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) Privatsphäre definieren, 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.

1 *http://www.schneier.com*

- 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?).

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

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 Stasi gemacht 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 Sicherheits-

netz, 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.

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

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].

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

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:

Abbildung 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.