BRUCE SCHNEIER

CLICK HERE TO KILL EVERYBODY

Sicherheitsrisiko Internet
und die Verantwortung von
Unternehmen und Regierungen

mitp

mitp

Hinweis des Verlages zum Urheberrecht und Digitalen Rechtemanagement (DRM)

Für Arlene, mit den besten Wünschen

Click Here to Kill Everybody

Sicherheitsrisiko Internet und die Verantwortung von Unternehmen und Regierungen

Bruce Schneier

Übersetzung aus dem Amerikanischen von Knut Lorenzen

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.

ISBN 978-3-95845-948-9
1. Auflage 2019

www.mitp.de
E-Mail: mitp-verlag@sigloch.de
Telefon: +49 7953 / 7189 - 079
Telefax: +49 7953 / 7189 - 082

Authorized German translation from the English language edition, entitled CLICK HERE TO KILL EVERYBODY: Security and Survival in a Hyper-connected World, ISBN 978-0-393-60888-5

Original English language edition published by W. W. Norton & Company, Inc., New York, NY, USA.

Lektorat: Janina Bahlmann, Lisa Kresse
Sprachkorrektorat: Eva Gößwein
Coverbild: © Francois Poirier / stock.adobe.com
Satz: III-satz, www.drei-satz.de

Inhalt

Über den Autor 9
Einleitung: Alles wird zum Computer 11
Dank 27

Teil I Die Schwachstellen 31

1 Computer sind immer noch schwierig zu sichern 35
Die meiste Software ist schlecht programmiert und unsicher 36
Sicherheit spielte bei der Entwicklung des Internets keine Rolle 38
Erweiterbarkeit heißt, alles kann gegen uns verwendet werden 41
Aufgrund ihrer Komplexität sind computerisierte Systeme einfacher anzugreifen als zu schützen 44
Interkonnektivität schafft neue Sicherheitslücken 46
Computer sind auf besondere Weise gefährdet 48
Die Angriffe werden immer besser, schneller und einfacher 51

2 Patchen ist keine Lösung 55
Installation der Patches 58
Schreiben und Veröffentlichen der Patches 60
Offenlegen der Sicherheitslücken 63
Aufspüren der Sicherheitslücken 64

3 Internetnutzer zu identifizieren, wird immer schwieriger 67
Die Authentifizierung wird schwieriger, das Stehlen von Zugangsdaten einfacher 67
Die Attribution wird sowohl schwieriger als auch einfacher 76

4 Alle begünstigen Unsicherheit 81
Das Internet wird immer noch durch den Überwachungskapitalismus gesteuert 82
Im nächsten Schritt werden Unternehmen Kunden und User kontrollieren 85
Auch Staaten nutzen das Internet zur Überwachung und Kontrolle 91
Cyberkrieg wird zur Normalität 95
Kriminelle profitieren von Unsicherheit 103

5 Die Risiken nehmen katastrophale Ausmaße an 109
Die Angriffe auf die Datenintegrität und die Verfügbarkeit nehmen zu 109
Algorithmen werden autonom und immer leistungsfähiger 113
Unsere Lieferketten sind zunehmend angreifbar 119
Es wird nur noch schlimmer 122

Teil II Die Lösungen 131

6 Wie ein sicheres Internet+ aussehen könnte 137
Absicherung der Geräte 140
Absicherung der Daten 142
Absicherung der Algorithmen 144
Absicherung der Netzwerkverbindungen 146
Absicherung des Internets 147
Absicherung kritischer Infrastruktur 149
Systeme voneinander trennen 152

7 Wie wir das Internet+ absichern können 155
Standards entwickeln 157
Fehlgerichtete Anreize korrigieren 160
Haftungsfragen klären 166
Informationsasymmetrie ausgleichen 172
Öffentliche Aufklärung verbessern 178

Berufliche Standards einführen 179
Dem Fachkräftemangel begegnen 181
Forschung weiter ausbauen 182
Wartung und Instandhaltung fördern 183

8 Der Staat ermöglicht Sicherheit 185
Eine neue Regierungsbehörde 186
Staatliche Regulierung 192
Herausforderungen der Regulierung. 194
Normen, Verträge und internationale Aufsichtsbehörden. 199

9 Wie der Staat die Defensive der Offensive vorziehen kann. 205
Offenlegen und Beheben von Sicherheitslücken 207
Design zugunsten der Sicherheit, nicht der Überwachung. 213
So viel wie möglich verschlüsseln 217
Sicherheit und Spionage voneinander trennen. 219
Strafverfolgung verbessern 221
Die Beziehung zwischen Regierung und Wirtschaft überdenken 224

10 Plan B: Was wahrscheinlich passieren wird 229
Die USA werden so schnell nichts unternehmen. 230
Andere Länder werden regulieren 234
Was wir tun können 238

11 Welche Fehler die Politik begehen kann 243
Hintertüren fordern. 244
Verschlüsselung beschränken 249
Anonymität verbieten 251
Massenüberwachung. 253
Hacking Back 256
Die Verfügbarkeit von Software begrenzen. 258

12 Für ein vertrauenswürdiges, resilientes und friedliches Internet+ 261
Ein resilientes Internet 265
Ein entmilitarisiertes Internet 267

Résumé: Technologie und Politik zusammenbringen 271

Ergänzende Hinweise und weiterführende Informationen 281
Stichwortverzeichnis 377

Über den Autor

Bruce Schneier ist ein international renommierter Sicherheitstechnologe, der vom *Economist* als »Sicherheits-Guru« bezeichnet wird. Er hat bislang 14 Bücher geschrieben, unter anderem den Bestseller *Data and Goliath* (dt. Titel: *Data und Goliath – Die Schlacht um die Kontrolle unserer Welt: Wie wir uns gegen Überwachung, Zensur und Datenklau wehren müssen*), und mehrere Hundert Artikel, Essays und wissenschaftliche Arbeiten verfasst. Sein einflussreicher Newsletter *Crypto-Gram* und sein Blog *Schneier on Security* haben mehr als 250.000 Leser. Schneier ist Mitglied der wissenschaftlichen Gesellschaft des Berkman Klein Center for Internet & Society an der Harvard University, lehrt öffentliche Sicherheit und Ordnung an der Harvard Kennedy School und sitzt bei der Electronic Frontier Foundation, bei Access Now und beim Tor-Projekt im Vorstand. Bei EPIC und bei VerifiedVoting.org ist er beratend tätig. Zudem ist er Berater bei IBM Security und leitet den Bereich Technologie bei IBM Resilient.

Einleitung

Alles wird zum Computer

Betrachten Sie die folgenden drei Vorfälle und ihre Folgen.

Erster Vorfall: 2015 übernahmen zwei Sicherheitsforscher die Steuerung eines Jeep Cherokee, und zwar aus rund 16 Kilometern Entfernung über das mit dem Internet verbundene Unterhaltungssystem des Fahrzeugs. Ein Video zeigt den entsetzten Gesichtsausdruck des Fahrers, der auf einer Schnellstraße unterwegs ist und hilflos zusehen muss, wie die Hacker die Klimaanlage aufdrehen, den Radiosender wechseln, die Scheibenwischer betätigen und schließlich den Motor abschalten. Da es sich hier nicht um einen Mordversuch, sondern um eine Demonstration handelte, verzichteten die Forscher darauf, die Kontrolle über das Steuer oder die Bremsen zu übernehmen. Aber sie hätten es tun können.

Das war keineswegs eine einmalige Sache. Hacker haben in verschiedenen Automodellen Sicherheitslücken aufgezeigt. Sie haben sich über den Diagnoseanschluss, über den DVD-Player, über das OnStar-Navigationssystem oder über die in die Reifen eingebetteten Computer eingehackt.

Auch Flugzeuge können gehackt werden. Es gibt zwar kein so anschauliches Beispiel wie die Übernahme der Steuerung des Jeeps, aber Sicherheitsforscher behaupten, dass die Bordelektronik von Flugzeugen über das Unterhaltungssystem und über die Luft-Boden-Kommunikationssysteme angreifbar ist. Die Flugzeughersteller haben das jahrelang bestritten. 2017 schließlich führte das US-Ministerium für Innere Sicherheit einen Remote Hack einer Boeing 757 vor. Einzelheiten wurden nicht veröffentlicht.

Zweiter Vorfall: 2016 zündeten – vermutlich russische – Hacker in einem Umspannwerk in Pivnichna bei Kiew in der Ukraine aus der Ferne eine Cyberwaffe namens CrashOverride und schalteten es ab.

Der Angriff mit CrashOverride unterschied sich von einem Cyberangriff im Jahr davor, der das Steuerungszentrum Prykarpattyaoblenergo im Westen der Ukraine zum Ziel hatte. Dort kam es zwar ebenfalls zu einem Stromausfall, der Angriff war aber eher manueller Natur. Die Angreifer, vermutlich ebenfalls Russen, erlangten über eine Hintertür einer Schadsoftware Zugriff auf das System, übernahmen die Computer des Steuerungszentrums und schalteten den Strom ab. (Ein Mitarbeiter hat davon ein Video aufgenommen.) CrashOverride hingegen hat alles vollkommen automatisch erledigt.

Letzten Endes hatten die Menschen, die vom Umspannwerk Pivnichna mit Strom versorgt wurden, noch Glück. Die Techniker nahmen das Kraftwerk kurzfristig vom Netz und konnten die Stromversorgung nach etwa einer Stunde von Hand wiederherstellen. Ob ähnliche Kraftwerke in den USA über vergleichbare Möglichkeiten des manuellen Eingriffs und das entsprechend geschulte Personal verfügen, ist unklar. CrashOverride war eine militärische Waffe, modular aufgebaut und problemlos für andere Ziele umkonfigurierbar: Gaspipelines, Wasseraufbereitungsanlagen und so weiter. Die Cyberwaffe besaß verschiedene weitere sogenannte »Payloads«, die beim Angriff in der Ukraine überhaupt nicht zum Einsatz kamen. Sie hätte die Stromversorgung durch das Umspannwerk wiederholt ein- und ausschalten und dadurch physische Schäden an der technischen Ausrüstung verursachen können, die zu einem tagelangen oder sogar wochenlangen Stromausfall geführt hätten. Mitten im ukrainischen Winter wäre das für viele Menschen verhängnisvoll gewesen. Die Waffe wurde im Rahmen einer Regierungsaktion eingesetzt, zugleich war sie aber auch ein Test der eigenen Fähigkeiten. In den letzten Jahren sind russische Hacker in mehr als 20 US-Kraftwerke eingedrungen und haben dabei häufig Zugriff auf kritische Systeme erlangt, ohne jedoch Schäden anzurichten; hierbei handelte es sich ebenfalls um Tests der eigenen Fähigkeiten.

Dritter Vorfall: An einem Wochenende im Jahr 2017 hackte irgendjemand 150.000 Drucker rund um den Globus. Der Hacker hatte ein Programm geschrieben, das automatisch unsichere Drucker erkannte und auf diesen Geräten wiederholt ASCII-Art und spöttische Bemerkungen ausdruckte. Dergleichen kommt regelmäßig vor und kann im Grunde als Vandalismus betrachtet werden. Im selben Jahr wurden an verschiedenen US-Universitäten Drucker gehackt, die dann Flugblätter mit antisemitischen Parolen ausdruckten.

Angriffe dieser Art auf 3D-Drucker sind bislang noch nicht bekannt, aber es gibt keinen Grund, anzunehmen, dass diese Geräte nicht ebenso angreifbar sind. Ein gehackter 3D-Drucker wäre nur ärgerlich und kostspielig, aber das Ausmaß der Bedrohung nimmt drastisch zu, wenn es sich um einen Biodrucker handelt. Diese Technologie steckt zwar noch in den Kinderschuhen, besitzt aber das Potenzial, speziell an individuelle Patienten angepasste Viren zur Bekämpfung von Krebs (oder anderer Krankheiten) hervorzubringen, die automatisch synthetisiert und zusammengesetzt werden.

Stellen Sie sich eine Zukunft vor, in der solche Biodrucker in Krankenhäusern, Apotheken und Arztpraxen verbreitet sind. Ein Hacker, der Fernzugriff besitzt und über die erforderlichen Druckeranweisungen verfügt, könnte mit einem Biodrucker ein Killervirus erzeugen. Er könnte das Virus auf einem Drucker massenhaft ausdrucken oder auf vielen Druckern jeweils eine kleinere Menge ausgeben. Wenn sich das Virus ausbreitet und sich genügend Menschen anstecken, hätten wir es mit einer weltweiten Epidemie zu tun.

Dann hieße es tatsächlich: »Click here to kill everybody.«

Warum sind solche Szenarien denkbar? Die Steuerung eines Autos aus dem Jahr 1998 konnte nicht von einem kilometerweit entfernten Angreifer übernommen werden. Gleiches gilt für ein Kraftwerk aus dem Jahr 1998. Die heutigen Automodelle sind angreifbar, und auch die zukünftigen Biodrucker werden angreifbar sein, weil es sich dabei im Grunde genommen um Computer handelt. Alles wird auf diese Weise angreifbar, weil alles zu einem Computer wird. Genauer gesagt: zu einem mit dem Internet verbundenen Computer.

Ihr Backofen ist ein Computer, der Speisen erhitzt. Ihr Kühlschrank ist ein Computer, der Lebensmittel kühlt. Ihre Kamera ist ein Computer mit einer Linse und einem Blendenverschluss. Ein Geldautomat ist ein Computer, der Bargeld enthält. Und moderne Glühlampen sind Computer, die leuchten, wenn irgendjemand oder irgendein anderer Computer einen Schalter betätigt.

Früher war Ihr Auto ein mechanischer Apparat, der einige Computer beherbergte. Heutzutage handelt es sich um ein aus 20 bis 40 Computern bestehendes verteiltes System mit vier Rädern und einem Motor. Wenn Sie auf die Bremse treten, haben Sie vielleicht den Eindruck, dass Sie das Auto physisch zum Stehen bringen, tatsächlich senden Sie jedoch lediglich ein

elektronisches Signal an die Bremsen – eine mechanische Verbindung zwischen Pedal und Bremsbelag gibt es nicht mehr.

2007 wurde Ihr Telefon mit der Einführung des iPhones zu einem leistungsfähigen Computer.

Smartphones sind unsere ständigen Begleiter. Wir verwenden das Präfix »smart« für computerisierte internetfähige Geräte und meinen damit, dass sie Daten sammeln, verarbeiten und weitergeben, um zu funktionieren. Auch ein Fernseher wird als smart bezeichnet, wenn er permanent Daten über Ihre Sehgewohnheiten sammelt, um Ihre User Experience zu optimieren.

Schon bald werden smarte Geräte Teil unseres Körpers werden. Moderne Herzschrittmacher und Insulinpumpen sind smart. Medikamente in Tablettenform sind auf dem Weg, smart zu werden. Smarte Kontaktlinsen zeigen nicht nur Informationen über das an, was Sie sehen, sondern auch Ihren Blutzuckerspiegel, und sie können Grünen Star diagnostizieren. Fitnessarmbänder sind smart und zunehmend in der Lage, unsere körperlichen Zustände zu erfassen.

Es gibt aber noch mehr smarte Objekte. Für Ihren Hund können Sie ein smartes Halsband kaufen und für Ihre Katze ein smartes Spielzeug. Darüber hinaus sind smarte Stifte, smarte Zahnbürsten, smarte Kaffeetassen, smarte Sexspielzeuge, smarte Barbiepuppen, smarte Maßbänder und smarte Sensoren für Ihre Zimmerpflanzen erhältlich. Sie können sogar einen smarten Motorradhelm erwerben, der automatisch den Krankenwagen ruft und Ihre Familie per Textnachricht informiert, falls Sie einen Unfall haben.

Das »Smart Home« hält gerade Einzug. Die virtuelle Assistentin Alexa und ihre Verwandten horchen auf Ihre Anweisungen und antworten Ihnen. Es gibt smarte Thermostate, smarte Steckdosen und smarte Küchengeräte, smarte Körperwaagen und smarte Toiletten, smarte Glühlampen und dazu smarte Hubs, die sie steuern. Es gibt smarte Türschlösser, die es Ihnen ermöglichen, Handwerkern oder Lieferanten einen Code zu übermitteln, der den einmaligen Zutritt zu Ihrer Wohnung gewährt, und es gibt smarte Betten, die Ihre Schlafmuster aufzeichnen und Schlafstörungen diagnostizieren.

An manchen Arbeitsstätten sind solche smarten Geräte mit Überwachungskameras vernetzt, mit Sensoren, die den Bewegungen von Kunden folgen und vielem mehr. Smarte Systeme sorgen in größeren Gebäuden für

eine effizientere Beleuchtung und einen besseren Fahrstuhlbetrieb, steuern die Klimaanlage und verrichten viele weitere Aufgaben.

Einige Städte haben damit angefangen, smarte Sensoren in Straßen, Laternen und Gehwege einzubauen, und verwenden smarte Stromnetze und smarte Verkehrsnetze. Schon bald wird Ihre Stadt in der Lage sein, Ihre Haushaltsgeräte und andere Stromverbraucher zu steuern, um den Energieverbrauch zu optimieren. Vernetzte fahrerlose Autos begeben sich dann automatisch dorthin, wo sie benötigt werden, und minimieren dabei den dazu erforderlichen Energieverbrauch. Die Sensoren und Steuerungsanlagen in den Straßen sorgen für einen besser geregelten Verkehr, verkürzen so die Anfahrtszeiten von Polizei und Rettungsdiensten und erstatten automatisch Bericht, wenn Straßen überlastet sind. Weitere Sensoren werden die Effizienz der öffentlichen Dienstleistungen steigern, von Polizeieinsätzen bis hin zu optimierten Wegstrecken bei der Müllentsorgung und der Reparatur von Schlaglöchern. Und smarte Anzeigetafeln werden Sie beim Vorbeigehen erkennen und auf Sie zugeschnittene Werbung zeigen.

Ein Umspannwerk ist im Grunde genommen nur ein Computer, der Elektrizität verteilt und – wie alles andere auch – mit dem Internet verbunden ist. CrashOverride hat das Umspannwerk Pivnichna nicht direkt infiziert. Es versteckte sich vielmehr in den Computern eines kilometerweit entfernten Steuerungszentrums, das via Internet mit dem Umspannwerk verbunden war.

Dieser technologische Wandel hat sich ungefähr im letzten Jahrzehnt vollzogen. Früher enthielten Objekte Computer. Heute *sind* sie Computer, die mit Objekten verbunden sind. Und weil Computer immer kleiner und preiswerter werden, werden sie in immer mehr Objekte eingebettet, die dadurch selbst zu Computern werden. Vielleicht ist Ihnen das noch gar nicht aufgefallen, denn beim Kauf eines Autos oder eines Kühlschranks achten Sie wohl kaum auf die Rechenleistung, sondern auf die Fähigkeit, Personen zu transportieren bzw. Lebensmittel zu kühlen. Aber eigentlich handelt es sich um Computer – und das spielt eine wichtige Rolle, wenn es um die Sicherheit geht.

Unsere Vorstellung vom Internet hat sich ebenfalls verändert. Wir suchen keinen bestimmten Ort in unserem Zuhause oder im Büro mehr auf, um uns mit einem scheinbar separaten Raum namens Internet zu verbinden. Das Betreten von Chatrooms, das Herunterladen von E-Mails oder – in vielen Fällen – das Surfen im Internet gehören der Vergangenheit an.

Diese räumlichen Metaphern sind nicht mehr passend, und in ein paar Jahren wird die Bemerkung »Ich gehe ins Internet« ungefähr so viel Sinn ergeben wie beim Anschließen eines Toasters an einer Steckdose zu sagen »Ich gehe ins Stromnetz.«

Diese allgegenwärtige Verbindung mit dem Internet wird als das »Internet of Things« (kurz IoT) bezeichnet. Dabei handelt es sich vornehmlich um einen Marketingbegriff, der allerdings durchaus treffend ist. Das Unternehmen Gartner, das technische Analysen durchführt, definiert das IoT als »das Netzwerk physischer Objekte mit Embedded-Technologie, die es ihnen ermöglicht, interne Zustände oder die externe Umgebung zu erfassen oder damit zu interagieren«. Es geht also darum, alle möglichen Geräte über das Internet miteinander zu verbinden, sodass wir mit den Geräten, die Geräte untereinander sowie Geräte und verschiedene Computeranwendungen miteinander kommunizieren können.

Das Ausmaß dieses Wandels ist atemberaubend. 2017 waren 8,4 Milliarden Geräte mit dem Internet verbunden – hauptsächlich Computer und Telefone. Das entspricht einer Zunahme um ein Drittel im Vergleich zum Vorjahr. 2020 werden es voraussichtlich zwischen 20 und 75 Milliarden Geräte sein – je nachdem, wessen Prognose Sie Glauben schenken.

Dieses explosionsartige Wachstum wird durch Hersteller verursacht, die auf einen Wettbewerbsvorteil bedacht sind oder einfach nur mit der Konkurrenz Schritt halten wollen und zu dem Schluss gelangt sind, dass sie mit smarten Produkten Erfolg haben werden. Computer werden nicht nur immer kleiner, sondern auch billiger, deshalb werden wir sie in immer mehr Bereichen vorfinden.

Ihre Waschmaschine ist bereits ein Computer, der Kleidungsstücke wäscht. Wenn die neuesten, billigsten und leistungsfähigsten »Embedded-Computer« (eingebettete Computer) über eine Internetverbindung verfügen, wird es für Ihren Waschmaschinenhersteller einfacher, dieses Feature anzubieten. Und für Sie wird es immer schwieriger werden, eine Waschmaschine zu kaufen, die ohne Internetverbindung auskommt.

Vor zwei Jahren habe ich versucht, ein neues Auto zu kaufen, das keine Internetverbindung benötigt, und bin gescheitert. Es wurden zwar auch Autos ohne Internetverbindung angeboten, aber bei all den Modellen, die mir aus anderen Gründen zusagten, war ein Internetanschluss Standard. Und da die Kosten für diese Technologie sinken, wird sie überall Einzug hal-

ten. Das Internet wird zunehmend auch zum Bestandteil günstigerer und wenig vielseitiger Geräte werden, bis es überall zum Standard geworden ist.

Heutzutage mag es albern erscheinen, dass Ihre Waschmaschine über einen Internetanschluss verfügt, und ausgeschlossen, dass Ihr T-Shirt eines Tages einen besitzen wird. In einigen Jahren jedoch wird das der Normalzustand sein. Computer werden immer leistungsfähiger, kleiner und billiger. Damit internetfähige Bekleidung zur Norm wird, müssen lediglich die Kosten eines Mikroprozessors niedriger sein als der Gewinn, den ein Händler durch automatische Lagerhaltung (vor dem Verkauf) und automatisches Nachverfolgen des Gebrauchs (nach dem Verkauf) erzielen kann. Wenn ein weiteres Jahrzehnt vergangen ist, werden Sie womöglich keine T-Shirts ohne Sensoren mehr kaufen können und es für selbstverständlich halten, dass Ihre Waschmaschine mit der Wäsche kommuniziert und automatisch ermittelt, welches Waschprogramm und welches Waschmittel verwendet werden soll. Und der Waschmaschinenhersteller verkauft die Informationen, welche Kleidung Sie tragen – oder nicht mehr tragen –, an die Bekleidungshersteller.

Wenn ich mich zu diesem Thema äußere, gibt es immer Leute, die fragen: »Warum?« Sie können nachvollziehen, dass Anwendungen sinnvoll sind, mit denen sich Energie sparen lässt, begreifen aber nicht, weshalb jemand seine Kaffeetasse oder seine Zahnbürste mit dem Internet verbinden sollte. 2016 war ein Bericht über einen internetfähigen Kühlschrank überschrieben mit »Der Trend, alle Gegenstände smart zu machen, ist nun offiziell dämlich«.

Die Antwort auf die Frage »Warum?« ist ganz einfach: Marktwirtschaft. Wenn die Kosten für die Computerisierung sinken, verringert sich auch der Grenznutzen, der erforderlich ist, um die Computerisierung zu begründen – entweder in Form der bereitgestellten Features oder in Form der gesammelten Daten. Das könnte dem Verbraucher zugutekommen, wenn er zusätzliche Features erhält, oder aber dem Hersteller, weil er herausfindet, wie er die Produkte an seine Kunden vermarkten kann. Unterdessen wenden sich die Chiphersteller von spezialisierten Chips ab und fertigen stattdessen billige Allzweckchips in Massenproduktion. Sobald Embedded-Computer erst einmal standardisiert sind, ist es für die Hersteller günstiger, sie mit integrierter Internetverbindung zu kaufen, als diese Funktion wegzulassen. Es wird sehr kostengünstig möglich sein, eine Stadt buchstäblich mit Sensoren zu übersäen.

Alles zu computerisieren, hat verschiedene Vorteile. Einige davon sind schon heute erkennbar, andere zeigen sich erst, sobald die Anzahl dieser Computer eine kritische Masse erreicht hat. Das Internet of Things wird zum Bestandteil sämtlicher Aspekte des täglichen Lebens werden, und ich glaube nicht, dass wir vorhersagen können, wohin diese Entwicklung führen wird. Aufgrund ihres Ausmaßes und ihrer Reichweite werden wir einen grundlegenden Wandel erleben. Wenn das IoT an Größe zunimmt, wird sich auch sein Charakter verändern. In der Gesamtheit entsteht ein komplexes System, in dem alles miteinander verbunden ist. Auch wenn die einzelnen Bestandteile nicht direkt zusammenwirken, so befinden sie sich doch im selben Netzwerk und beeinflussen einander.

Diese Entwicklung geht über das Internet of Things hinaus. Betrachten Sie zunächst einmal das Internet of Things oder, allgemeiner formuliert, cyberphysische Systeme. Hinzu kommen die Miniaturisierung von Sensoren, Controllern und Sendern/Empfängern sowie autonome Algorithmen, Machine Learning und künstliche Intelligenz. Außerdem Cloud-Computing mit zunehmend wachsender Speicherkapazität und Rechenleistung. Die generelle Verbreitung des Internets, die allgegenwärtigen Computer und die weitreichende Verfügbarkeit schneller drahtloser Internetverbindungen müssen ebenfalls berücksichtigt werden. Und schließlich spielt auch die Robotertechnik eine Rolle. Zusammengenommen ergibt sich so ein globales Internet, das direkten physischen Einfluss auf seine Umwelt nimmt: ein Internet, das fühlt, denkt und handelt.

Das sind keine voneinander unabhängigen, eindeutigen Trends, sondern Entwicklungen, die sich angleichen, aufeinander aufbauen und sich gegenseitig verstärken. In der Robotertechnik kommen autonome Algorithmen zum Einsatz. Drohnen stellen eine Kombination aus dem IoT, Autonomie und Anwendungen auf mobilen Endgeräten dar. Smarte Werbetafeln kombinieren Personalisierung mit dem IoT. Und ein System, das den Wasserdurchfluss eines Staudamms steuert, kombiniert cyberphysische Systeme, autonome Agenten und (vermutlich) Cloud-Computing.

Auch wenn wir es lieber nicht wahrhaben wollen: In vielen dieser Systeme sind Menschen nicht mehr als ein Bestandteil unter vielen. Wir liefern den Computern Eingaben und nehmen ihre Ausgaben entgegen. Wir sind die Konsumenten ihrer automatisierten Funktionalität. Wir stellen die Verbindungen und die Kommunikationswege zwischen Systemen bereit, die noch nicht smart genug sind, ganz ohne uns zurechtzukommen. Wir tragen

diese Systeme mit uns herum – zumindest solche, die physisch autonom funktionieren. Wir nehmen Einfluss auf diese Systeme und werden von ihnen beeinflusst. Wir werden tatsächlich gewissermaßen zu virtuellen Cyborgs werden, auch wenn sich die Geräte außerhalb unseres Körpers befinden.

Für dieses neue »System aus Systemen« fehlt noch eine Bezeichnung. Es umfasst mehr als das Internet und mehr als das Internet of Things. Tatsächlich besteht es aus dem Internet + den Dingen, oder genauer: dem Internet + den Dingen + uns Menschen. Oder kurz und bündig: Internet+. Ich wünschte, ich hätte mir diesen Begriff nicht ausdenken müssen, allerdings ist es mir nicht gelungen, eine vorhandene Bezeichnung für die Kulmination all dieser Trends zu finden. Ich verwende also die Bezeichnung »Internet+«, zumindest in diesem Buch.

Wörter wie »smart« oder »denken« sind natürlich relativ und vor allem sehr ambitioniert, denn der überwiegende Teil des IoT ist nicht besonders smart, und ein Großteil wird noch sehr lange dumm bleiben. Dennoch wird es kontinuierlich smarter werden. Es ist zwar sehr unwahrscheinlich, dass es in absehbarer Zukunft Computer mit eigenem Bewusstsein geben wird, allerdings verhalten sich Computer bei bestimmten Aufgaben schon durchaus intelligent. Durch die ständig zunehmende Interkonnektivität wird das Internet+ nicht nur immer leistungsfähiger, sondern auch immer unsicherer. Dieses Buch beschreibt, warum dem so ist und was wir dagegen unternehmen können.

Die Sache ist ziemlich kompliziert, und ich beschreibe sie in zwei Teilen. In Teil I geht es um den aktuellen Stand der Computersicherheit in technischer, politischer und wirtschaftlicher Hinsicht sowie um die Entwicklungen, die dazu geführt haben. Computer werden immer kleiner und sind zunehmend besser in der Lage, ihre physische Umgebung zu beeinflussen, allerdings handelt es sich nach wie vor im Wesentlichen um die gleichen Computer, die wir seit Jahrzehnten verwenden. Die technischen Sicherheitsprobleme sind unverändert, und die politischen Fragen sind dieselben, mit denen wir schon immer zu kämpfen hatten. Und weil Computer und Kommunikationssysteme überall Einzug halten, gleicht sich eine Branche nach der anderen immer mehr der Computerbranche an. Computersicherheit spielt für die allgemeine Sicherheit eine immer bedeutendere Rolle, und die Lehren, die wir aus der Computersicherheit gezogen haben, werden sich auf alles übertragen lassen. Ob es sich bei einem Computer um ein

Auto, ein Kraftwerk oder um einen Biodrucker handelt, spielt keine Rolle, denn eins steht fest: Sie sind anfällig für Angriffe durch Hobbyisten, Aktivisten, Kriminelle, Nationalstaaten und alle anderen, die über technische Fähigkeiten verfügen.

In Kapitel 1 lege ich kurz die technischen Gründe dar, wieso das Internet so unsicher ist. In Kapitel 2 erörtere ich, wie wir versuchen, die Sicherheit unserer Systeme aufrechtzuerhalten, nämlich durch das Patchen von Sicherheitslücken, wenn sie entdeckt werden, und warum diese Vorgehensweise beim Internet+ scheitern wird. In Kapitel 3 geht es darum, wie wir uns im Internet identifizieren oder unsere Identität verbergen können. In Kapitel 4 beschreibe ich die politischen und wirtschaftlichen Kräfte, die zur Unsicherheit beitragen, nämlich Überwachungskapitalismus, Computer- bzw. Internetkriminalität und Cyberkrieg, sowie die aggressiven von Unternehmen und Regierungen eingesetzten Praktiken, die der Unsicherheit einen Nährboden bieten.

In Kapitel 5 erläutere ich, warum die Risiken zunehmen und wie sie zu einer Katastrophe führen können. »Click here to kill everybody« ist zwar eine Übertreibung, allerdings leben wir bereits in einer Welt, in der Computerangriffe Autounfälle verursachen und Kraftwerke lahmlegen können – und das sind Aktionen, die katastrophale, tödliche Ausmaße annehmen können, wenn sie in großem Maßstab durchgeführt werden. Wenn dann auch noch Hacks von Flugzeugen, medizinischen Geräten und praktisch der gesamten globalen kritischen Infrastruktur hinzukommen, ergibt sich ein ziemlich erschreckendes Gesamtbild.

Wenn Sie meine Bücher kennen und regelmäßig meine Artikel und mein Blog lesen, wird Ihnen vieles in Teil I bekannt vorkommen. Falls Ihnen das Ganze neu ist: Diese Kapitel bilden die Grundlage der nachfolgenden.

Das Problem bei der Sicherheit des Internet+ ist, dass wir uns alle an die aktuelle Situation gewöhnt haben. Bislang haben wir die Sicherheitsaspekte von Computern und dem Internet hauptsächlich dem Markt überlassen. Dieser Ansatz hat im Großen und Ganzen deshalb zufriedenstellend funktioniert, weil das Thema Sicherheit nicht so wichtig war. Es ging dabei vor allem um die Privatsphäre und lediglich um Kleinigkeiten. Wenn Ihr Computer gehackt wurde, gingen vielleicht wichtige Daten verloren oder Ihre Identität wurde gestohlen. Das war zwar sehr ärgerlich und mitunter kostspielig, aber keine Katastrophe. Doch jetzt, da alles ein Computer ist, sind

Leben und Eigentum bedroht. Hacker können mit Ihrem Auto einen Unfall bauen, Ihren Herzschrittmacher abschalten oder das Stromnetz Ihrer Stadt lahmlegen – und das ist katastrophal.

In Teil II des Buchs erläutere ich die Änderungen der Richtlinien, die erforderlich sind, um das Internet+ abzusichern. In Kapitel 6, Kapitel 7 und Kapitel 8 geht um die Verbesserung der Sicherheit des Internet+: was verbessert werden muss, wie das geschehen könnte und wer dafür verantwortlich ist. Nichts davon ist völlig neu oder sehr kompliziert, aber der Teufel steckt ja bekanntlich im Detail. Nach der Lektüre von Kapitel 8 sind Sie hoffentlich davon überzeugt, dass die Regierung die Verantwortung übernehmen muss. Diese Rolle der Regierung zuzuweisen, bedeutet zwar ein beträchtliches Risiko, aber es gibt keine praktikable Alternative. Der derzeit unzureichende Sicherheitszustand des Internet+ hat folgende Ursachen: falsch gesetzte wirtschaftliche Anreize, eine Regierung, die offensive Formen der Internetnutzung den defensiven vorzieht, Probleme kollektiven Handelns und ein Marktversagen, das durch Intervention behoben werden muss. In Kapitel 8 schlage ich unter anderem die Gründung einer Regierungsbehörde vor, die mit anderen staatlichen Stellen zusammenarbeitet und diese bezüglich der Sicherheitsrichtlinien und der Technologie des Internet+ berät. Vielleicht sind Sie anderer Meinung. Das ist völlig in Ordnung, aber diese Debatte muss geführt werden.

Kapitel 9 ist allgemeiner gehalten. Damit man ihr vertrauen kann, muss die Regierung der Defensive Vorrang vor der Offensive geben. Ich beschreibe, wie das vor sich gehen kann.

Aus praktischer Sicht ist es unwahrscheinlich, dass viele der von mir in Kapitel 6 bis Kapitel 9 vorgeschlagenen Änderungen der Richtlinien kurzfristig umgesetzt werden. Deshalb versuche ich in Kapitel 10, realistischer zu sein, und erläutere, was voraussichtlich geschehen wird und wie wir darauf reagieren können, sowohl in den Vereinigten Staaten als auch in anderen Ländern.

Kapitel 11 hat einige aktuelle politische Vorschläge zum Thema, die der Sicherheit des Internet+ tatsächlich schaden würden. Kapitel 12 ist wieder allgemeiner und zeigt auf, wie wir ein Internet+ erschaffen können, in dem Vertrauen, Stabilität und Frieden die Norm sind – und wie es gestaltet sein könnte.

Ich bin grundsätzlich der Meinung, dass eine vernünftige Regierung gute Arbeit leisten kann. Es kann schwierig sein, diesen Standpunkt zu ver-

treten, insbesondere in Anbetracht der ausgeprägt libertären Computerbranche, die tendenziell gegen eine Einmischung des Gesetzgebers und gegen Regulierung ist. Dieser Standpunkt ist jedoch von großer Bedeutung. Wir haben alle schon von den Fehlern der Regierung gehört, davon, wie mangelhaft sie ihre Aufgaben erledigt und dass sie schlicht und einfach den technologischen Fortschritt behindert. Weniger im Licht der Öffentlichkeit steht, dass die Regierung Märkte lenkt, Individuen schützt und als Gegengewicht zur Macht der Konzerne fungiert. Das Fehlen einer staatlichen Aufsicht ist einer der Hauptgründe dafür, dass das Internet+ heutzutage so unsicher ist. Und da die Risiken immer katastrophalere Ausmaße annehmen, ist eine Beteiligung der Regierung nötiger als je zuvor.

Ich beende das Buch mit einem Aufruf zum Handeln, der sowohl an die politischen Entscheidungsträger als auch an die technisch Verantwortlichen gerichtet ist. Die Erörterungen der Richtlinien sind ihrem Wesen nach sehr technisch. Wir brauchen deshalb politische Entscheidungsträger mit technischem Sachverstand und technisch Verantwortliche, die sich in der Politik engagieren. Wir müssen ein Fachgebiet erschaffen und fördern, das sich mit im öffentlichen Interesse stehenden Technologien befasst. Das ist nicht nur für die Sicherheit des Internet+ von Bedeutung, aber ich rufe dazu für meinen speziellen Technologiebereich auf, weil ich mich hier auskenne.

Im gesamten Buch kommen verschiedene weitere Themen zur Sprache.

- *Das Sicherheitswettrüsten*. Es ist oft aufschlussreich, Sicherheit als ein technologisches Wettrüsten zwischen Angreifer und Verteidiger zu betrachten. Der Angreifer entwickelt eine neue Technologie, und der Verteidiger reagiert darauf, indem er eine Schutztechnologie entwickelt. Oder der Verteidiger entwickelt eine neue Defensivtechnologie, die den Angreifer dazu zwingt, sich daran anzupassen. Wie sich dieses Wettrüsten im Internet+ abspielt, ist für das Verständnis der Sicherheit von entscheidender Bedeutung.
- *Vertrauen*. Wir denken zwar nur selten darüber nach, aber Vertrauen ist für das Funktionieren der Gesellschaft auf allen Ebenen ungemein wichtig. Im Internet ist Vertrauen allgegenwärtig. Wir vertrauen den Computern, der Software und den Internetdiensten, die wir nutzen. Wir vertrauen den unsichtbaren Teilen des Netzwerks und den Verfahren zur Herstellung der Geräte, die wir verwenden. Wie wir dieses Vertrauen aufrechterhalten und wie es untergraben wird, ist für das Verständnis der Sicherheit im Internet+ ebenfalls von entscheidender Bedeutung.

- *Komplexität.* Bei diesen Aufgaben ist alles komplex: die Technologie, die Richtlinien und das Zusammenspiel von Technologie und Richtlinien. Politik, Wirtschaft und Soziologie sind ebenfalls in vielerlei Hinsicht komplex, und die Komplexität nimmt im Laufe der Zeit weiter zu. Die Sicherheit im Internet+ ist ein sogenanntes »Wicked Problem«. »Wicked« bedeutet nicht, dass das Problem »böse« ist, sondern dass es schwer oder gar nicht lösbar ist. Das liegt daran, dass es schon knifflig ist, die Aufgabe und die Anforderungen überhaupt zu definieren, geschweige denn, eine brauchbare Lösung zu finden.

In diesem Buch kommen sehr viele verschiedene Themen zur Sprache, deshalb werden sie oft nur beiläufig und oberflächlich erwähnt. Die ausführlichen Endnoten sollen sowohl als Referenz als auch als Einladung zur weiteren Lektüre dienen. Sie wurden Ende April 2018 überprüft und sind auf der englischen Website zum Buch als anklickbare Links zu finden: *https://www.schneier.com/ch2ke.html*. Auch Aktualisierungen zum Buch werden gegebenenfalls dort veröffentlicht. Auf *https://www.schneier.com* finden Sie zudem meinen monatlich erscheinenden E-Mail-Newsletter und mein täglich aktualisiertes Blog zu diesen Themen sowie alle anderen Veröffentlichungen von mir.

Ich betrachte diese Herausforderungen von einer Metaebene aus. Ich bin vor allem Technologe, kein Entscheidungsträger und schon gar kein politischer Analyst. Ich bin in der Lage, technologische Lösungen für Sicherheitsprobleme zu beschreiben, und kann sogar erklären, welche neuen Arten von Richtlinien erforderlich sind, um die technologischen Lösungen zu finden, zu entwickeln und zu implementieren. Ich schreibe jedoch nichts über die Politik, die zu dieser Änderung der Richtlinien führt. Wie Sie Unterstützung für derartige Gesetzesänderungen gewinnen und diese durchsetzen können, kann ich Ihnen nicht sagen, nicht einmal, wie Sie erreichen, dass zumindest deren Realisierbarkeit erörtert wird. Hierbei handelt es sich um eine klaffende Lücke in diesem Buch, die ich in Kauf nehme.

Darüber hinaus schreibe ich aus Sicht der Vereinigten Staaten. Die meisten Beispiele entstammen den USA, und die meisten Empfehlungen sind auf die dortige Situation anwendbar. Zum einen kenne ich mich in meiner Heimat am besten aus. Zum anderen glaube ich allerdings auch, dass die USA ein ausgezeichnetes Beispiel dafür sind, was schiefgehen kann. Zugleich befinden sie sich – aufgrund ihrer Größe und ihrer Marktposition – in der einzigartigen Lage, die Umstände verbessern zu können. In diesem

Buch geht es zwar nicht schwerpunktmäßig um internationale Belange oder die Geopolitik der Sicherheit des Internets, diese Themen sind jedoch in den verschiedenen Kapiteln eingestreut.

Die Fragestellungen, um die es hier geht, entwickeln sich kontinuierlich weiter, und ein Buch wie dieses kann dementsprechend nur eine Momentaufnahme liefern. Als ich im März 2014 das Buch *Data and Goliath* (dt. Ausgabe *Data und Goliath*, 2015) fertiggestellt hatte, machte ich mir Sorgen, weil das Buch erst sechs Monate später erscheinen sollte. Ich hoffte, dass während dieses Zeitraums nichts geschieht, durch das die Inhalte des Buches überholt wären. So geht es mir jetzt wieder, allerdings bin ich zuversichtlicher. Denn es ist sehr unwahrscheinlich, dass ein bedeutendes Ereignis eintritt, das ein Umschreiben des Buchs erforderlich machen würde. Mit Sicherheit werden neue Geschichten und Beispiele auftauchen, aber das hier beschriebene Gesamtbild wird wahrscheinlich noch viele Jahre aktuell bleiben.

Die Zukunft der Sicherheit des Internet+ – oder die Cybersicherheit, wenn Ihnen militärische Ausdrücke zusagen – ist ein riesiges Themengebiet, und für die meisten Kapitel dieses Buchs wären eigentlich eigene Bücher angemessen. Ich habe die Hoffnung, dass ich den Lesern einen Überblick verschaffen, ein Gespür für die Probleme vermitteln und einen ungefähren Plan für Verbesserungen liefern kann, indem ich thematisch nicht in die Tiefe, sondern in die Breite gehe. Mein Ziel ist es, dass sich ein größeres Publikum an dieser wichtigen Debatte beteiligt, und ich möchte den Lesern das Wissen für eine sachkundige Diskussion vermitteln. Wir werden in den kommenden Jahren bedeutsame Entscheidungen treffen. Selbst wenn wir uns entschließen, nichts zu ändern, ist das eine wichtige Entscheidung.

Die Risiken werden nicht verschwinden. Sie sind nicht auf Länder mit wenig entwickelter Infrastruktur oder eher totalitären Regierungen beschränkt. Und sie werden auch dann nicht verschwinden, wenn wir endlich Ordnung in das Durcheinander des zerrütteten politischen Systems in den Vereinigten Staaten gebracht haben. Die Probleme werden auch nicht durch die Kräfte des Marktes wie von Zauberhand von allein gelöst werden. Wenn es Lösungen geben wird, dann nur deshalb, weil wir uns bewusst dazu entschlossen haben und bereit sind, den politischen, wirtschaftlichen und sozialen Aufwand, der mit diesen Lösungen verbunden ist, in Kauf zu nehmen.

Die ganze Welt ist voller Computer, und wir müssen diese Computer absichern. Dazu müssen wir umdenken. Der frühere FCC-Vorsitzende Tom Wheeler scherzte 2017 auf einer Konferenz zum Thema Internetsicherheit in Anlehnung an die ehemalige US-Außenministerin Madeleine Albright: »Wir stehen vor einem Problem des 21. Jahrhunderts, diskutieren es mit Begriffen aus dem 20. Jahrhundert und schlagen Lösungen aus dem 19. Jahrhundert vor.« Er hat völlig recht – das müssen wir besser machen. Unsere Zukunft hängt davon ab.

– Minneapolis, Minnesota und Cambridge, Massachusetts, April 2018

Dank

Man sollte meinen, dass man nach einem Dutzend Büchern allmählich weiß, wie der Hase läuft. Aber jedes Buch ist anders. Ich habe mit der Arbeit an diesem Buch zu früh nach *Data and Goliath* begonnen und deshalb wohl einige Fehlstarts hingelegt. Ich habe mit dem Schreiben des Buchs, das Sie gerade lesen, im Sommer 2017 angefangen und es Ende März 2018 zur Veröffentlichung eingereicht.

Bei meinen anderen Büchern wurde ich von einem Spitzenteam unterstützt, das auch bei diesem Buch wieder zusammengefunden hat. Kathleen Seidel ist eine außerordentliche Forscherin, die auch ein gutes Gespür für Prosa besitzt, im Großen wie im Kleinen. Beth Friedmann hat alles redigiert, was ich in den letzten 20 Jahren geschrieben habe. Sie kennt mich und meinen Schreibstil, und ich wüsste nicht, was ich ohne sie machen sollte. Sie hat das Buch nicht nur redigiert, bevor es beim Verlag eingereicht wurde, sondern sie hat sich auch mit der dortigen Redakteurin auseinandergesetzt, damit ich das nicht tun musste. Rebecca Kessler hat eine dringend nötige Überarbeitung vorgenommen, als das Buch schon fast fertig war. Sie ist ebenfalls unbezahlbar. Zu diesen drei kommt noch Katherine Mansted hinzu, die kurz vor Fertigstellung weitere Beiträge und Zusammenfassungen lieferte.

Viele Leute haben das gesamte Manuskript oder Teile davon gelesen. Alle gefundenen Fehler und Hinweise auf Unklarheiten haben zur Verbesserung des Buchs beigetragen. Hier sind diese Menschen: Michael Adame, Ross Anderson, Steve Bass, Michael Brennan, John Bruce, Cody Charette, John Davis, Judith Donath, Nora Ellingsen, Mieke Eoyang, Greg Falco, Hubert Feyrer, John Fousek, Brett Frischmann, Blair Ganson, Jason Giffey, Jack Goldsmith, Chloe Goodwin, Sarah Grant, Eldar Haber, Bill Herdle,

Trey Herr, Christopher Izant, Andrei Jaffe, Danielle Kehl, Eliot Kim, Xia King, Jonathan Korn, Nadiya Kostyuk, Alexander Krey, Lydia Lichlyter, Aleecia McDonald, Daniel Miessler, Adam Montville, Kee Nethery, David O'Brien, Christen Paine, David Perry, Stuart Russell, Martin Schneier, Nick Sinai, Nathaniel Sobel, Hannah Solomon-Strauss, Lance Spitzner, Stephen Taylor, Marc van Zadelhoff, Arun Vishwanath, Sara M. Watson, Jarad Webber, Tom Wheeler und Ben Wizner. Es ist keine Übertreibung, zu behaupten, dass dieses Buch ohne sie deutlich schlechter wäre.

W. W. Norton (der amerikanische Originalverlag) ist und bleibt hervorragend und ich möchte meinem ursprünglichen Lektor Jeff Shreve sowie Brendan Curry danken, der nach Jeffs Ausscheiden seine Aufgaben übernommen hat. Jeff hatte den übereilten Vertrag unterzeichnet und erwies sich als sehr geduldig, als ich ins Schwimmen kam und den geplanten Abgabetermin verpasste. Mir ist klar, dass es sich nach einem Klischee anhört, zu sagen, dass mein Lektor nie das Vertrauen in mich verloren hat – tatsächlich habe ich keine Ahnung, was in seinem Kopf vorgeht –, aber er *behauptet selbst*, nie das Vertrauen in mich verloren zu haben. Und Norton wollte den Vorschuss nicht zurücknehmen, obwohl ich die Rückzahlung anbot. Brendan Curry hatte es leichter. Zu dem Zeitpunkt, als er übernahm, machte ich tatsächlich Fortschritte. Seine Arbeit bei der Veröffentlichung war vorbildlich, insbesondere in Anbetracht der Tatsache, dass ich ständig auf einen engeren Zeitplan drängte.

Auch Susan Rabiner ist und bleibt eine ausgezeichnete Agentin. Wenn es lediglich um das Aushandeln eines Vertrags ginge, könnte jeder diese Aufgabe erledigen, aber ich bin immer wieder überrascht, wie wichtig es ist, dass jemand zwischen mir und dem Verlag vermittelt.

Ich möchte auch der Harvard University danken – dem Berkman Klein Center for Internet & Society, dem Cybersicherheitsprojekt am Belfer Center for Science and International Affairs im Besonderen sowie der Harvard Kennedy School of Government im Allgemeinen, die mir beim Schreiben, bei Vorträgen und beim Unterrichten ein Zuhause bietet. Ich schätze meine Kollegen und Freunde, die in diesen Institutionen tätig sind, wirklich sehr. Dieses Buch ist von ihren Ideen und Idealen durchdrungen. Ich möchte meinem Hauptarbeitgeber Resilient Systems (aus dem inzwischen IBM Resilient geworden ist, das wiederum schon bald ein Teil von IBM Security sein wird) danken, dass er mir den für das Schreiben und die Veröffentlichung dieses Buchs erforderlichen Raum gegeben hat.