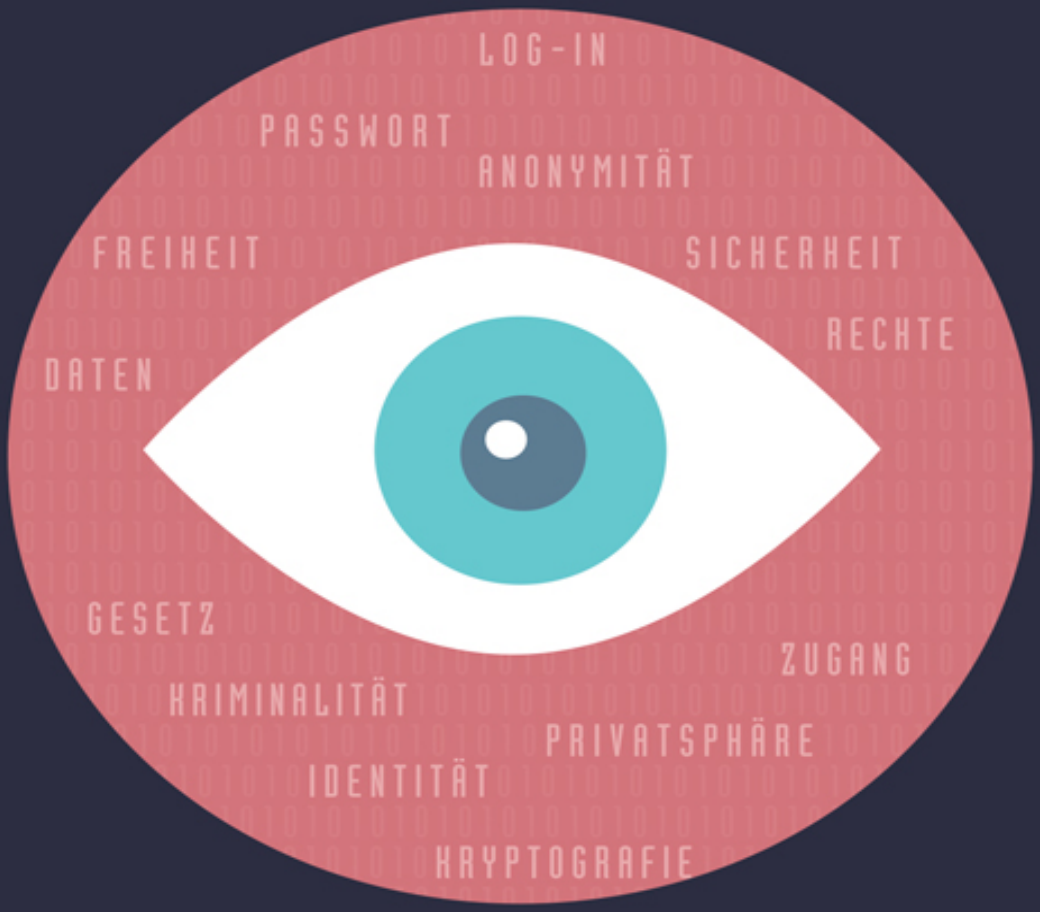
Christina Czeschik ◆ Matthias Lindhorst ◆ Roswitha Jehle

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

SYBEX
A Wiley Brand

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

Inhaltsverzeichnis

Stichwortverzeichnis

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