkeit, die in der Hand der Patienten liegen würde, fällt also weg.

Zu guter Letzt soll der Notfalldatensatz auf der eGK bei akuten lebensbedrohlichen Erkrankungen dem Notarzt helfen, eine schnelle lebensrettende Therapie einzuleiten. Die Notfallakte soll unter anderem Diagnosen und verordnete Medikamente enthalten, Allergien, die Kontaktdaten des Hausarztes sowie einer im Notfall zu benachrichtigenden Person. Um sie von Ihrer regulären Patientenakte zu trennen, ist geplant, die Abfragen zu protokollieren – jede Notfallabfrage wird auf der Karte gespeichert, und außerhalb von Notfällen ist Ihr explizites Einverständnis notwendig, um die Daten abzurufen.

Eine Reihe von Vereinen und Verbänden von Patienten, Ärzten und Datenschützern unterstützen das Bündnis »Stoppt die e-Card« (www.stoppt-die-e-card.de). Dieses setzt sich, wie der Name schon sagt, dafür ein, die Einführung der eGK rückgängig zu machen.

Das Bündnis »Stoppt die e-Card« und andere Kritiker der eGK empfehlen den Versicherten, so lange wie möglich an ihren alten Versichertenkarten festzuhalten und die Ausstellung einer eGK zu boykottieren, beispielsweise durch Einsendung eines falschen Fotos. Sie weisen darauf hin, dass Kassenpatienten sich auch ohne Vorlage eines Versichertenausweises behandeln lassen können. In der Tat ist es so, dass Sie ohne Vorlage einer Versichertenkarte zum Arzt gehen können. In der Regel müssen Sie in einem solchen Fall die Versichertenkarte innerhalb

von zehn Tagen nachreichen, ansonsten darf der Arzt Ihnen eine private Rechnung schicken. Diese können Sie selbst bezahlen und anschließend bei Ihrer Krankenkasse einreichen (ähnlich wie bei einer privaten Krankenversicherung). Alternativ können Sie versuchen, statt der Versichertenkarte eine schriftliche Versicherungsbestätigung Ihrer Krankenkasse vorzulegen. Sollte es hierbei allerdings zu Problemen kommen, bleiben Sie im Zweifelsfall auf den Kosten der Behandlung sitzen.

Wenn Sie (zu recht) um die Sicherheit Ihrer auf der eGK gespeicherten Patientendaten besorgt sind, empfehlen wir, auf die Speicherung der freiwilligen Informationen zu verzichten (bis möglicherweise eines Tages die Infrastruktur datenschutzfreundlicher gestaltet wird).

6.4 A rose by any other name – Pseudonymität und Anonymität

An mehreren Stellen in diesem Buch ging es bereits darum, wie Sie im Internet anonym bleiben können, um Ihre Daten zu schützen. Was aber bedeutet es, anonym zu sein?

Wörtlich bedeutet anonym »ohne Namensnennung«. Wir können uns wahrscheinlich darauf einigen, dass Sie, wenn Sie bei Amazon unter Ihrem wahren Namen ein Buch über das Bierbrauen bestellen und an Ihre private Adresse liefern lassen, überhaupt nicht anonym sind. Wenn Sie in ein Internetcafé marschieren und dort über einen Tor-Browser eine Webseite mit Anleitungen zum Bierbrauen lesen, bleiben Sie vermutlich vollständig anonym – vorausgesetzt, Sie benutzen dabei nicht Ihr Smartphone, und der Besitzer des Internetcafés kennt Sie nicht.

Was aber, wenn Sie schon seit mehreren Jahren unter dem Namen Hopfenhilde79 mit anderen Hobbybierbrauern Rezepte austauschen? Die anderen Forenbenutzer wissen, wie alt Sie sind, aus welcher Region Sie stammen und was Ihre Lieblingsbiere sind. Sie wissen vielleicht auch, ob Sie in einer Wohnung oder einem Haus leben, ob Sie einen Keller haben und ob Sie Groß- oder Kleinstädterin sind. Möglicherweise überlegen Sie auch gemeinsam mit den anderen Brauern aus dem Forum, sich mal zu einem Kölsch-Workshop in Köln (oder auch zu einem Alt-Workshop in Düsseldorf) zu treffen. Wenn die anderen dann sehen, welche Person sich hinter dem Namen Hopfenhilde79 verbirgt, auch wenn Sie nicht Ihren Personalausweis herzeigen – sind Sie dann immer noch anonym?

Und was, wenn Sie eine berufliche Webseite mit Beispielen für erfolgreich abgeschlossene Projekte haben, und daneben eine private Webseite, auf der Sie Bierrezepte sammeln, für beide aber die gleiche, öffentlich sichtbare E-Mail-Adresse benutzen?

Sie sehen also: Zwischen Anonymität und der völligen Preisgabe Ihrer Identität und persönlichen Daten besteht kein scharfer Kontrast, sondern ein Spektrum von Möglichkeiten.

Wie Sie bereits in Kapitel 1 erfahren haben, gewinnen an sich harmlose oder unwichtige Daten oft an Wert und Brisanz, wenn man sie mit anderen Daten sinnvoll in Zusammenhang bringen kann. Aus so einem Datenpuzzle lassen sich oft Informationen rekonstruieren, die von jemandem eigentlich als privat gehütet werden. Dies wird als Vernetzbarkeit oder Verkettbarkeit von Daten bezeichnet (englisch »linkability«). Auch Anonymität wird durch Verkettbarkeit von Daten aus verschiedenen Quellen gefährdet, wie Sie in obigem Beispiel schon gesehen haben.

So wichtig Anonymität für Datenschutz und Wahrung der Privatsphäre auch ist – in vielen Fällen ist es wünschenswert, dass andere Menschen gewisse Informationen mit Ihrer Person verknüpfen können. Im Falle des Bierbrau-Forums möchten Sie bestimmt, dass andere Benutzer Ihre alten Beiträge lesen können, weil Sie schon viele wertvolle Tipps zum richtigen Umgang mit Hefe gegeben haben. Aus diesem Grund haben Sie sich den Benutzernamen Hopfenhilde79 zugelegt.

Wenn Sie sich entscheiden, in irgendeiner Beziehung in der digitalen Welt (sei es in einem Forum, bei der E-Mail-Kommunikation oder in einem Multiplayer-Computerspiel) einen anderen als den Namen aus Ihrem Personalausweis anzugeben, verwenden Sie ein *Pseudonym*. Wenn dieses Pseudonym nach und nach mit mehr persönlichen Informationen verknüpft wird, die Sie identifizierbar machen, entsteht eine *digitale Identität*.

Sobald andere Menschen persönliche Informationen über Sie kennen, anhand derer man Sie aus einer Gruppe von Menschen heraus identifizieren könnte, sind Sie nicht mehr anonym. Sie sehen also, dass Anonymität gar nicht so viel mit der Geheimhaltung oder Preisgabe des Namens zu tun hat, der in Ihrem Personalausweis steht. Wenn eine gewisse Caryn Johnson in Ihrem Onlineforum posten würde, dass sie Bier für ein ekelhaftes Gesöff hält, und Ihnen empfiehlt, Ihre Zeit doch lieber mit etwas Sinnvollem zu verbringen, hätten Sie das vermutlich am nächsten Tag schon wieder vergessen. Wenn diese Aussage dagegen von Whoopi Goldberg stammen würde, würde sich wahrscheinlich schon die eine oder andere Augenbraue heben,

und im Sommerloch wäre es vielleicht sogar eine Meldung in der Rubrik »Aus aller Welt« der Tageszeitung wert. Im Fall von Caryn Johnson, die fast ihr ganzes Berufsleben lang unter dem Pseudonym Whoopi Goldberg gearbeitet hat, ist also das Pseudonym mittlerweile informativer als der Geburtsname.

Das Fazit: Wenn Sie im Internet anonym, also nicht identifizierbar, bleiben wollen, genügt es nicht, einen anderen Namen als den aus Ihrem Personalausweis zu verwenden. Sie müssen genauso darauf achten, dass die digitalen Informationsspuren, die Sie hinterlassen, nicht miteinander verknüpft werden können, beispielsweise anhand einer gemeinsamen E-Mail-Adresse.

Wenn Ihr Ziel nicht die völlige Anonymität ist, sondern die Kontrolle darüber, wer was über Sie erfährt, zahlt es sich aus, für verschiedene Zwecke verschiedene Identitäten anzulegen. Wenn Sie später zwei Identitäten miteinander verschmelzen wollen (wenn zum Beispiel auch Ihre Kunden oder Arbeitskollegen erfahren sollen, wie beliebt Ihre selbstgebrauten Biere in der Community mittlerweile sind), können Sie das jederzeit tun. Anders herum geht es leider nicht – Informationen, die einmal freigelassen wurden, können Sie kaum wieder einfangen.

6.5 Für Vergessliche und solche, die es werden wollen –

Passwort-Manager

Passwörter spielen eine zentrale Rolle bei der Nutzung von Onlinediensten jeglicher Art. Die meisten Menschen, von den Gedächtnissportlern unter uns mal abgesehen, sind eher faul, wenn es darum geht, abstrakte Zeichenkolonnen auswendig zu lernen. Daher neigen wir (die Autoren dieses Buches ausdrücklich eingeschlossen) dazu, Passwörter zu wählen, die man einfach und ohne viele Wiederholungen in den Kopf bekommt.

Nehmen Sie an, Sie hätten es nach mehreren Anläufen geschafft, ein Passwort zu erfinden, das Sie sich nicht nur einfach merken können, sondern das auch noch ziemlich sicher (also zum Beispiel lang und nicht aus realen Wörtern bestehend) ist. Aus Bequemlichkeitsgründen verwenden Sie es nicht nur für Ihr Google-Mail-Konto, sondern auch für Facebook, Twitter, Amazon und Plüschpantoffel24, einen kleinen Onlineshop, bei dem Sie im letzten Jahr ihre

derzeitigen Lieblingspantoffeln gefunden haben. Die Shopbetreiber, ein kleines Familienunternehmen aus dem Harz, haben es vielleicht versäumt, kritische Sicherheitslücken in der Shopsoftware durch entsprechende Updates zu schließen. Eine dieser Sicherheitslücken ermöglicht es irgendwann einem Angreifer, die gespeicherten Kundendaten samt Passwörtern auszulesen. Obendrein sind Letztere dummerweise im Klartext in der Datenbank hinterlegt. So muss der Eindringling sich nicht mal die Mühe machen, diese wieder in eine lesbare Form zu bringen. Davon bekommen Sie als Kunde und auch die Betreiber des Shops zunächst nichts mit.

Eines Tages wundern Sie sich allerdings darüber, dass Sie sich plötzlich nicht mehr in Ihrem Amazon-Konto anmelden können. Genervt von sich selbst (weil Sie denken, Sie seien nicht mehr fähig, ein Kennwort korrekt einzugeben) klicken Sie auf den Passwort-vergessen-Link, geben Ihre E-Mail-Adresse an und senden das Formular ab. In der Hoffnung, dass Amazon Ihnen nun einen Link geschickt hat, mit dem Sie ein neues Passwort wählen können, rufen Sie nun Google Mail auf. Auch hier stellen Sie fest, dass Sie sich nicht mehr in Ihrem Konto anmelden können. Zu allem Überfluss informiert Sie ein guter Freund später am Tag telefonisch darüber, dass anscheinend jemand Ihren Facebook-Account übernommen hat und fleißig versucht, Ihre Freunde, Bekannten und Verwandten davon zu überzeugen, dass Sie gerade in Australien festsitzen und dringend Geld benötigen, um wieder nach Hause zu kommen.

Zugegeben, dieses Szenario wirkt auf den ersten Blick etwas konstruiert, hat sich aber so ähnlich schon oft zugetragen. Auf die eigentliche Ursache des Problems haben Sie als Nutzer zunächst keinen Einfluss. Ihnen war weder bewusst, welche Shopsoftware bei Plüschpantoffel24 eingesetzt wird, noch dass diese erhebliche Sicherheitslücken aufwies. Derartige Probleme können übrigens nicht nur bei kleinen Onlineangeboten auftreten, sondern auch bei großen Konzernen, die viel mehr Geld in die Sicherheit ihrer Infrastruktur investieren (Adobe-Hack November 2013[2], Vodafone-Hack September 2013[3] und Playstation Network Hack von 2011[4]). Daher hilft es an dieser Stelle nicht weiter, nur auf die Fähigkeiten und Weitsicht der großen Unternehmen zu vertrauen.

Weitaus mehr Einfluss haben Sie in dieser Situation allerdings auf die Begrenzung Ihres persönlichen Schadens. Nehmen Sie an, Sie hätten im oberen Beispiel für jeden einzelnen Dienst ein einmaliges, möglichst sicheres Passwort verwendet. In diesem Falle könnte besagter Angreifer sich zwar auf Ihre Kosten für die nächsten Jahre mit hochwertigen Plüschpantoffeln

eindecken, aber Ihr Amazon-, Facebook- und vor allem Ihr Google-Mail-Konto blieben für ihn unzugänglich. Letzteres nimmt übrigens in der heutigen Zeit eine Sonderrolle ein, da Sie bei den meisten Onlinediensten Ihr Passwort mithilfe Ihres Mail-Accounts jederzeit zurücksetzen können. Befindet sich Ihr Mail-Account unter der Kontrolle eines Angreifers, stehen diesem potenziell auch Ihre anderen Online-Accounts offen.

Sich viele verschiedene Passwörter auszudenken, die möglichst lang und schwer zu erraten sind und sich diese dann auch zu merken zu müssen, stellt Sie allerdings vor eine schwierige Aufgabe. Sie auf einen Schmierzettel zu schreiben oder in einer Textdatei auf dem Desktop zu speichern, ist, wie Sie bereits wissen, eine Idee, von der wir dringend abraten. Helfen kann Ihnen an dieser Stelle aber ein sogenannter Passwort-Manager. Das ist eine Software, mit deren Hilfe Sie Zugangsdaten und zugehörige Informationen in einer verschlüsselten Datei speichern können. Dazu werden in der Regel symmetrische Verschlüsselungsverfahren verwendet, die hinreichend getestet und für sicher befunden wurden. Um an die so gespeicherten Zugangsdaten zu gelangen, geben Sie beim Start des Programms lediglich ein Master-Passwort ein, das Sie sich merken müssen.

Die meisten Programme dieser Art unterstützen Sie nicht nur dabei, sich viele verschiedene Zugangsdaten zu merken, sondern helfen Ihnen auch bei der Generierung sicherer Passwörter und deren einfacher Verwendung in Ihrem Browser. Grundsätzlich ist es so auch möglich, die Passwortdaten über Dropbox oder ähnliche Datendienste auf mehreren Geräten gleichzeitig zu nutzen – aufgrund der starken Verschlüsselung sollte das relativ unbedenklich sein. Wenn Sie allerdings ein schlechtes Gefühl bei der Sache haben, was vollkommen legitim ist, tut es aber auch ein kleiner USB-Stick, den Sie mit sich tragen.

Nahezu alle gängigen Browser besitzen heute integrierte Lösungen, um Zugangsdaten für Ihre Onlinedienste abzuspeichern und für die spätere Verwendung vorzuhalten. Wie wir an anderer Stelle schon besprochen haben, ist es aber vor allem bei proprietären Programmen schwer zu beurteilen, wie gut die entsprechende Datenbank verschlüsselt ist – das gilt auch für Passwortdatenbanken von Browsern. Die Datenbanken von Open-Source-Browsern sollten tendenziell eher sicher sein, da die Open-Source-Community Sicherheitslücken vermutlich gefunden hätte (auch wenn es dafür keine Garantie gibt). Ansonsten bestünde die Gefahr, dass Schadsoftware auf Webseiten, die Sie besuchen, die Passwortdatenbank ausliest. Daneben

macht es auch wenig Sinn, Passwörter, die Sie nur für Offline-Anwendungen nutzen, im Passwort-Manager Ihres Browsers zu hinterlegen.

Wenn Sie die Nutzung eines separaten Passwort-Managers überlegen, sollten Sie daran denken, dass Sie auf Ihre dort verschlüsselten Zugangsdaten nicht mehr zugreifen können, wenn Sie das Master-Passwort vergessen. Wird das Speichermedium oder die auf ihm enthaltene Passwortdatenbank beschädigt, haben Sie das gleiche Problem. In letzterem Fall helfen Ihnen regelmäßige Back-ups der Passwortdatenbank auf einem USB-Stick, den Sie danach am besten in Ihrem Safe oder an einem anderen sicheren Ort deponieren.

Ein weit verbreiteter kommerzieller Passwort-Manager ist 1Password von AgileBits (siehe Abbildung 6.1). Die Software gibt es bisher für OS X, iOS, Windows und Android. Sie eignet sich besonders für Anfänger, da sie sehr einfach zu verstehen und anzuwenden ist. Neben vielen nützlichen Features liefert der Hersteller Plug-ins für die Browser Opera, Safari, Firefox und Chrome. Die Anschaffung hat allerdings ihren Preis, und 1Password ist proprietäre Software. Daher ist eine unabhängige Beurteilung der Sicherheit des Programms, wie schon gesagt, schwierig.

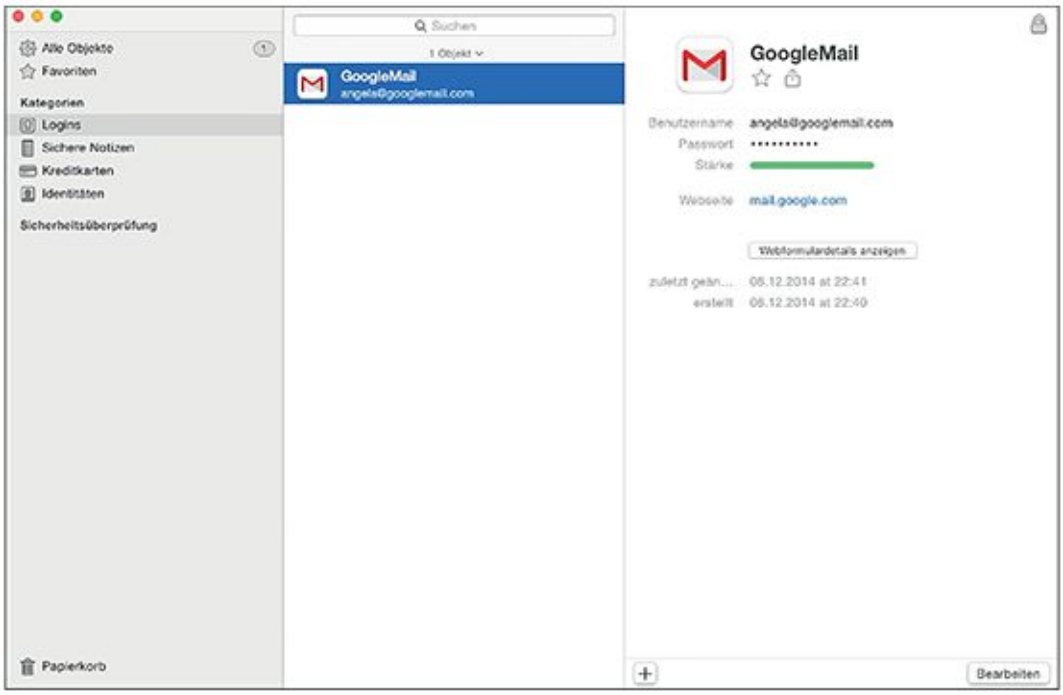


Abb. 6.1 Passwort-Manager 1Password

Eine Alternative zu 1Password ist KeePassX (siehe Abbildung 6.2). Das kostenlose Programm wird von Freiwilligen entwickelt und kann durch Spenden unterstützt werden. Es ist für OS X,

Windows und Linux verfügbar und verschlüsselt die gespeicherten Zugangsdaten mit dem *Advanced Encryption Standard*, kurz *AES*, oder der *Twofish*-Chiffre. KeePassX ist Open Source und daher jederzeit für eine unabhängige Prüfung des Quellcodes durch Dritte zugänglich.

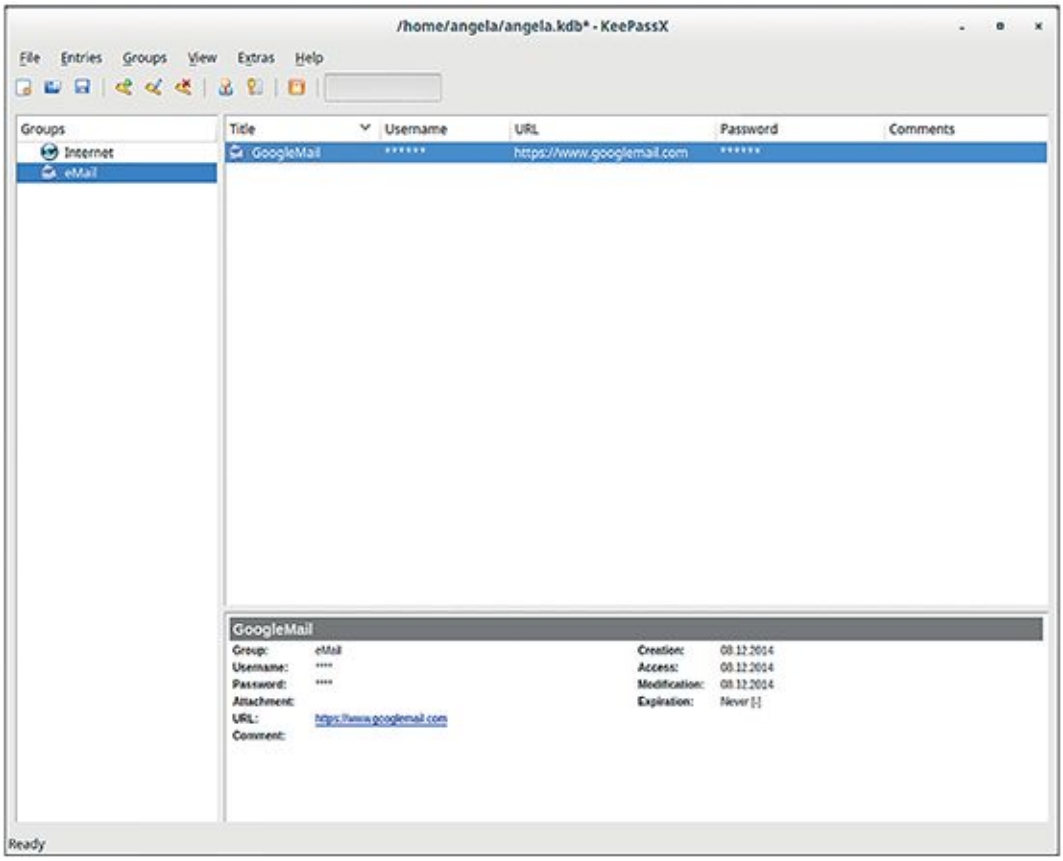


Abb. 6.2 Passwort-Manager KeePassX

Wenn Sie einen Passwort-Manager einsetzen wollen, informieren Sie sich im Vorfeld gründlich über dessen Fähigkeiten und eventuelle Sicherheitsprobleme. Gerne helfen Ihnen hier auch Menschen oder Organisationen weiter, die Cryptoparties veranstalten (https://www.cryptoparty.in/parties/upcoming).

Es gibt Kennwörter, die Sie trotzdem besser nicht ausschließlich in einem Passwortsafe aufbewahren, sondern auswendig kennen sollten. Das sind wie bereits erwähnt solche, die eine zentrale Rolle bei der Wiedererlangung von verlorenen Zugangsdaten spielen – zum Beispiel die Log-in-Daten zu Ihrem primären E-Mail-Account. Haben Sie diese im Kopf, stellen Sie damit sicher, dass Sie selbst bei komplettem Verlust der Passwort-Manager-Datenbank nicht die Kontrolle über alle darin enthaltenen Zugänge verlieren, sondern diese mit ein wenig Geduld mit neuen Passwörtern versehen und wieder nutzen können.

6.6 Tunnel durch Feindesland – VPNs

Vielleicht haben Sie schon einmal den Begriff Virtual Private Network(kurz VPN) gehört und haben eine Technologie dieses Typs auch bereits verwendet, eventuell ohne es zu merken. Wenn Sie zu den glücklichen Menschen gehören, die in regelmäßigen Abständen von zu Hause aus für Ihren Arbeitgeber tätig sind, ist das sogar sehr wahrscheinlich. Um von Ihrem heimischen Arbeitsplatz auf Dienste, die sonst nur innerhalb des Firmennetzwerks erreichbar sind, zuzugreifen, nutzen Sie einen sogenannten VPN-Client. Diese Software authentifiziert Sie zunächst gegenüber dem VPN-Server und handelt mit diesem eine verschlüsselte Verbindung aus, über die eine Datenübertragung durch einen geschützten »Tunnel« durch das Internet erfolgt. Ihr Unternehmen kann Ihnen auf diesem Wege interne Dienste (beispielsweise Zugriff auf die Telefonanlage oder Verwaltungssoftware) zur Verfügung stellen, ohne diese dem gesamten Internet und potenziellen Angreifern auszusetzen. Im Idealfall können Sie dann Ihrer Arbeit so nachgehen, als säßen Sie persönlich an Ihrem Schreibtisch im Büro.

VPNs sind eine ganze Gruppe von unterschiedlichen Technologien, die es Ihnen ermöglichen, verschlüsselte Datenverbindungen zwischen zwei Punkten durch ein nicht vertrauenswürdiges Netzwerk hindurch herzustellen.

Beim Aufbau einer Datenverbindung stellt Ihr VPN-Client lediglich eine Netzwerkverbindung zu einem in der Konfiguration hinterlegten VPN-Server her. Server und Client handeln dann mittels eines geeigneten sicheren Austauschverfahrens (siehe Kapitel 2) einen geheimen Schlüssel aus, mit dem die weitere Kommunikation chiffriert wird. Aus technischer Sicht verhält sich ein VPN-Client nach dem Verbindungsaufbau ähnlich wie eine zusätzliche Netzwerkkarte in Ihrem Computer. Wenn Ihr Rechner ein Datenpaket an einen anderen Teilnehmer schicken möchte, von dem er weiß, dass dieser nur über die virtuelle Verbindung erreicht werden kann, passiert im Grunde Folgendes: Der installierte VPN-Client nimmt das Datenpaket an und verschlüsselt es mit dem zwischen ihm und dem Server ausgetauschten symmetrischen Schlüssel. Danach stopft er es in ein weiteres Datenpaket, welches er an den VPN-Server adressiert, und versendet es über die normale Netzwerkverbindung Ihres Rechners. Der Server empfängt seinerseits das Paket, dechiffriert es mit dem gemeinsamen Schlüssel und leitet es gemäß seiner ursprünglichen Adressierung an den Empfänger weiter.

Ein Angreifer kann eine so verschlüsselte Netzwerkverbindung zwar gezielt zwischen Client und Server abfangen und die gesamte Kommunikation mitschneiden, allerdings ist er nicht in

der Lage, die übertragenen Daten zu entschlüsseln, solange er den verwendeten Schlüssel nicht kennt. Ein wichtiges Feature moderner VPN-Technologien ist zudem Perfect Forward Secrecy (siehe Kapitel 2). Es stellt sicher, dass die übertragenen Daten im Nachhinein auch dann nicht vollständig entschlüsselt werden können, wenn ein Angreifer tatsächlich irgendwann in den Besitz des geheimen Schlüssels gelangen sollte.

Auch für VPNs gibt es viele Softwarelösungen. Eine Auswahl der gängigsten Systeme wollen wir Ihnen an dieser Stelle kurz vorstellen:

PPTP

Das Point-to-Point Tunneling Protocol findet vor allem im Windows-Umfeld Anwendung. Entsprechende Serverprogramme sind sogar in vielen Heimroutern integriert. Ein proprietärer Client ist unter Windows und OS X vorinstalliert und eng mit den Betriebssystemen verzahnt. Zudem existieren freie Clients und auch Server für Linux. Trotz der einfachen Bedienbarkeit der meisten VPN-Clients für dieses Protokoll ist es wenig empfehlenswert, da die verwendeten Verschlüsselungsmechanismen veraltet und unsicher sind.

IPSec

Internet Protocol Security (IPSec) ist eine Netzwerk-Protokollfamilie, die es ebenfalls ermöglicht, verschlüsselte Punkt-zu-Punkt-Verbindungen aufzubauen. Es existieren sowohl quelloffene als auch proprietäre Client- und Server-Systeme. IPSec gilt als sehr sicher, aber auch als sehr komplex und daher als fehleranfällig.

OpenVPN

OpenVPN ist ein Programm zum Aufbau eines VPNs über das weit verbreitete hybride Verschlüsselungsprotokoll Transport Layer Security, kurz TLS. Es ist quelloffen und für alle gängigen Betriebssysteme verfügbar. OpenVPN besitzt von sich aus keine Bedienoberfläche und ist nur über die Kommandozeile (Konsole) verwendbar. Allerdings existieren für nahezu jede Plattform Zusatzprogramme, die OpenVPN mit einer der jeweiligen Plattform entsprechenden grafischen Benutzeroberfläche versehen.

tinc

Tinc ist ein freies VPN-Protokoll, das im Gegensatz zu den meisten anderen Systemen nicht auf eine klassische Client-Server-Architektur setzt, sondern ein sogenanntes Mesh-Netzwerk aufbaut. Dabei verbinden sich die einzelnen Teilnehmer selbstständig untereinander und kommunizieren nicht über einen zentralen Server. Damit wird vermieden, dass bei einem Ausfall des Servers das gesamte Netzwerk zusammenbricht. Fällt ein tinc-Client aus, bleibt im Idealfall das VPN vollständig intakt. Die verwendete Verschlüsselungstechnologie gilt bisher ebenfalls als sicher. Tinc ist für alle gängigen Desktop-Betriebssysteme verfügbar. Leider gibt es bisher keine brauchbare grafische Benutzeroberfläche, daher ist es eher für ambitionierte Nutzer zu empfehlen.

VPNs können aber nicht nur eingesetzt werden, um Datenströme verschlüsselt von A nach B zu übertragen, sondern auch, um Ihre Identität zu verschleiern. Ein VPN-Server kann nämlich so konfiguriert sein, dass es aussieht, als würde er selbst eine Anfrage an einen Teilnehmer stellen und nicht Sie. Durch dieses Feature können Sie beispielsweise so tun, als würden Sie eine Webseite aus Schweden oder Spanien aufrufen, obwohl Sie sich gerade in Berlin aufhalten.

Das ist vor allem dann hilfreich, wenn Sie sogenannte *Geo-Locks* bestimmter Webdienste umgehen wollen. Geo-Locks beschränken den Zugang zu bestimmten Internetinhalten auf Basis Ihres derzeitigen Aufenthaltsortes. Wenn Sie also beispielsweise mittels eines VPN-Tunnels so tun, als wären Sie woanders, können Sie plötzlich YouTube-Videos ansehen, die eigentlich in Ihrem Land »nicht verfügbar« sind. Das Anonymisierungsnetzwerk Tor ist übrigens auch ein virtuelles privates Netzwerk (siehe Kapitel 3) und nutzt dieses Prinzip, um Ihre eigentliche IP-Adresse und damit Ihre Identität zu verbergen.

6.7 Was dem Merkelfon fehlte – verschlüsselte Telefonie

Von Bundeskanzlerin Angela Merkel kursieren seit Jahren schon viele Fotos, die sie, SMS tippend, über ihr Handy gebeugt zeigen. Von Boulevardzeitungen wurde das begeistert aufgegriffen – sie titelten auch schon mal, dass die »SMS-Kanzlerin« das Land per Handy regiere.

Im Oktober 2013 berichtete dann die New York Times, dass Merkels Handy in den Fokus des amerikanischen Geheimdienstes geraten war: Unter den Dokumenten der NSA, die durch

Edward Snowden an die Öffentlichkeit gelangt waren, befand sich auch ein Datenbankeintrag, der darauf hinwies, dass Merkels Handy überwacht werden sollte. Diese Überwachung sollte von der US-amerikanischen Botschaft in Berlin aus durchgeführt werden. Der Datenbankeintrag stammte bereits von 2002 – allerdings wurde Merkel bereits als »chancellor«, also Kanzlerin, bezeichnet, sodass er vermutlich 2005, als sie Kanzlerin wurde, noch einmal aktualisiert worden war. Mitarbeiter der NSA, die anonym bleiben wollten, gaben bei der New York Times zu Protokoll, dass die NSA nicht nur eine Aufzeichnung der Metadaten von Merkels Telefonaten gestattete, sondern auch ein Abhören der Gesprächsinhalte. Ob jemals Protokolle von Merkels Gesprächen angefertigt wurden, und wenn ja, um welche Gespräche es sich gehandelt hat, ist bis heute unklar. Präsident Obama stritt jedenfalls ab, von einer Überwachung von Merkels Handy gewusst zu haben, und versprach anschließend, die Überwachung von Politikern befreundeter Staaten durch die NSA abzustellen.

Unabhängig davon, ob man glaubt, dass Obama die Überwachung von Politikern anderer Länder durch die NSA unterbinden kann oder will, stellt sich die Frage, was man technisch gegen solche Abhöraktionen unternehmen kann.

Schon ein halbes Jahr vor Bekanntwerden der Abhöraffäre wurden zwei neue, sichere Smartphone-Entwürfe vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert: eines von Samsung mit einem sicheren Betriebssystem von T-Systems und eines von Blackberry mit einem sicheren Betriebssystem der deutschen Firma Secusmart. Den Zuschlag für das Smartphone der Kanzlerin und ihrer Minister erhielten schließlich Blackberry und Secusmart. T-Systems und Samsung waren jedoch nicht aus dem Rennen, sondern beliefern andere deutsche Behörden mit verschlüsselungsfähigen Smartphones. Ende 2014 waren 2500 Secusmart-Geräte und 600 T-Systems-Geräte in Ministerien und Behörden im Einsatz (G. Mascolo und B. Strunz, »Bundesregierung schließt Anti-Spionage-Vertrag mit Blackberry«, Süddeutsche Zeitung, 27.11.2014). Secusmart wurde in der Zwischenzeit von Blackberry gekauft – ein Geschäft, dem die Bundesregierung unter anderem unter der Bedingung zugestimmt hat, dass sie (beziehungsweise in ihrem Auftrag das BSI) Zugriff auf die verwendeten Quellcodes von Secusmart hat. In der Vergangenheit hat Blackberry jedoch schon Behörden aus Saudi-Arabien, Indien, Russland und China Zugang zu den auf den eigenen Servern gespeicherten Nachrichten gewährt. Im Fall der Smartphones für die deutsche

Regierung wurde zusätzlich vereinbart, dass die Daten nicht zentral auf Blackberrys Servern gespeichert werden – möglicherweise wird sich das Unternehmen daran halten.

Die neuen sicheren Smartphones sollen sowohl Sprache als auch Datenverkehr verschlüsselt übertragen und private und dienstliche Daten getrennt handhaben können. Bis zur Lieferung des Secusmart-Handys hatte Frau Merkel noch das Anfang 2010 gelieferte Simko2-Handy im Einsatz, dessen Hardware von HTC stammt. Das Betriebssystem des Simko2-Handys verschlüsselt jedoch nur Datenverkehr sicher – zum sicheren Telefonieren ist ein Zusatzgerät notwendig. Davor war das Merkelfon ein Nokia E63, in das eine Verschlüsselungskarte von Secusmart eingesteckt werden konnte.

Wie Sie schon in den ersten zwei Kapiteln dieses Buchs gesehen haben, werden auch Sicherheitsmaßnahmen, die an sich zuverlässig sind, im Alltag oft beiläufig umgangen, weil sie einem zu mühsam und umständlich sind. »Mal eben« ein vermeintlich unwichtiges Telefonat unverschlüsselt zu führen, das kann sicher auch der Kanzlerin passieren. (Vielleicht hatte sie das Verschlüsselungsgerät gerade in der anderen Handtasche?) Rückblickend lässt sich also nicht genau sagen, ob und wie viel von Frau Merkels Kommunikation durch die NSA abgehört werden konnte. Hier zeigt sich jedenfalls erneut, wie wichtig es ist, dass Sicherheitsmaßnahmen nicht nur sicher, sondern auch benutzerfreundlich sind.

Wie genau funktioniert nun die Verschlüsselung des neuen Merkelfons? Die Informationen, die Secusmart hierzu veröffentlicht, sind eher spärlich. Die Firma teilt mit, dass das symmetrische Verschlüsselungsverfahren AES mit einer Schlüssellänge von 128 bit eingesetzt wird. Dieses Verfahren ist in der Tat (mit den heute zur Verfügung stehenden Computern) ein sicheres. Wie Sie schon wissen, muss für eine symmetrische Verschlüsselung aber zuvor ein geheimer Schlüssel übermittelt werden, in der Regel mithilfe von asymmetrischer Verschlüsselung. Welches asymmetrische Verschlüsselungsverfahren eingesetzt wird, dazu äußert Secusmart sich nicht.

Sie erinnern sich vielleicht noch an unseren Abschnitt über Sicherheit und Open Source: Ein Verschlüsselungsverfahren beweist seine Sicherheit am besten damit, dass sein Quellcode offen gelegt wird, sodass möglichst viele Menschen sich daran versuchen können, es zu knacken. Das Gegenteil wird in Fachkreisen als »Security through Obscurity« (Sicherheit durch Unklarheit) bezeichnet und von vielen Experten als unsicher und nicht kundenfreundlich abgelehnt.

Welche Alternativen zum verschlüsselten Telefonieren gibt es also, wenn Sie nicht annähernd 2000 Euro auf den Tisch legen wollen, um das derzeitige Merkelfon mit seinem obskuren Kryptosystem zu erwerben?

Edward Snowden empfahl 2014 die App Redphone von Open Whisper Systems. Redphone ist Open Source und basiert auf dem ebenfalls frei zugänglichen Protokoll ZRTP (Zimmermann Real-Time Transport Protocol, nach dem PGP-Erfinder Zimmermann). Bei diesem Protokoll wird die Diffie-Hellman-Methode (siehe Kapitel 2) verwendet – ein Verfahren, mit dem eine Alice und ein Bob ohne vorherige Absprache über eine Entfernung ein gemeinsames »Geheimnis« (also einen geheimen Schlüssel) vereinbaren können. Anschließend findet eine symmetrische Verschlüsselung mit dem Protokoll SRTP (Secure Real-Time Transport Protocol) statt. Am Ende jedes Telefonats werden die Schlüssel zerstört, sodass Telefonate auch im Nachhinein nicht von einem Angreifer zu entschlüsseln sind (Perfect Forward Secrecy).

Redphone behandelt Telefonate als paketbasierte Datenströme (Voice over IP, VoIP). Bei VoIP wird Sprache als analoges Signal in ein digitales Signal umgewandelt und in ein Audioformat codiert. Diese digitalen Daten werden nun in einzelnen Paketen über das Internet (oder beispielsweise ein Firmenintranet) versandt. Die Komprimierung der Daten in ein Audioformat und der eventuelle Verlust einzelner Datenpakete führen dazu, dass die Sprachqualität sinken kann. Bei einer stabilen Internetverbindung mit ausreichender Bandbreite bleibt sie jedoch annehmbar. Beim Empfänger wird das digitale Signal wieder in ein analoges umgewandelt und über einen Lautsprecher ausgegeben.

Die Sprachübertragung ist, abhängig vom verwendeten Audiokompressionsverfahren, eine datenintensive Angelegenheit. Eine VoIP-App (zum Beispiel Redphone) ist also nur mit ausreichend Datenvolumen von Ihrem Anbieter nutzbar. Für einen Anruf fallen dafür aber auch keine weiteren Gebühren an. Eine weitere Voraussetzung ist eine ausreichende Bandbreite der Internetverbindung, um Verzögerungen oder ein Abbrechen der Verbindung zu vermeiden.

Mitarbeiter von Open Whisper Systems geben im Supportforum an, dass eine langsame 3G-Verbindung schon für eine gute Sprachqualität ausreicht (Verbrauch von etwa 1 MB pro Anrufstunde). Andere Benutzer berichten Datenraten von bis zu 17.5 MB pro Stunde. Die benötigte Datenrate hängt unter anderem von der Kompression der Daten ab, so dass hier möglicherweise noch Verbesserungsspielraum für die Entwickler von Redphone besteht.

Mittlerweile gibt es von der gleichen Firma auch eine Version für iOS namens *Signal*, die ebenfalls frei und kostenlos ist. Bei der Benutzung sollten Sie beachten, dass nur Anrufe zwischen Redphone und Redphone oder zwischen Redphone und Signal verschlüsselt sind – im Zweifelsfall müssen Sie also Leute, mit denen Sie verschlüsselt telefonieren wollen, erst davon überzeugen, sich Redphone oder Signal zu installieren.

Open Whisper Systems hat übrigens nicht nur den Quellcode der App offengelegt, sondern für Benutzer, die Fehler im Quellcode finden oder Verbesserungsvorschläge einreichen, eine Belohnung in Bitcoins ausgelobt – das Gegenteil von »Security through Obscurity«!

6.8 Das eigene Betriebssystem immer dabei – Linux on a Stick

Anfang 2013 stand Edward Snowden, der NSA-Whistleblower, vor einem Dilemma:

Er wollte geheime Dokumente über das Ausmaß der Überwachung durch die NSA öffentlich machen, aber der Journalist seiner Wahl, Glenn Greenwald, benutzte kein GPG für seinen E-Mail-Verkehr (siehe E-Mail-Kapitel). Snowden hatte ihm eine anonyme, unverschlüsselte Mail geschickt und vorgeschlagen, dass er sich mit der Public-Key-Verschlüsselung beschäftigen sollte – auf Greenwalds Prioritätenliste schien dieser Punkt aber weit unten zu stehen.

Daher suchte Snowden zunächst Kontakt zur Filmemacherin Laura Poitras. Poitras erkannte die Notwendigkeit, Greenwald nicht nur mit GPG, sondern mit einem komplett sicheren Betriebssystem auszustatten. Auch auf Computern von Personen, die ihre E-Mails verschlüsseln, gibt es noch zahlreiche Datenlecks, die Namen, Aufenthaltsort und andere wichtige Daten preisgeben können – beispielsweise durch die Rückverfolgung von IP-Adressen beim Aufrufen von Webseiten (siehe Kapitel 3).

Auf einem herkömmlichen System machen Sie, wenn Sie sicher kommunizieren wollen, stets einen Kompromiss zwischen Sicherheit und Benutzbarkeit. Zum Beispiel können Sie Ihrem E-Mail-Client befehlen, jede Mail an einen Empfänger, dessen öffentlichen Schlüssel Sie haben, verschlüsselt zu senden. Wenn Sie eine unverschlüsselte Mail verschicken wollen, müssen Sie das entsprechende Kästchen von Hand deaktivieren. Da das Versenden einer verschlüsselten E-Mail länger dauert und möglicherweise auch für den Empfänger unbequemer ist (da er die Mail beispielsweise nicht auf seinem Smartphone lesen kann), machen Sie die Einstellung vielleicht

bald wieder rückgängig, sodass Sie nun von Hand die Option zum verschlüsselten Versand aktivieren müssen.

Und was ist mit der digitalen Signatur? Möchten Sie jedes Mal signieren, wenn Sie eine Mail verschicken (erhöht das Vertrauen des Empfängers), oder möchten Sie normalerweise darauf verzichten (sodass Sie im Zweifelsfall abstreiten können, eine E-Mail jemals geschrieben zu haben)? Je mehr Optionen Sie haben, desto höher wird die Fehlerwahrscheinlichkeit und damit die Wahrscheinlichkeit, dass Ihre vertrauliche Kommunikation oder Ihre geheime Identität nicht vertraulich oder geheim bleiben.

Bei Glenn Greenwald, einem vielbeschäftigten Journalisten (der sich selbst als nicht besonders technikbegabt beschreibt), war die Wahrscheinlichkeit, dass er aus Unaufmerksamkeit oder Unwissenheit irgendwo ein falsches Häkchen setzen würde, sicher nicht niedriger als bei jedem anderen. Laura Poitras erkannte daher, dass die Kommunikation zwischen ihm und Snowden am besten über ein kompaktes System mit geringem Potenzial für menschliche Fehler laufen sollte, um Snowdens Sicherheit (und die von Greenwald und ihr selbst) möglichst wenig zu gefährden. Hierbei spielte das Betriebssystem *Tails* eine große Rolle.

Tails ist eine Linux-Distribution (Open Source und frei im Netz verfügbar), die ganz auf das Ziel anonymer und spurenloser Kommunikation ausgelegt ist. Der Name Tails ist ein Akronym und steht für »The Amnesic Incognito Live System«.

Genau das, nämlich vergesslich (englisch »amnesic«) und inkognito, ist Tails auch:

- Es »vergisst« von einer Sitzung zur nächsten alle zwischenzeitlich gespeicherten Informationen.
- Es gestattet, »inkognito« zu surfen, zu chatten und zu e-mailen.

Wir werden im Folgenden die Installation und die ersten Schritte mit Tails erklären, allerdings nicht so detailreich wie die Programme in den drei vorangehenden Kapiteln, weil das den Rahmen dieses Buchs sprengen würde. Wir vertrauen darauf, dass Sie nach der Lektüre dieses Buches fit genug sind, um mithilfe dieser etwas gestrafften Erklärung sowie der guten deutschsprachigen Dokumentation von Tails https://tails.boum.org/doc/first_steps/index.de.html zurechtzukommen. Falls es an einer Stelle dann doch einmal haken sollte, hilft man Ihnen auf der nächsten Cryptoparty bestimmt gern weiter!

Tails wird in der Regel nicht auf der Festplatte Ihres Computers installiert – es ist für Menschen entwickelt worden, die auch auf fremden oder potenziell überwachten Computern sicher surfen wollen. Sie können es stattdessen auf einem USB-Stick oder einer DVD installieren und damit über einen Computer völlig ohne Verwendung der Festplatte kommunizieren und surfen. Bei einer Installation auf USB-Stick besteht zusätzlich die Möglichkeit, dass Sie sich ein verschlüsseltes Verzeichnis anlegen, auf dem Sie wichtige Daten speichern können. Diese Option besteht bei einer DVD natürlich nicht.

Da Sie mit Tails auch dann sicher unterwegs sein sollen, wenn Sie in Ihrem Umfeld niemandem vertrauen, beginnt die sichere Installation schon mit dem Download von der Tails-Webseite. Hier wird Ihnen nicht nur ein ISO-Image zum Download zur Verfügung gestellt, das Tails enthält, sondern auch eine Signatur des Hashwertes dieses Images. Wenn Sie diese mit dem öffentlichen Schlüssel der Tails-Urheber abgleichen, können Sie bestätigen, dass Sie tatsächlich eine unveränderte Tails-Version heruntergeladen haben und nicht eine, die beispielsweise von einem Angreifer manipuliert wurde.

Was ist ein ISO-Image?

Ein ISO-Image ist eine Computerdatei, die ein genaues Speicherabbild von einem Datenträger, also zum Beispiel einer DVD oder eines USB-Sticks, enthält. Es bleibt dabei nicht nur die Struktur des Dateisystems unverändert, sondern auch Zugriffsberechtigungen und insbesondere der Startsektor. Dies erlaubt die Herstellung eines USB-Sticks oder einer DVD, von der aus man den Computer booten kann.

ISO-Images haben ihren Namen vom Dateisystem-Standard ISO 9660 für CDs und DVDs. Sie können nur mit Spezialprogrammen gelesen werden.

Das Signieren des ISO-Images wird von den Urhebern von Tails mit GPG durchgeführt, das Sie in den vergangenen Kapiteln bereits kennengelernt haben. Um die Echtheit zu prüfen, müssen Sie daher den öffentlichen Schlüssel des Tails-Teams herunterladen und in GPG importieren. Unter Windows verwenden Sie dazu Gpg4win, unter Linux das Tool seahorse-nautilus. Als Nächstes laden Sie die Signatur herunter und laden Sie mit dem jeweiligen Tool, um die Signatur zu verifizieren. Sie sollten vom Programm eine Meldung erhalten, ob der Signatur vertraut werden kann.

Wenn Sie das Image heruntergeladen und die Signatur geprüft haben, transferieren Sie es als Nächstes auf eine DVD oder einen USB-Stick. Eine DVD erstellen Sie einfach mit einem

Brennprogramm (beispielsweise Nero), so wie Sie auch andere Dateien oder Musikstücke auf DVD brennen würden. Die DVD wird dabei »aus der ISO-Datei« gebrannt – das heißt, eins zu eins nach dem Abbild der ISO-Datei erstellt.

Wenn Sie keine DVD, sondern einen USB-Stick erstellen wollen, können Sie dies nicht einfach mithilfe der Kopierfunktion Ihres Betriebssystems erledigen, da diese die Datei wieder in ein eigenes Dateisystem einbettet und so zum Beispiel der Startsektor beim Booten nicht mehr gelesen werden kann. Unter Windows müssen Sie hierzu zunächst ein Programm namens Universal USB Installer herunterladen (http://www.pendrivelinux.com/universal-usb-installer-easy-as-1-2-3/) und installieren. Unter Linux verwenden Sie das Tool isohybrid und den Befehl dd. Auf der Homepage der Tails-Entwickler finden Sie hierzu eine ausführliche deutsche Anleitung: https://tails.boum.org/doc/first_steps/index.de.html.

Vor einer Gefahr müssen wir Sie warnen, wenn Sie Linux verwenden (auch in der Tails-Installationsanleitung werden Sie noch einmal darauf aufmerksam gemacht): Wenn Sie mit dem Befehl dd das ISO-Image versehentlich auf Ihre Festplatte statt auf den USB-Stick transferieren, verlieren Sie Ihre kompletten Daten auf der Festplatte! Daher stellen Sie sicher, dass Sie den richtigen Pfad für Ihren USB-Stick angeben (also beispielsweise /dev/sdb oder /dev/sdc). Wenn Sie sich nicht sicher sind, schauen Sie sich vor Einstecken des USB-Sticks den Inhalt des Verzeichnisses /dev an und vergleichen ihn mit dem Inhalt nach Einstecken des USB-Sticks. Das Unterverzeichnis, das hinzugekommen ist, muss Ihrem Stick entsprechen. Wenn Sie zwei oder mehr zusätzliche Pfade vorfinden, zum Beispiel /dev/sdb und /dev/sdb1, entspricht das Verzeichnis ohne Zahl am Ende dem Stick (das andere ist die Partition auf dem Stick).

Wenn Sie die ISO-Datei dann erfolgreich auf Stick oder DVD abgelegt haben, legen Sie erst einmal eine Pause ein und gratulieren sich selbst. Bis hierhin zu kommen, war schon eine stramme Leistung!

Jetzt haben Sie eine DVD oder einen USB-Stick, von dem aus Sie booten können. Sie legen oder stecken den Datenträger ein und starten den Computer. Wenn Tails nicht startet, sondern Ihr übliches Betriebssystem, müssen Sie im BIOS des Computers noch die Bootreihenfolge verändern (bei modernen Computern dürfte dies aber nicht notwendig sein). Hierzu müssen Sie beim Start eine Taste auf dem Keyboard gedrückt halten. In der Regel ist das Entf oder F1, kann aber trotzdem je nach Hersteller und Modell abweichen. Falls das der Fall ist, suchen Sie im Internet nach der entsprechenden Anleitung. Wenn alles klappt, erscheint statt

Ihrem Betriebssystem ein Konfigurationsmenü. Hier suchen Sie dann nach einem Eintrag wie »Boot Priority« oder Ähnlichem und setzen USB beziehungsweise DVD an die erste Stelle.

Wenn Sie auch diese Hürde genommen haben, startet Tails. Als Erstes werden Sie gefragt, ob Sie vor dem Start noch weitere Optionen definieren möchten. Wählen Sie ruhig No – mit den Feinheiten können Sie sich später beschäftigen.

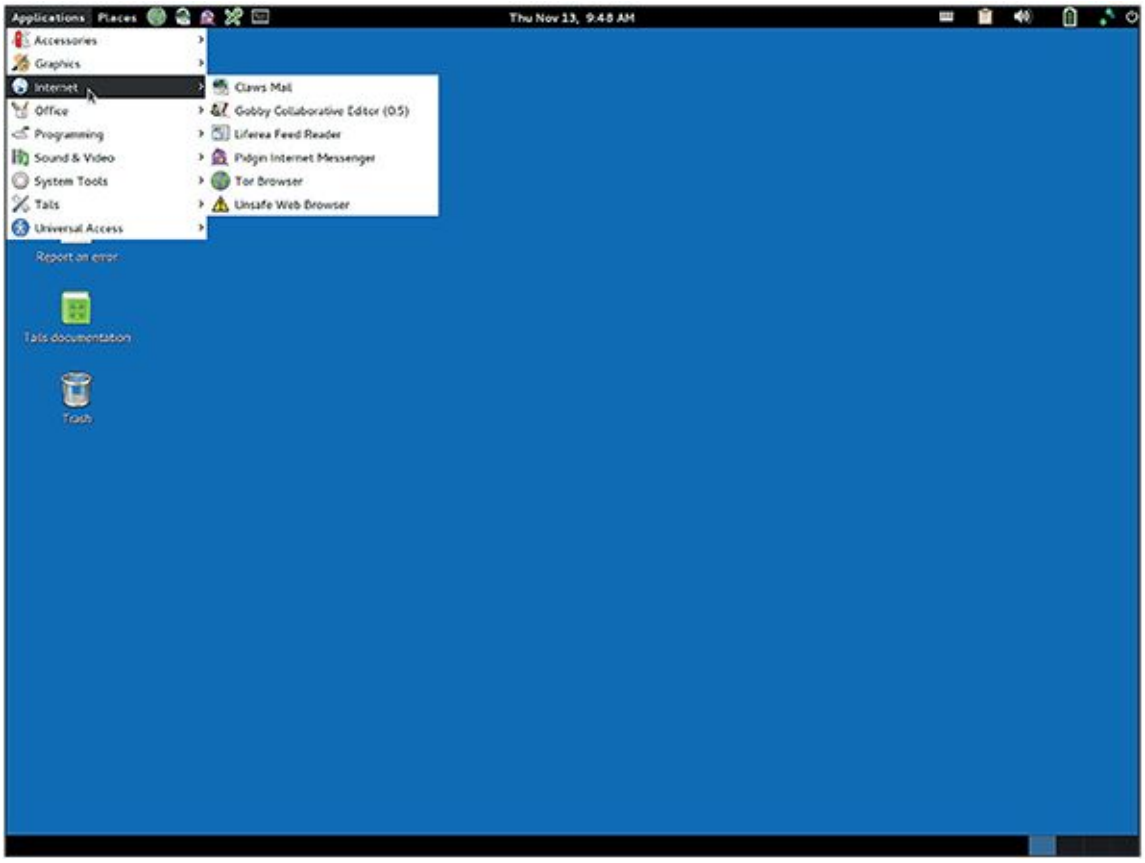


Abb. 6.3 Screenshot des sicheren Betriebssystems Tails

Tails, das Sie jetzt vor sich sehen (Abbildung 6.3), ist ein Linux-basiertes Betriebssystem. Wenn Sie ein Windows-System gewohnt sind, ist die Anordnung der Icons und Menüs auf dem Bildschirm vielleicht etwas überraschend. Da es sich auch um eine grafische Benutzeroberfläche handelt, müssen Sie aber nicht mit rätselhaften Kommandozeilen-Befehlen umgehen, sondern können zunächst einmal ein bisschen herumklicken.

Im Menü werden Sie sehen, dass einige Programme schon vorinstalliert sind. Dies sind insbesondere der Tor-Browser zum sicheren Surfen, der Mailclient Claws zum sicheren Versand von E-Mails, der Chatclient Pidgin zum sicheren Chatten sowie der Passwortverwalter KeePassX, den wir im Abschnitt über Passwort-Manager schon angesprochen haben.

Als Alternative zum Tor-Browser haben Sie zusätzlich einen unsicheren Webbrowser installiert, der kein anonymes Surfen ermöglicht, aber manchmal notwendig ist, falls Sie beispielsweise das WLAN eines Hotels verwenden und zuerst eine Log-in-Seite aufrufen müssen, bevor Ihnen der WLAN-Zugang freigeschaltet wird.

Neben diesen Programmen für die sichere Kommunikation sind auch Programme für normale Bürotätigkeiten vorinstalliert. Als Office-Suite haben Sie LibreOffice, als Bildbearbeitungsprogramm GIMP und so weiter.

In dieser Installation von Tails ist es nicht möglich, irgendetwas zu speichern. Auf der DVD sowieso nicht, da DVDs nach dem Erstellen schreibgeschützt sind – auf dem USB-Stick aber auch nicht. Diese Art von Tails wird daher »nicht-persistent« genannt – die Daten persistieren nicht, wenn Sie den Rechner ausschalten.

Wenn Sie doch Dateien dauerhaft ablegen wollten, können Sie einen weiteren Datenträger einführen, beispielsweise einen zweiten USB-Stick, auf dem Sie dann die Daten ablegen. Sie können sich aber auch eine persistente Tails-Installation anlegen. Dies geht logischerweise nur auf einem USB-Stick, nicht auf einer DVD. Der USB-Stick mit persistentem Tails enthält dann ein verschlüsseltes Verzeichnis, in dem Sie Ihre Daten sicher ablegen können. Auch Einstellungen für die in Tails enthaltenen Programme oder neu installierte Programme können in so einem persistenten Tails gespeichert werden. Sie müssen aber wissen, dass die Anonymität, die Tails per Voreinstellung bietet, durch unsichere Programme oder unsichere Einstellungen möglicherweise wieder untergraben wird.

6.9 Kritische Masse: Verschlüsselung setzt sich durch

Jeder, der neue Kommunikationsmedien und soziale Netzwerke nutzt, befindet sich irgendwo auf dem Spektrum zwischen folgenden beiden Extremen: auf der einen Seite dem Vorreiter, der jede App und jedes Netzwerk sofort selbst ausprobieren muss, und auf der anderen Seite der Abwarter, der sich erst monatelang von Freunden breitschlagen lassen muss, bis er sich irgendwo einen neuen Zugang einrichtet. Welchem von beiden stehen Sie näher?

Wenn Sie eher ein Vorreiter sind, kennen Sie sicher dieses Problem: Sie haben sich bei einem vielversprechenden neuen Netzwerk angemeldet (nennen wir es in diesem Beispiel mal frei

erfunden »Google#«) und suchen jetzt nach Freunden und Bekannten, die Sie zu Ihrer Freundesliste hinzufügen können. Die Einzige, die Sie finden, ist Ihre Arbeitskollegin Alex, die genau so eine Vorreiterin ist wie Sie, von der Sie schon die Handynummer und drei verschiedene E-Mail-Adressen haben und die bereits auf Ihren Freundeslisten bei WhatsApp, Threema, Facebook und Xing steht. Sie klicken noch ein bisschen bei Google# herum, teilen mit Alex ein lustiges Katzenvideo und ein Rezept für Kürbis-Chutney und loggen sich dann wieder aus. Nach drei Wochen loggen Sie sich noch einmal ein, weil Sie per E-Mail benachrichtigt wurden, dass ein Schulfreund von Ihnen jetzt auch auf Google# ist. Sie schicken ihm eine Nachricht, bekommen aber keine Antwort – auch er lässt seinen Account brachliegen, weil er kaum Bekannte gefunden hat.

Auf eine gewisse Art können Sie auch die Gemeinschaft der Benutzer von GPG (oder anderen Verschlüsselungsverfahren) als soziales Netzwerk betrachten. Eine Kommunikation mittels Verschlüsselung ist nur mit anderen Leuten möglich, die das gleiche Verfahren verwenden. Wenn jemand sich für ein bestimmtes Verschlüsselungsverfahren interessiert und vielleicht sogar ein Plug-in dafür installiert, dann aber feststellt, dass er mit niemandem kommunizieren kann, verfliegt der anfängliche Enthusiasmus schnell. Nur wenige Menschen haben die Energie und Hartnäckigkeit, ihre Freunde und Familie zu missionieren.

Wenn dagegen eine gewisse kritische Anzahl an Benutzern erreicht wird, kann dieser Zuwachs eine Eigendynamik erreichen wie eine Schneelawine. Irgendwann ist dann der Punkt erreicht, an dem Leute mitmachen wollen, um den Anschluss nicht zu verpassen – weil sie den Nutzen von Verschlüsselung verstehen, weil sie sich selbst ein Bild von den Technologien machen wollen, von denen neuerdings alle reden, und weil sie vielleicht auch vor ihren langsameren Freunden mit den neugewonnenen Kenntnissen ein wenig angeben wollen.

Welchen Nutzen Verschlüsselung für Sie persönlich haben kann, haben wir Ihnen in diesem Buch hoffentlich ein bisschen nähergebracht. Wir freuen uns, wenn wir Ihnen damit helfen konnten, sich vor Gefahren zu schützen, potenzielle Risiken leichter zu erkennen und das Schicksal Ihrer Daten in die eigenen Hände zu nehmen. Vielleicht ist es für Sie auch eine zusätzliche Motivation, dass Sie mit dem Verschlüsseln Ihrer Kommunikation auch anderen helfen, nämlich den Edward Snowdens der Welt und den namenlosen Menschenrechtsaktivisten in China, im Nahen Osten und anderswo, die sich oft allein durch den Einsatz von Verschlüsselung schon für Regierungen und Geheimdienste verdächtig machen. Je

mehr harmloses Zeug verschlüsselt zwischen Ihnen und Ihren Freunden hin und her geschickt wird, desto mehr Mühe haben die Geheimdienste, die Spreu vom Weizen zu trennen, und desto leichter wird es auf der ganzen Welt, vertraulich zu kommunizieren.

[1] Wenn Sie bis hierhin aufmerksam gelesen haben, wissen Sie natürlich, dass wir unsere Privatsphäre damit überhaupt nicht schützen – aber was tut man nicht alles für seine Leser.

[2] http://www.heise.de/security/meldung/Passwoerter-von-Adobe-Kunden-geknackt-2039972.html

[3] http://www.heise.de/security/meldung/Insider-Angriff-Bankdaten-von-zwei-Millionen-Vodafone-Kunden-entwendet-1955090.html

[4] http://www.heise.de/security/meldung/Angriff-auf-Playstation-Network-Persoenliche-Daten-von-Millionen-Kunden-gestohlen-1233136.html

Glossar

Account Benutzerkonto bei einem Anbieter von Onlinediensten (beispielsweise E-Mail-Provider, soziales Netzwerk, Shoppingportal)

Add-on Kleines Programm, das den Funktionsumfang eines Browsers (oder eines anderen Programms) erweitert; ist für sich allein nicht funktionsfähig

America Online (AOL) Einer der ersten Anbieter von Internetzugängen für Otto (und Ottilie) Normalnutzer mit sehr weiter Verbreitung in den 90er-Jahren und eigenem Instant Messaging (AOL Instant Messenger, AIM)

App Kleines, eigenständiges Programm, das auf einem Smartphone oder auch als Zubehör zu einem sozialen Netzwerk (Facebook-App) oder größeren Programm installiert wird; inzwischen auch für Desktop-Computer erhältlich, sodass der Übergang von Apps zu Programmen fließend geworden ist

ARPANET Historischer Vorläufer des Internets, entwickelt vom Massachusetts Institute of Technology (MIT) und dem US-Verteidigungsministerium

Asymmetrische Verschlüsselung Verschlüsselung mit einem öffentlichen Schlüssel (Public Key) und Entschlüsselung mit einem privaten Schlüssel (Private Key), zum Beispiel PGP

Authentizität Echtheit einer Nachricht, also die Sicherheit, dass sie tatsächlich vom angegebenen Absender stammt; eines der vier Ziele der Computersicherheit

Bookmark Auch als Lesezeichen oder Favorit bezeichnet; Markierung einer Webseite, sodass im Bookmark-Menü des Browsers ein Link zu dieser Webseite angelegt wird, um sie schnell wiederfinden zu können

Browser Programm zum Anzeigen von Webseiten; beispielsweise Mozilla Firefox, Chrome, Opera, Internet Explorer oder Safari

Brute-Force-Angriff Ein Verfahren zum Entschlüsseln eines Codes oder zum Herausfinden eines Passwortes, bei dem alle möglichen Zeichenkombinationen stur hintereinander ausprobiert werden; sehr zeit- und rechenintensiv

Bug Fehler in einer Software

Cache Zwischenspeicher des Browsers, in dem Inhalte abgelegt sind, die häufig abgerufen werden

Chat Austausch von Kurznachrichten über ein Computernetzwerk, meist live; beispielsweise mit Chatprogrammen wie AIM, ICQ oder Pidgin beziehungsweise per Smartphone über WhatsApp, Threema, TextSecure oder iMessage

Chiffre Auch als Code bezeichnet; Verfahren zur Verschlüsselung von Nachrichten, die den Klartext in den Geheimtext umwandelt; Beispiel: Caesar-Chiffre

Chronik Auch Browserhistorie oder Verlauf genannt; im Browser gespeicherte Adressen der letzten besuchten Webseiten

Cookie Kleine Datei, die beim Besuch einer Webseite auf dem Computer des Benutzers abgelegt wird und von dieser Webseite oder anderen Seiten, die danach besucht werden, wieder ausgelesen werden kann

Elektronische Identifikationsfunktion (eID) Funktion zur Identifizierung einer Person durch den neuen Personalausweis (nPA), die auch von privaten Unternehmen genutzt werden darf

E-Mail-Client Programm zum Abruf oder Versenden von E-Mails; als eigenständiges Programm auf dem Rechner des Nutzers oder als webbasierte Applikation

Ende-zu-Ende-Verschlüsselung Verschlüsselung der Nachricht, beispielsweise mit PGP, auf dem gesamten Weg zwischen dem Client des Absenders und dem Client des Empfängers

Geolokalisation Bestimmung des geografischen Standortes des Besuchers einer Webseite

Google Hangouts Proprietäres Instant-Messaging-System von Google, das Instant Messaging, Videotelefonie und auch Broadcasting von Videos erlaubt

Google Mail (GMail) E-Mail-Dienst von Google; webbasiert, kann aber auch mit einem E-Mail-Client verwendet werden, um beispielsweise Mailverschlüsselung umzusetzen

GPG (Gnu Privacy Guard) Eine der Open-Source-Varianten von PGP (Pretty Good Privacy) zur E-Mail- und Datenverschlüsselung

Global Positioning System (GPS) Satellitenbasiertes System, mit dem ein Empfänger geografisch geortet werden kann; GPS-Empfänger sind beispielsweise in Smartphones oder Navis (mobile Navigationssysteme) eingebaut

Hashwert Zahlenwert, der aus einer Nachricht berechnet werden kann; sollte möglichst einzigartig sein, ist es aber meistens nicht (Hashkollision)

Header Kopf einer E-Mail, der Steuerungsinformationen enthält (inklusive Betreff der E-Mail) und aus diesem Grund auch bei verschlüsselten Mails im Klartext lesbar bleibt

Hybride Verschlüsselung Übermittlung eines asymmetrisch verschlüsselten Sitzungsschlüssels, mit dessen Hilfe die Sitzung (Chat, E-Mail oder Ähnliches) dann symmetrisch verschlüsselt wird

Hyperlink Auch als Link oder Verknüpfung bezeichnet – besonders ausgezeichnetes Wort, Reihe von Wörtern oder Grafik in einem HTML-Dokument, das den Nutzer zu einem anderen Dokument weiterführt

Hypertext Markup Language (HTML) Auszeichnungssprache, mit der Informationen auf Webseiten strukturiert werden; ermöglicht beispielsweise auch das Einbetten von Grafiken oder die Erstellung von Hyperlinks

Hypertext Transfer Protocol (HTTP) Protokoll, mit dem Daten im Web vom Webserver zum Client (Besucher der Webseite) übertragen werden

ICQ Erster Instant Messenger mit wirklich weiter Verbreitung, kam 1996 auf

Inbox Posteingang, in dem eingehende E-Mails für einen Benutzer gespeichert werden

Instant Messaging Austausch von Kurznachrichten über ein Computernetzwerk, live oder mit asynchroner Zustellung (also mit einem Posteingang wie E-Mail)

Integrität Unversehrtheit einer Nachricht, also die Sicherheit, dass sie auf dem Weg vom Absender zum Empfänger nicht verändert wurde; eines der vier Ziele der Computersicherheit

Internet Message Access Protocol Version 4 (IMAP4) Protokoll zum Abrufen von E-Mail mit erweitertem Funktionsumfang im Vergleich zu POP3

Internet Relay Chat (IRC) Eines der ersten Chatprotokolle im Internet

IP-Adresse Adresse eines Computers im Internet

Jabber Siehe XMPP

Jitsi Open-Source-Programm für Videotelefonie und Instant Messaging

Kommandozeile Auch als Konsole, Terminal (unter Linux und Mac OS) oder Eingabeaufforderung (unter Windows) bekannt; Schnittstelle zum Benutzer, die meist nur Texteingabe erlaubt

Kryptografie Wissenschaft von der Verschlüsselung von Nachrichten

Like-Button Link auf einer Webseite, mit dem man als Facebook-Benutzer seinen Facebook-Freunden mitteilen kann, dass einem diese Webseite gefallen hat; wird von Facebook für Werbezwecke verwendet, auch bei Nicht-Facebook-Usern

Man-in-the-Middle-Attacke Lauschangriff, bei dem der Angreifer die Nachrichten des Absenders abfängt, liest und an den Empfänger weiterleitet, ohne dass das Mitlesen von Absender oder Empfänger bemerkt wird

Metadaten Alle Daten über ein Gespräch, die nicht der Gesprächsinhalt sind, also Identität der Kommunikationspartner, Zeitpunkt und Dauer des Gesprächs, verwendetes Protokoll, Größe der Nachrichten und so weiter; bleiben auch bei verschlüsselter Kommunikation in der Regel klar erkennbar

Off the record (OTR) Kommunikationsmodus, in dem hinterher den Gesprächsteilnehmern nicht nachgewiesen kann, dass das Gespräch stattgefunden hat oder was dessen Inhalte waren

Open Source (Oft nicht kommerzielle) Software, deren Quellcode für die Öffentlichkeit einsehbar (quelloffen) ist; Gegenteil: Closed Source, proprietär

Open System for Communication in Realtime (OSCAR) Chatprotokoll mit 2008 offen gelegtem Quellcode, auf dem ICQ und AIM basieren

Partitionierung Unterteilung eines physikalischen Speichermediums in ein oder mehrere logische Speicherbereiche (Partitionen), die dann jeweils verschiedene Dateisysteme beherbergen können

Patch Ein kleines Programm (englisch für »Flicken«), das einen Bug (Fehler) in einer anderen Software (zum Beispiel einem Add-on oder einem Browser-Plug-in, oder auch einem Betriebssystem) ausbessert

Perfect Forward Secrecy (PFS) Sicherheit, dass eine Kommunikation nicht nachträglich entschlüsselt werden kann, auch wenn private Keys einem Angreifer in die Hände fallen

Plug-in Kleines (im Gegensatz zu einem Add-on aber selbstständiges) Programm, das den Funktionsumfang eines Browsers (oder eines anderen Programms) erweitert, beispielsweise um Videos im Browser abzuspielen

Pop-up-Fenster Neues Browserfenster (meist in kleinem Format), das sich ohne Zutun des Benutzers öffnet

Post Office Protocol Version 3 (POP3) Protokoll zum Abrufen von E-Mails mit sehr einfachem Funktionsumfang, daher als veraltet anzusehen

Post-Privacy Philosophie, nach der der Begriff und die Existenz einer Privatsphäre überholt ist, da durch den technischen Fortschritt und die damit einhergehenden Möglichkeiten der Datenerhebung und -speicherung auch persönliche Daten weitgehend transparent werden

Pretty Good Privacy (PGP) Protokoll zur asymmetrischen Verschlüsselung von E-Mails und anderen Dokumenten; beruht auf einer netzartigen Public-Key-Infrastruktur (Web of Trust)

Proprietär In den Händen einer Firma; Gegenteil: quelloffen, Open Source

Protokoll Satz von Befehlen, mit denen Computer und Programme (Clients) sich im Internet unterhalten, beispielsweise SMTP für E-Mail oder HTTP für Hypertext (Surfen im Web)

Proxy Server in einem Netzwerk, der eine Anfrage annimmt und unter eigener Adresse als Stellvertreter weiterleitet

Pseudonym Erfundener Name, den eine Person sich in der Regel selbst gibt, der ihr aber auch von anderen zugeordnet werden kann, wenn der reale (bürgerliche) Name vertraulich bleiben soll

Qualifizierte Elektronische Signatur (QES) Rechtlich bindende elektronische Unterschrift mithilfe des neuen Personalausweises (nPA)

Request Anfrage, die ein Webclient an einen Webserver stellt, um die Daten einer Webseite geliefert zu bekommen, sodass diese im Browser angezeigt werden kann

Response Antwort des Webservers auf ein Request (eine Anfrage) des Webclients; liefert die Daten einer Webseite zur Anzeige im Browser (oder eine Fehlermeldung, wenn die Seite beispielsweise nicht gefunden wird)

RFID-Chip Bauteil (auch Transponder genannt), meist ohne eigene aktive Stromversorgung, dessen Daten kontaktlos über elektromagnetische Wellen von einem Lesegerät ausgelesen werden können (RFID: Radio Frequency Identification)

Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA) Agentur in Form einer AG, die Daten zur Beurteilung der Kreditwürdigkeit von Personen und Firmen sammelt und Auskünfte über diese Kreditwürdigkeit erteilt

Short Messaging Service (SMS) Kurznachrichten, die über das Mobilfunknetz (also nicht per Internet) von Handy zu Handy verschickt werden

Signatur Digitale Unterschrift, die darauf beruht, dass der Unterschreibende den Hashwert der Nachricht mit seinem privaten Schlüssel verschlüsselt und dieser vom Empfänger (oder der Öffentlichkeit) mit dem öffentlichen Schlüssel entschlüsselt, also verifiziert, werden kann

Simple Mail Transfer Protocol (SMTP) Protokoll zum Versand von E-Mails

Sitzungsschlüssel (Session Key) Schlüssel für die symmetrische Verschlüsselung, der nur für die Dauer eines Gesprächs verwendet wird

Skype Proprietäres Programm für Videotelefonie und Instant Messaging

Smartphone Internetfähiges Handy, auf dem kleine Programme (Apps) installiert werden können

S/MIME Protokoll zur Verschlüsselung von Nachrichten, das auf einer hierarchischen Infrastruktur beruht (im Gegensatz zum Web of Trust von PGP)

Social Engineering Verfahren, um in der realen Welt (nicht digital) an Zugangsdaten und sensible Informationen zu kommen; beispielsweise durch Beobachtung von Personen, die sich in ihren Account einloggen (Shoulder Surfing) oder das Durchsuchen von Mülleimern nach sensiblen Dokumenten (Dumpster Diving)

Solid State Drive (SSD) Laufwerk, auf dem Daten elektronisch (und nicht magnetisch, wie auf herkömmlichen Festplatten) gespeichert werden; teurer als herkömmliche Festplatten, aber schneller, robuster gegenüber Stößen und geräuschlos im Betrieb

Symmetrische Verschlüsselung Verschlüsselung mit einem einzigen Schlüssel, der sowohl zur Ver- als auch zur Entschlüsselung verwendet wird und deswegen von beiden Teilnehmern einer privaten Kommunikation geheim gegenüber allen anderen gehalten werden muss

Synchronisation Abgleichen von Daten oder Einstellungen eines Benutzers über mehrere Geräte hinweg, sodass beispielsweise am Laptop eingetragene Termine in der Kalender-App auch auf dem Smartphone zur Verfügung stehen

TextSecure Quelloffener Instant Messenger für Mobiltelefone mit Ende-zu-Ende-Verschlüsselung und Authentifizierung, entwickelt von Open Whisper Systems

Timeline Chronologische Abfolge von Nachrichten, die einem individuellen Nutzer in einem sozialen Netzwerk (beispielsweise Twitter oder Facebook) angezeigt werden, inklusive der selbst geposteten Nachrichten

Threema Proprietärer Instant Messenger für Mobiltelefone mit Ende-zu-Ende-Verschlüsselung und Authentifizierung, zentralisierter Service der Schweizer Firma Kasper Systems

Transmission Control Protocol (TCP) Paketvermitteltes Protokoll im Internet

Transport Layer Security (TLS) Protokoll für die Transportverschlüsselung von E-Mail und Instant Messages

Transportverschlüsselung In Bezug auf E-Mail: Verschlüsselung der Nachricht, beispielsweise mit TLS, auf dem Weg zwischen Mailserver des Absenders und Mailserver des Empfängers (im Gegensatz zu Ende-zu-Ende-Verschlüsselung, die den gesamten Weg vom Client des Absenders zum Client des Empfängers einschließt)

Tweet Kurznachricht bei Twitter, in der Regel öffentlich einsehbar

Uniform Resource Locator (URL) Adresse einer Webseite, Datei oder sonstigen Ressource im Internet (beispielsweise de.wikipedia.org/wiki/Uniform_Resource_Locator)

Update Aktualisierung von Software auf eine neuere Version, in der beispielsweise mehr Funktionen zur Verfügung stehen oder Fehler behoben wurden

Verfügbarkeit Die Sicherheit, dass eine Nachricht abgerufen werden kann, wenn der Empfänger dies möchte; eines der vier Ziele der Computersicherheit

Vertraulichkeit Die Sicherheit, dass eine Nachricht auf dem Weg vom Absender zum Empfänger nicht von einem Dritten gelesen wurde; eines der vier Ziele der Computersicherheit

Virtual Private Network (VPN) Verschlüsselte Datenverbindung zwischen zwei Teilnehmern oder Teilnetzen in Form eines »Tunnels« durch das nicht verschlüsselte Internet

WhatsApp Proprietärer Instant Messenger für Mobiltelefone, seit Februar 2014 zu Facebook gehörend, basierend auf XMPP

World Wide Web (WWW) Der Teil des Internets, der aus Webseiten besteht, die auf Webservern liegen und von Webclients aus mit der Hilfe von Webbrowsern angezeigt werden

XMPP Quelloffenes Protokoll für das Instant Messaging, das ähnlich wie SMTP für E-Mail funktioniert; kurz für Extensible Messaging and Presence Protocol

YouTube Zurzeit größtes Videoportal im Internet (Besitzer: Google)

Zufallszahlengenerator Programm, das zufällig ausgewählte Zahlen zurückliefert (die beispielsweise für Verschlüsselungsalgorithmen benötigt werden); oft schon ins Betriebssystem eines Computers integriert

Stichwortverzeichnis

B

C

F

J

K

L

M

Q

R

S

W

X

Z

WILEY END USER LICENSE AGREEMENT

Besuchen Sie www.wiley.com/go/eula, um Wiley's E-Book-EULA einzusehen.