BRUCE SCHNEIER

CLICK HERE TO KILL EVERYBODY

Sicherheitsrisiko Internet
und die Verantwortung von
Unternehmen und Regierungen

mitp

Inhalt

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.

Zum Abschluss möchte ich meiner Frau Karen Cooper, mit der ich seit 21 Jahren verheiratet bin, sowie allen Freunden und Kollegen dafür danken, dass sie Geduld mit mir hatten, während ich das Buch schrieb. Ich neige dazu, eine gewisse Abhängigkeit von meinen Buchmanuskripten zu entwickeln. Wenn mit ihnen alles in Ordnung ist, geht es mir gut. Falls Schwierigkeiten auftreten, bin ich unzufrieden. Dieses Buch hatte, wie alle anderen auch, so seine Momente. Ich danke euch allen für eure Geduld und euer Wohlwollen.

1

Computer sind immer noch schwierig zu sichern

Sicherheit ist immer eine Frage von Kompromissen. Meistens muss Sicherheit gegen Bequemlichkeit abgewogen werden, manchmal auch gegen Funktionalität oder Performance. Dass wir diese Eigenschaften der Sicherheit vorziehen, ist der Hauptgrund dafür, dass Computer unsicher sind. Allerdings ist es auch alles andere als einfach, Computer abzusichern.

Berühmt ist das folgende Zitat des Internetsicherheitsforscher Gene Spafford: »Das einzige wirklich sichere System ist ausgeschaltet, in einen Betonblock eingegossen und befindet sich in einem mit Blei abgeschirmten, versiegelten Raum, der von bewaffnetem Sicherheitspersonal bewacht wird – und selbst dann habe ich noch meine Zweifel.« Diese Aussage stammt aus dem Jahr 1989 und ist damit fast 30 Jahre alt, aber immer noch richtig.

Sie trifft auf herkömmliche Computer ebenso zu wie auf die mit dem Internet verbundenen Embedded-Computer, die heute allgegenwärtig sind. Der ehemalige Direktor des National Cybersecurity Center, Rod Beckstrom, fasste die Situation kürzlich folgendermaßen zusammen:

1. Alle mit dem Internet verbundenen Geräte können gehackt werden.
2. Alle Geräte sind mit dem Internet verbunden.
3. Folglich können alle Geräte gehackt werden.

Tatsächlich ist es dermaßen schwierig, Computer abzusichern, dass jeder Sicherheitsforscher einen eigenen pointierten Spruch zu diesem Thema parat hat. Meiner stammt aus dem Jahr 2000 und lautet: »Sicherheit ist ein Prozess und kein Produkt.«

Die Gründe dafür sind äußerst vielfältig.

Die meiste Software ist schlecht programmiert und unsicher

Ich spiele Pokémon Go auf meinem Smartphone, und das Spiel stürzt ständig ab. Es ist extrem instabil, aber das ist nichts Ungewöhnliches. Wir kennen das alle. Unsere Computer und Smartphones hängen sich regelmäßig auf. Websites werden nicht geladen. Features funktionieren nicht. Wir sichern unsere Daten zwanghaft und erstellen Sicherheitskopien unserer Dateien oder verwenden Systeme, die das automatisch für uns erledigen. Wir starten unsere Computer neu, wenn sie anfangen, sich merkwürdig zu verhalten. Hin und wieder verlieren wir wichtige Daten. Und wir erwarten auch gar nicht, dass unsere Computer genauso zuverlässig funktionieren wie die anderen Produkte, die wir im Alltag verwenden, obwohl wir stets frustriert sind, wenn sie es nicht tun.

Die Software ist so mangelhaft programmiert, weil der Markt qualitativ hochwertige Software – von einigen wenigen Ausnahmen abgesehen – nicht honoriert. »Gut, schnell, billig – Sie können nur zwei davon wählen«; geringe Kosten und schnelle Verfügbarkeit auf dem Markt sind in der Regel wichtiger als die Qualität. Für die meisten von uns hat sich mangelhaft programmierte Software in vielen Fällen als gut genug erwiesen.

Die Softwarebranche ist auf allen Ebenen von dieser Philosophie durchdrungen. Die Unternehmen belohnen qualitativ hochwertige Software nicht im selben Maß wie eine frühzeitige Fertigstellung oder eine Unterschreitung des Budgets. Universitäten legen vor allem Wert darauf, dass Code funktioniert, und sei es auch nur notdürftig, seine Zuverlässigkeit ist weniger wichtig. Und die meisten Nutzer sind nicht bereit, die Kosten zu tragen, die mit einer höheren Qualität verbunden wären.

Moderne Software ist mit unzähligen Bugs gespickt. Einige davon sind aufgrund der Komplexität der Software unvermeidlich – mehr dazu später –, aber die meisten sind Programmierfehler, die während des Entwicklungsprozesses nicht behoben wurden. Nachdem die Entwicklung abgeschlossen und die Software ausgeliefert wurde, sind diese Bugs noch immer vorhanden. Dass auf diese Weise erstellte Software überhaupt funktioniert, zeigt nur, wie gut wir mit den Einschränkungen fehlerhafter Software umgehen können.

Natürlich sind nicht alle Entwicklungsprozesse von Software miteinander vergleichbar. Microsoft hat das Jahrzehnt nach 2002 der Prozessverbes-

serung gewidmet, um die Anzahl der Sicherheitslücken in der ausgelieferten Software zu minimieren. Die Produkte sind zwar beileibe nicht perfekt – das liegt noch außerhalb der Möglichkeiten der Technologie –, sie sind jedoch deutlich besser als der Durchschnitt. Apple ist für die Qualität seiner Software bekannt, ebenso Google.

Es gibt auch kleine Programmteile von entscheidender Bedeutung, die qualitativ hochwertig sind. So unterliegt etwa die Software zur Steuerung der Bordelektronik von Flugzeugen einer sehr strengen Qualitätskontrolle. Und die Qualitätskontrolle der NASA für die Software der Spaceshuttles ist legendär.

Dass es sich hierbei um Ausnahmen handelt, hängt sowohl mit der Branche als auch mit den betroffenen Unternehmen zusammen: Die Betriebssystemhersteller investieren grundsätzlich sehr viel Geld, kurze Codeabschnitte korrekt zu programmieren, ist relativ einfach, und Steuerungssoftware für Flugzeuge ist hochgradig reglementiert. Die Standards der Qualitätskontrolle der NASA sind nach wie vor extrem konservativ. Und selbst vergleichsweise hochwertige Systeme wie Windows, macOS, iOS und Android müssen ständig gepatcht werden.

Einige dieser Bugs stellen auch Sicherheitslücken dar, von denen wiederum einige von Angreifern ausgenutzt werden können. Ein typisches Beispiel für einen solchen Bug ist ein sogenannter »Buffer-Overflow« (Pufferüberlauf). Dabei handelt es sich um einen Programmierfehler, der es einem Angreifer unter bestimmten Umständen ermöglicht, das Programm zu zwingen, beliebigen Code auszuführen und so die Kontrolle über den Rechner zu übernehmen. Es gibt eine Vielzahl von potenziellen Fehlern wie diesen. Einige davon unterlaufen den Programmierern leichter als andere.

Es ist schwierig, hier Zahlen zu nennen. Wir wissen nicht, wie viel Prozent der Bugs auch Sicherheitslücken darstellen und wie groß der Anteil der ausnutzbaren Sicherheitslücken ist. Deshalb wird zu Recht diskutiert, ob ausnutzbare Sicherheitslücken eher selten oder doch massenhaft vorhanden sind. Ich bin der festen Überzeugung, dass sie sehr zahlreich sind. Umfassende Softwaresysteme weisen Tausende ausnutzbarer Sicherheitslücken auf, und man muss nur eine einzige davon finden, um in das System einzubrechen.

Sicherheitslücken sind also reichlich vorhanden, das heißt jedoch nicht, dass sie gleichmäßig verteilt sind. Manche sind leicht zu finden, bei anderen ist es schwieriger. Die Sicherheit von Software wurde durch Tools, die ganze

Klassen von Sicherheitslücken aufspüren und beheben können, erheblich verbessert. Wenn jemand eine Sicherheitslücke entdeckt, ist es wahrscheinlich, dass jemand anderes sie ebenfalls bald entdecken wird oder schon entdeckt hat. Heartbleed zum Beispiel ist eine Sicherheitslücke in der OpenSSL-Bibliothek, die zwei Jahre lang unentdeckt blieb. Dann wurde sie innerhalb weniger Tage unabhängig voneinander von zwei Forschern entdeckt. Die Sicherheitslücken Spectre und Meltdown, die Mikroprozessoren betreffen, existierten schon mindestens zehn Jahre, bevor sie 2017 von mehreren Forschern entdeckt wurden. Dass diese Sicherheitslücken zur gleichen Zeit gefunden wurden, scheint Zufall zu sein, zumindest kenne ich keine andere plausible Erklärung. Wir werden in Kapitel 9 darauf zurückkommen, wenn es darum geht, dass Regierungen Sicherheitslücken horten, um sie zur Spionage und als Cyberwaffen einzusetzen.

Mit der explosionsartigen Zunahme der Anzahl von IoT-Geräten sind mehr Software, mehr Codezeilen und dementsprechend noch mehr Bugs und weitere Sicherheitslücken verbunden. Die niedrigen Preise von IoT-Geräten bedeuten weniger sachkundige Programmierer, nachlässigere Softwareentwicklungsprozesse und mehr wiederverwendeten Code. Einzelne Sicherheitslücken haben noch weitreichendere Auswirkungen, da sie unzählige Male vervielfältigt werden. Die von uns verwendete Software, die auf unseren Computern und Smartphones, auf medizinischen Geräten, im Internet und auf Systemen zur Steuerung kritischer Infrastruktur läuft, ist also in mehrfacher Hinsicht unsicher. Das lässt sich nicht einfach dadurch lösen, dass die einzelnen Sicherheitslücken gefunden und behoben werden – dafür sind es viel zu viele. Vielmehr ist unsichere Software ein Problem, mit dem wir auf absehbare Zeit leben müssen.

Sicherheit spielte bei der Entwicklung des Internets keine Rolle

Im April 2017 wurde plötzlich rund 18 Minuten lang 15 Prozent des gesamten Datenverkehrs im Internet über chinesische Server umgeleitet. Wir wissen nicht, ob die chinesische Regierung dahintersteckte und Überwachungsmöglichkeiten getestet hat oder ob es sich tatsächlich um ein Versehen handelte. Wir wissen aber sehr wohl, wie die Angreifer das angestellt haben: Sie nutzten eine Schwäche des Border Gateway Protocol aus.

Das Border Gateway Protocol oder kurz BGP legt fest, wie der Datenverkehr des Internets physisch durch diverse Kabel und andere Verbindungen zwischen den Internetanbietern und den verschiedenen Ländern bzw. Kontinenten geleitet wird. Da es keine Authentifizierung gibt und alle beteiligten Systeme sämtlichen Informationen über die Geschwindigkeit einer Verbindung und deren Auslastung vertrauen, kann das BGP manipuliert werden. Dank der von dem Whistleblower und ehemaligen CIA-Mitarbeiter Edward Snowden offengelegten Dokumente wissen wir, dass die NSA diese Schwachstelle des Protokolls ausnutzt, um bestimmte Datenströme leichter abhören zu können. 2013 berichtete ein Unternehmen von 38 Vorfällen, bei denen der Internetdatenverkehr über in Weißrussland oder bei isländischen Providern befindliche Router umgeleitet wurde. 2014 nutzte die türkische Regierung dieses Verfahren, um Teile des Internets zu zensieren. 2017 wurde ein- und ausgehender Datenverkehr mehrerer bedeutender Internetprovider in den Vereinigten Staaten kurzzeitig über einen obskuren russischen Provider umgeleitet. Und diese Angriffsmethode wird nicht nur von Staaten eingesetzt. Schon 2008 wurde in einem Vortrag auf der Hackerkonferenz DefCon vorgeführt, wie jeder davon Gebrauch machen kann.

Als das Internet entwickelt wurde, ging es bei der Sicherheit vornehmlich um den Schutz vor physischen Angriffen auf das Netzwerk. Dank der fehlertoleranten Architektur kann das Internet mit dem Ausfall oder der Zerstörung von Servern und Verbindungen umgehen. Mit systembedingten Angriffen auf die zugrunde liegenden Protokolle kommt es hingegen nicht zurecht.

Bei der Entwicklung der grundlegenden Internetprotokolle wurde der Sicherheit keine Beachtung geschenkt, und viele davon sind noch heute unsicher. Das Absenderfeld einer E-Mail wird beispielsweise überhaupt nicht überprüft: Als Absender kann eine beliebige Person oder Firma angegeben werden. Der Domain Name Service (DNS), der für Menschen verständliche Bezeichnungen in numerische Internetadressen übersetzt, ist ebenfalls ungeschützt. Auch das Network Time Protocol, das für die zeitliche Synchronisierung sorgt, ist unsicher, ebenso wie das ursprüngliche HTML-Protokoll, auf dem das World Wide Web beruht. Das etwas sicherere HTTPS-Protokoll weist immer noch eine Reihe von Sicherheitslücken auf. All diese Protokolle können von Angreifern leicht für ihre Zwecke missbraucht werden.

Entwickelt wurden diese Protokolle in den 1970ern und Anfang der 1980er-Jahre, als das Internet nur für Forschungseinrichtungen zugänglich war und nicht für kritische Aufgaben genutzt wurde. Der MIT-Professor David Clark, einer der Architekten des frühen Internets, erinnert sich: »Es ist nicht so, dass wir uns keine Gedanken um die Sicherheit gemacht hätten. Uns war klar, dass es irgendwo da draußen Menschen gab, die nicht vertrauenswürdig waren, aber wir dachten, wir könnten sie von der Nutzung des Internets ausschließen.« Ja, sie glaubten damals tatsächlich, sie könnten den Internetzugang auf ihnen bekannte Personen beschränken.

Noch bis Ende 1996 war die vorherrschende Meinung, dass die Endpunkte, also die Computer, vor denen die Leute sitzen, für die Sicherheit zuständig sind, nicht das Netzwerk. Die Internet Engineering Task Force (IETF), die für die Industriestandards des Internets verantwortlich zeichnet, äußerte sich dazu 1996 folgendermaßen:

Es ist erstrebenswert, dass Netzbetreiber die Privatsphäre schützen und die Authentizität sämtlichen Datenverkehrs sicherstellen, doch die Architektur erfordert das nicht. Für Vertraulichkeit und die Authentifizierung sind die Nutzer verantwortlich, und beides muss in den von ihnen verwendeten Protokollen implementiert werden. Die Endpunkte sollten nicht auf die Vertraulichkeit und Integrität der Netzbetreiber angewiesen sein. Die Netzbetreiber können gewisse Schutzmaßnahmen bereitstellen, die aber der Verantwortlichkeit des Nutzers, sich selbst zu schützen, untergeordnet sind.

Das ist gar nicht so unvernünftig, wie es vielleicht auf den ersten Blick erscheint. In Kapitel 6 komme ich auf das Ende-zu-Ende-Netzwerkmodell zu sprechen, bei dem, wie von der IETF beschrieben, nicht das Netzwerk für die Sicherheit verantwortlich ist. Die Anwender waren jedoch viel zu lange uneinsichtig, und selbst Sicherheitsaspekte, die ohnehin nur innerhalb des Netzwerks sinnvoll sind, wurden nicht berücksichtigt.

Das zu ändern war schwierig und manchmal sogar unmöglich. Die IETF hat schon seit Anfang der 1990er-Jahre immer wieder Vorschläge zur Erhöhung der BGP-Sicherheit gemacht, um Angriffen vorzubeugen, aber all diese Maßnahmen krankten stets daran, dass kein gemeinsames Handeln zustande kam. Die besser abgesicherten Systeme einzusetzen, bot nur dann Vorteile, wenn es in hinreichend vielen Netzwerken geschah. Die ersten Umsteiger wurden für ihre harte Arbeit also kaum belohnt. Das Ganze führte zu einer absurden Situation: Für einen Provider ist es wenig sinnvoll, die neue Technologie als Erster einzuführen, weil sie mit hohen Kosten ver-

bunden ist und praktisch keinen Nutzen hat. Es erscheint erheblich klüger, zu warten, bis andere die Umstellung vollziehen. Das Ergebnis kennen wir natürlich: Das Problem ist seit 20 Jahren bekannt, aber es gibt noch immer keine Lösung.

Es gibt weitere vergleichbare Beispiele. DNSSEC ist ein Upgrade, das die Sicherheitsprobleme des DNS-Protokolls lösen würde. Das DNS-Protokoll ist wie das BGP ungeschützt, und das System ist dadurch auf vielfältige Weise angreifbar. Und wie beim BGP ist es 20 Jahre her, dass die Tech-Community eine Lösung entwickelt hat, die jedoch noch nicht implementiert wurde, weil die Mehrheit der DNS-Server sie zunächst übernehmen müsste, bevor irgendjemand einen Vorteil davon hat.

Erweiterbarkeit heißt, alles kann gegen uns verwendet werden

Erinnern Sie sich an die altmodischen Telefone, die Ihre Eltern oder Großeltern zu Hause verwendeten? Ein solches Gerät war dafür ausgelegt, damit zu telefonieren, nicht mehr und nicht weniger. Vergleichen Sie das einmal mit dem Telefon, das Sie in der Tasche haben. Eigentlich ist es gar kein Telefon, sondern ein Computer, auf dem eine Telefon-App läuft. Und wie Sie wissen, kann das Gerät noch sehr, sehr viel mehr. Es ist ein Telefon, eine Kamera, ein Benachrichtigungssystem, ein E-Book-Reader, ein Navigationsgerät und eine Million andere Dinge. Der Spruch »There's an app for that« ergibt für ein altmodisches Telefon keinen Sinn, für einen Computer, mit dem Sie Anrufe tätigen können, aber sehr wohl.

Nachdem Johannes Gutenberg 1440 die Druckpresse erfunden hatte, wurde die Technologie im Laufe der nachfolgenden Jahrhunderte erheblich verbessert, allerdings handelte es sich noch immer um das gleiche mechanische – und später elektromechanische – Gerät. Während all dieser Jahrhunderte blieb eine Druckpresse immer eine Druckpresse. Der Drucker konnte sich die größte Mühe geben, aber die Maschine war nicht dazu zu bewegen, Berechnungen durchzuführen, Musik abzuspielen oder Fisch abzuwiegen. Gleichermaßen war ein Thermostat nur ein elektromechanisches Gerät mit einem Temperaturfühler, der auf unterschiedliche Messwerte mit dem Öffnen oder Schließen eines Schaltkreises reagierte. Dieser Schaltkreis war mit der Heizung verbunden, was es dem Thermostat ermög-

lichte, die Temperatur zu regeln. Und das war auch schon alles, was er konnte. Auch eine Kamera konnte früher nur Fotos aufnehmen.

Heutzutage sind solche Geräte Computer und können somit für nahezu alle Aufgaben programmiert werden. Das haben einige Hacker kürzlich demonstriert, indem sie einen PIXMA-Drucker von Canon, das Thermostatmodell Honeywell Prestige und eine Digitalkamera von Kodak darauf programmiert haben, den Ego-Shooter Doom zu spielen.

Wenn ich diese Anekdote bei technischen Konferenzen auf der Bühne zum Besten gebe, lacht das Publikum darüber, dass diese neuen IoT-Geräte ein 25 Jahre altes Computerspiel steuern können – aber überrascht ist davon niemand. Schließlich handelt es sich um Computer, die selbstverständlich darauf programmiert werden können, Doom zu spielen.

Wenn ich diese Anekdote hingegen einem technisch nicht versierten Publikum erzähle, fallen die Reaktionen ganz anders aus. Unser mentales Modell von Maschinen besagt, dass sie nur eine einzige Aufgabe erledigen können – und wenn sie kaputt sind, funktioniert auch das nicht mehr. Allzweckcomputer ähneln in dieser Hinsicht jedoch eher Menschen; sie können fast jede beliebige Aufgabe übernehmen.

Computer können erweitert werden. Und wenn alles zu einem Computer wird, dann ist bald auch alles erweiterbar. Bezüglich der Sicherheit zieht das drei Konsequenzen nach sich:

Erstens: Es ist schwierig, erweiterbare Systeme abzusichern, weil die Designer nicht alle Konfigurationen, Umgebungsbedingungen, Anwendungen, Verwendungsmöglichkeiten usw. voraussehen können. Hier geht es eigentlich um Komplexität, ein Thema, auf das wir in Kürze noch kommen werden.

Zweitens: Erweiterbare Systeme lassen sich nicht extern beschränken. Es ist problemlos möglich, ein mechanisches Abspielgerät zu konstruieren, das nur Magnetbänder abspielt, die sich in einem bestimmten Gehäuse befinden, oder eine Kaffeemaschine zu bauen, die nur Einwegkaffeekapseln von bestimmter Form verwenden kann. Doch derartige physische Beschränkungen sind nicht auf die digitale Welt übertragbar. Das bedeutet, dass ein Kopierschutz – auch bekannt unter der Bezeichnung DRM (Digital Rights Management, digitale Rechteverwaltung) – im Grunde unmöglich ist. Wie die Erfahrungen der Musik- und Filmbranche in den vergangenen zwei Jahrzehnten gezeigt haben, kann man die Leute nicht davon abhalten, unautorisierte Kopien digitaler Dateien anzufertigen und abzuspielen.

Allgemeiner formuliert kann ein Softwaresystem nicht eingeschränkt werden, weil die zur Einschränkung eingesetzte Software umfunktioniert, umgeschrieben oder überarbeitet werden kann. Ebenso wie es unmöglich ist, ein Abspielgerät zu bauen, das keine raubkopierten Musikdateien wiedergibt, ist es auch unmöglich, einen 3D-Drucker zu entwickeln, der keine Bauteile für Schusswaffen druckt. Es ist natürlich relativ einfach, Otto Normalverbraucher davon abzuhalten, aber ein Experte lässt sich nicht aufhalten. Und sobald ein Experte Software geschrieben hat, um die wie auch immer gearteten Beschränkungen zu umgehen, können alle anderen sie ebenfalls nutzen. Und das geht sogar ziemlich schnell. Selbst die besten DRM-Systeme werden in weniger als 24 Stunden geknackt. In Kapitel 11 kommen wir auf dieses Thema zurück.

Drittens: Erweiterbarkeit bedeutet auch, dass jeder Computer durch Software um zusätzliche Features ergänzt werden kann. Diese können versehentlich Sicherheitslücken mit sich bringen, sowohl weil die neuen Features selbst angreifbar sind als auch weil sie im ursprünglichen Design nicht vorgesehen waren. Entscheidend ist jedoch, dass auch Angreifer neue Features hinzufügen können. Wenn jemand Ihren Computer hackt und Schadsoftware installiert, geschieht genau das. Dabei handelt es sich zwar um Features, die Sie nicht haben wollen, um die Sie nicht gebeten haben und die sogar gegen Ihre Interessen gerichtet sind, aber dessen ungeachtet sind es Features. Und diese Features können, zumindest theoretisch, allen anderen mit dem Internet verbundenen Computern ebenfalls hinzugefügt werden.

Hintertüren (auch »Backdoors« genannt) sind ein weiteres zusätzliches Feature eines Systems. Ich werde diesen Begriff im Buch sehr oft verwenden, deshalb lohnt es, einen Moment innezuhalten und ihn zu definieren. Dieser schon ziemlich alte Begriff stammt aus der Kryptografie. Er kennzeichnet ganz allgemein einen bewusst erstellten Zugriffsmechanismus, der die normalen Sicherheitsmaßnahmen eines Computersystems umgeht. Hintertüren sind meistens geheim und werden ohne Ihr Wissen und ohne Ihre Zustimmung hinzugefügt, aber das muss nicht unbedingt so sein. Wenn das FBI Apple auffordert, eine Möglichkeit bereitzustellen, die Verschlüsselung eines iPhones zu umgehen, verlangt die Behörde nach einer Hintertür. Wenn Forscher in einer Firewall von Fortinet ein fest einprogrammiertes zusätzliches Kennwort entdecken, dann haben sie eine Hintertür gefunden. Und wenn das chinesische Unternehmen Huawei in seinen Internetroutern einen geheimen Zugriffsmechanismus einrichtet, dann hat es eine Hintertür installiert. Mehr zu diesem Thema in Kapitel 11.

Alle Computer können mit Schadsoftware infiziert werden. Alle Computer können durch Ransomware (Erpressungssoftware) unter fremde Kontrolle geraten. Alle Computer können zur Teilnahme an einem Botnet – einem Netzwerk, das aus mit Schadsoftware infizierten Rechnern besteht und ferngesteuert wird – gezwungen werden. Die Daten aller Computer können aus der Ferne vollständig gelöscht werden. Die eigentliche Funktion des Embedded-Computers oder die Art des IoT-Geräts spielen keine Rolle. Angreifer können IoT-Geräte auf die gleiche Weise missbrauchen wie schon jetzt Desktop-PCs und Laptops.

Aufgrund ihrer Komplexität sind computerisierte Systeme einfacher anzugreifen als zu schützen

Im Internet sind die Angreifer den Verteidigern gegenüber im Vorteil.

Das muss aber nicht zwangsläufig so sein. Wie die Geschichte zeigt, waren über Zeiträume von Jahrzehnten oder Jahrhunderten mal die Angreifer und mal die Verteidiger im Vorteil. Die Geschichte der Kriegsführung veranschaulicht das sehr schön, denn die verschiedenen Technologien wie Maschinengewehre und Panzer kamen mal der einen, mal der anderen Seite zugute. Doch bei den heutigen Computern und im Internet ist der Angriff einfacher als die Verteidigung – und das wird vermutlich auf absehbare Zeit so bleiben.

Dafür gibt es viele Gründe, entscheidend ist jedoch die Komplexität dieser Systeme. Komplexität ist der ärgste Feind der Sicherheit. Je komplexer ein System ist, desto unsicherer ist es. Und die Milliarden Computer mit jeweils Millionen Codezeilen, die zum Internet zusammengeschlossen sind, das Billionen Webseiten und Zettabytes an Daten enthält, stellen das komplexeste System dar, das die Menschheit je erschaffen hat.

Die erhöhte Komplexität bedeutet mehr beteiligte Menschen, mehr Bestandteile, mehr Interaktionen, mehr Abstraktionsebenen, mehr Fehler beim Design und beim Entwicklungsprozess, mehr Probleme beim Testen und mehr Schlupfwinkel im Code, in denen sich Sicherheitslücken verbergen können.

Computersicherheitsforscher sprechen gern von der »Angriffsfläche« eines Systems. Damit sind alle Schwachstellen gemeint, die ein Angreifer ins Visier nehmen könnte und die geschützt werden müssen. Mit einem komplexen System geht eine große Angriffsfläche einher, und das ist ein

großer Vorteil für einen potenziellen Angreifer. Der Angreifer muss nur eine der Sicherheitslücken aufspüren – eine Schwachstelle, die einen Angriff ermöglicht – und dann den Zeitpunkt und die Angriffsmethode auswählen. Diese Angriffe kann er fortsetzen, bis er damit Erfolg hat. Der Verteidiger hingegen muss ständig die gesamte Angriffsfläche gegen alle möglichen Angriffe abschotten. Er muss jedes Mal die Oberhand behalten, während der Angreifer nur ein einziges Mal Glück haben muss. Es handelt sich schlicht und einfach um einen ungleichen Kampf. Der Aufwand, ein System anzugreifen, beträgt nur einen Bruchteil des Aufwands, der erforderlich ist, um es zu verteidigen.

Komplexität ist einer der wesentlichen Gründe, weshalb Computersicherheit immer noch ein Problem darstellt, obwohl die Sicherheitstechnologien ständig verbessert werden. Jedes Jahr werden neue Ideen entwickelt, neue Forschungsergebnisse vorgelegt sowie neue Produkte und Dienste vorgestellt. Gleichzeitig nimmt jedoch auch die Komplexität jedes Jahr zu, was zu neuen Sicherheitslücken und Angriffsmöglichkeiten führt. Wir geraten ins Hintertreffen, obwohl wir uns verbessern.

Die Komplexität bewirkt auch, dass die Anwender die Sicherheit oft nicht richtig handhaben. Komplexe Systeme bieten in der Regel sehr vielfältige Möglichkeiten, was es erschwert, sie auf sichere Weise zu verwenden. Die Anwender vergessen häufig, Standardkennwörter zu ändern, oder sie konfigurieren die Zugriffsrechte für die in der Cloud befindlichen Daten falsch. 2017 gab die Stanford University »fehlkonfigurierte Zugriffsrechte« als Grund dafür an, dass die Daten von Tausenden von Studenten und Mitarbeitern öffentlich zugänglich waren. Vorfälle dieser Art treten ständig auf.

Neben der Komplexität gibt es weitere Gründe dafür, dass ein Angriff einfacher ist als die Verteidigung. Angreifer haben den Vorteil, als Erste am Zug zu sein. Hinzu kommt, dass sie naturgemäß über eine hohe Beweglichkeit verfügen, die den Verteidigern oft fehlt. Für gewöhnlich pfeifen sie auf gesetzliche Vorschriften oder moralische bzw. ethische Grundsätze und können technische Neuerungen schneller einsetzen. In Sachen proaktiver Sicherheit sieht es hingegen düster aus, da es an Anreizen fehlt, Verbesserungen vorzunehmen. Wir treffen nur selten Sicherheitsvorkehrungen, bevor ein Angriff stattfindet. Zudem winkt den Angreifern bei Erfolg ein Gewinn, während die Verteidigung typischerweise lediglich einen Kostenfaktor darstellt, den die Unternehmen zu minimieren versuchen – und viele

Führungskräfte glauben noch immer nicht, dass ihr Unternehmen ein Ziel darstellt. Die Vorteile des Angreifers überwiegen also deutlich.

Das heißt aber nicht, dass es sinnlos ist, sich zu schützen, sondern nur, dass es schwierig und kostspielig ist. Wenn der Angreifer ein krimineller Einzeltäter ist, fällt es natürlich leichter, ihn dazu zu bringen, sich ein einfacheres Angriffsziel zu suchen. Aber ein entsprechend ausgebildeter, finanziell unterstützter und motivierter Angreifer wird früher oder später immer Erfolg haben. Chris Inglis, der ehemalige stellvertretende Direktor der NSA, äußerte sich zum Thema nationalstaatliche Cyberoperationen folgendermaßen: »Wenn es bei Cyberangriffen einen Spielstand wie beim Fußball gäbe, würde es 20 Minuten nach dem Anpfiff 462:456 für die Angreifer stehen.« Das kommt ungefähr hin.

Aber dass eine Angriffsmethode technisch unkompliziert ist, bedeutet nicht, dass sie weit verbreitet ist. Jemanden zu ermorden, ist auch nicht besonders schwierig, dennoch gibt es nur wenige Mörder, weil alle Gesellschaftsformen Mörder ausfindig machen, verurteilen und strafrechtlich verfolgen. Im Internet ist eine strafrechtliche Verfolgung allerdings nicht so einfach, weil es schwierig ist, Angreifer zu identifizieren – ein Thema, mit dem wir uns in Kapitel 3 befassen werden – und weil grenzüberschreitende Internetangriffe komplizierte Probleme hinsichtlich der gerichtlichen Zuständigkeiten mit sich bringen.

Das Internet+ wird diese Entwicklung noch verschärfen. Mehr Computer, insbesondere mehrere verschiedene Arten von Computern, bedeuten mehr Komplexität.

Interkonnektivität schafft neue Sicherheitslücken

Das Internet bringt immer wieder neuartige Eigenschaften hervor, die manchmal zu ungewollten Folgeerscheinungen führen. Tatsächlich verstehen selbst wir Experten das Zusammenwirken der verschiedenen Teile des Internets nicht so genau, wie wir vielleicht denken, und sind immer wieder überrascht, wenn wir erfahren, wie manche Dinge funktionieren. Das trifft auch auf Sicherheitslücken zu.

Durch die zunehmende Vernetzung haben immer mehr Sicherheitslücken in einem System Auswirkungen auf andere Systeme. Hier sind drei Beispiele:

- 2013 hackten sich Kriminelle in das Netzwerk der Target Corporation und stahlen die Daten von 70 Millionen Kunden und 40 Millionen Kreditkartendaten. Die Kriminellen erlangten Zugang zu Targets Netzwerk, weil sie zunächst die Anmeldedaten von einem Heizungs- und Klimaanlagenlieferanten des Unternehmens erbeuten konnten.
- 2016 schlossen Hacker Millionen IoT-Geräte – Router, digitale Videorekorder, Webcams usw. – zu einem gewaltigen Botnet namens Mirai zusammen. Dieses Botnet benutzten sie, um einen DDoS-Angriff (Distributed Denial of Service, verbreitete Verweigerung des Dienstes) auf den Domain-Provider Dyn zu starten. Dyn stellt für viele bedeutende Sites im Internet betriebsnotwendige Funktionen bereit. Als Dyn nicht mehr erreichbar war, gingen Dutzende beliebter Websites wie Reddit, BBC, Yelp, PayPal und Etsy ebenfalls offline.
- 2017 drangen Hacker über ein mit dem Internet verbundenes Aquarium in das Netzwerk eines Casinos (dessen Name nicht genannt wurde) ein und stahlen Daten.

Systeme können andere Systeme auf unvorhersehbare, potenziell gefährliche Weise beeinflussen. Was dem Designer eines bestimmten Systems völlig harmlos erscheint, kann zu einer Gefahr werden, wenn es mit einem anderen System verbunden wird. Schwachstellen des einen Systems können sich auf andere Systeme ausbreiten, und das hat Sicherheitslücken zur Folge, mit denen niemand gerechnet hat. Dadurch waren auch Katastrophen wie der Reaktorunfall im Kernkraftwerk Three Mile Island, die Explosion des Spaceshuttles Challenger oder der Stromausfall im Jahr 2003 in den USA und Kanada möglich.

Unbeabsichtigte Effekte wie diese rücken zwei Aspekte in den Blick: Zum einen ist es durch die Interkonnektivität schwierig, herauszufinden, in welchem System der Fehler liegt. Zum anderen ist es durchaus möglich, dass nicht eines der Systeme allein für den Fehler verantwortlich ist. Die Ursache könnte ein unsicheres Zusammenwirken zweier Systeme sein, die für sich genommen sicher sind. 2012 kompromittierte ein Unbekannter den Amazon-Account des Journalisten Mat Honan. Dadurch konnte er auf Honans Apple-Account zugreifen, was ihm auch Zugriff auf dessen Gmail-Account verschaffte, was ihm wiederum die Übernahme seines Twitter-Accounts ermöglichte. Der genaue Ablauf des Angriffs ist hier von Bedeutung, denn einige der Sicherheitslücken waren nicht Teil der einzelnen Sys-

teme, sondern ließen sich nur in Verbindung mit den anderen Systemen ausnutzen.

Es gibt weitere Beispiele. Eine Sicherheitslücke in einem smarten Kühlschrank von Samsung setzte die User von Gmail-Accounts der Gefahr eines Angriffs aus. Das Gyroskop in einem iPhone, das dazu dient, Bewegungen und die Orientierung im Raum zu messen, ist so empfindlich, dass es akustische Schwingungen erfassen und so Gespräche belauschen kann. Die Antivirus-Software von Kaspersky hat versehentlich (oder absichtlich) geheime Informationen der US-Regierung an den Hersteller übermittelt.

Wenn 100 Systeme miteinander interagieren, entspricht das rund 5.000 Interaktionen und 5.000 potenziellen Sicherheitslücken, die sich durch diese Interaktionen ergeben. Bei 300 Systemen sind es schon etwa 45.000 und bei 1.000 Systemen circa eine halbe Millionen Interaktionen. Die meisten davon sind harmlos oder nicht beachtenswert, aber einige werden äußerst verheerende Folgen haben.

Computer sind auf besondere Weise gefährdet

Computer sind nicht auf die gleiche Weise wie »normale« Geräte von Sicherheitsrisiken betroffen. Sie sind auf dreierlei Weise gefährdet.

Erstens: Entfernung spielt keine Rolle. Im wahren Leben machen wir uns Sorgen, dass wir einem mittelmäßigen Angreifer zum Opfer fallen. Wir kaufen kein Türschloss, um uns vor dem besten Einbrecher der Welt zu schützen, sondern um die durchschnittlichen Einbrecher, die sich vermutlich in der Nachbarschaft herumtreiben, fernzuhalten. Mein Haus befindet sich in Cambridge, und wenn es in Canberra eine supertalentierte Einbrecherin gibt, ist mir das egal. Sie wird wohl kaum um die halbe Welt fliegen, um mein Haus auszuplündern. Im Internet jedoch kann eine Hackerin in Canberra mein Heimnetzwerk genauso leicht hacken wie ein Netzwerk im Nachbarhaus.

Zweitens: Die Möglichkeit, Computer anzugreifen, ist entkoppelt von den technischen Fähigkeiten, die dafür nötig sind. Denn Software kann technische Fähigkeiten miteinschließen. So kann beispielsweise die supertalentierte Hackerin in Canberra ihre Expertise in Software einbetten. Sie kann den Angriff automatisieren und ihn ausführen lassen, während sie schläft. Anschließend kann sie die Software an beliebige Personen rund um den Globus weitergeben. Auf diese Weise entstand der Begriff »Script-

kiddie«: Dabei handelt es sich um eine Person mit minimalen Fachkenntnissen, die aber über leistungsstarke Software verfügt. Wenn der beste Einbrecher der Welt ungehindert ein Tool verbreiten könnte, das es mittelmäßigen Einbrechern ermöglicht, in Ihr Haus einzusteigen, würden Sie sich wohl mehr Gedanken über Einbruchschutz machen.

Die freie Verbreitung potenziell gefährlicher Hackertools ist im Internet gang und gäbe. Die Angreifer, die das Mirai-Botnet eingerichtet haben, veröffentlichten ihren Code, und innerhalb weniger Wochen war er in einem Dutzend Angreifertools integriert. Hierbei handelt es sich um ein Beispiel für das, was wir als »Schadsoftware« oder »Malware« bezeichnen: Würmer, Viren und Rootkits, die auch unbegabten Angreifern enorme Möglichkeiten bieten. Hacker können auf dem Schwarzmarkt Rootkits erwerben oder Ransomware als Dienstleistung (»Ransomware as a Service«) einkaufen. Europäische Unternehmen wie HackingTeam oder Gamma Group verkaufen Angreifertools an die Regierungen kleinerer Länder rund um den Globus. Der Inlandsgeheimdienst der Russischen Föderation FSB ließ einen 21-jährigen kasachisch-kanadischen Bürger namens Karim Baratov einen Phishing-Angriff ausführen, der 2016 zum erfolgreichen Hack der nationalen Organisation der Demokratischen Partei der USA (Democratic National Committee, DNC) führte. Erstellt wurde die Schadsoftware von dem talentierten Hacker Alexsey Belan.

Drittens: Alle Computer sind gleichzeitig betroffen – oder eben gar keiner. Der sogenannte »Class Break« ist ein Konzept aus der Computersicherheit. Dabei wird eine spezielle Art von Sicherheitslücke ausgenutzt, die nicht nur ein System kompromittiert, sondern eine ganze Reihe von gleichen Systemen. Denken Sie beispielsweise an eine Sicherheitslücke in einem Betriebssystem, die es einem Angreifer ermöglicht, aus der Ferne die Kontrolle über alle Systeme zu übernehmen, auf denen dieses Betriebssystem läuft, oder an eine Sicherheitslücke bei mit dem Internet verbundenen digitalen Videorekordern und Webcams, die es dem Angreifer erlaubt, diese Geräte in ein Botnet einzubinden.

Der elektronische Personalausweis in Estland fiel 2017 solch einem Class Break zum Opfer. Aufgrund einer kryptografischen Schwachstelle war die estnische Regierung gezwungen, die Gültigkeit von 760.000 Personalausweisen zeitweise außer Kraft zu setzen, die für alle möglichen staatlichen Dienstleistungen eingesetzt wurden, von denen einige Hochsicherheitsbereiche betrafen.

Die Risiken werden durch die Software- und Hardware-Monokultur weiter verschärft. Wir verwenden fast ausnahmslos eins der drei »großen« Computerbetriebssysteme oder eins der beiden gängigsten Betriebssysteme für Smartphones bzw. Tablets. Mehr als die Hälfte von uns verwendet den Webbrowser Chrome, die übrigen einen der fünf anderen. Zur Textverarbeitung und für Tabellenkalkulationen verwenden die meisten von uns Microsoft Word bzw. Excel. Und praktisch jeder liest PDFs, betrachtet JPEGs, hört MP3-Dateien und sieht sich AVI-Videos an. Fast alle Geräte rund um den Globus kommunizieren über das Internetprotokoll TCP/IP. Standards wie diese sind aber nicht die einzige Ursache für Monokulturen. Laut einer Studie des US-Ministeriums für Innere Sicherheit aus dem Jahr 2011 ist GPS für elf von 15 kritischen Infrastrukturbereichen unverzichtbar. Ein Class Break des GPS und zahlreicher anderer Funktionen und Protokolle würde Millionen Geräte und Anwender betreffen. Noch ist das Internet of Things vielfältiger, das wird jedoch nicht so bleiben, wenn nicht ein paar ziemlich grundlegende wirtschaftliche Richtlinien geändert werden. Zukünftig wird es nur einige wenige IoT-Prozessoren, Betriebssysteme, Controller und Kommunikationsprotokolle geben.

Ein Class Break mündet in Würmern, Viren und anderer Schadsoftware. Das Motto lautet: »Nur einmal angreifen, aber viele treffen.« Bislang haben wir uns Wahlbetrug so vorgestellt, dass unberechtigte Personen versuchen zu wählen, und nicht als Manipulation von Onlinewahllisten oder mit dem Internet verbundenen Wahlmaschinen durch eine einzelne Person oder Organisation. Aber genau das gefährdet Computersysteme: Jemand hackt die Maschinen.

Stellen Sie sich einen Taschendieb vor, der seine Fähigkeiten lange trainiert hat. Jedes Opfer ist eine neue Herausforderung und ein erfolgreicher Diebstahl garantiert nicht, dass der nächste Versuch ebenfalls erfolgreich sein wird. Vergleichen Sie das mit elektronischen Türschlössern, wie man sie in vielen Hotelzimmern findet. Sie weisen verschiedene Schwachstellen auf. Ein Hacker könnte einen Fehler im Design entdecken, der es ihm ermöglicht, eine Schlüsselkarte zu erstellen, mit der sich jede Tür öffnen lässt. Wenn er seine Software veröffentlicht, kann nicht nur der Hacker selbst, sondern jede beliebige Person sämtliche Schlösser öffnen. Und wenn diese Schlösser mit dem Internet verbunden sind, könnten Angreifer die Türschlösser auch aus der Ferne öffnen – sogar alle gleichzeitig. Hierbei handelt es sich um einen Class Break.

2012 ist genau das Onity widerfahren, einem Unternehmen, das elektronische Schlösser herstellt, die in mehr als vier Millionen Zimmertüren von Hotelketten wie Marriott, Hilton oder InterContinental verbaut sind. Ein selbst gebautes Gerät ermöglichte es Hackern, die Schlösser in wenigen Sekunden zu öffnen. Irgendjemand hatte sich das ausgedacht, und die Bauanleitung für das Gerät verbreitete sich in Windeseile. Es dauerte Monate, bis Onity bemerkte, dass sie gehackt worden waren. Und weil es keine Möglichkeit gab, das System zu patchen (mehr dazu in Kapitel 2), waren die Hotelzimmer monate- oder sogar jahrelang gefährdet.

Für das Risikomanagement ist Class Break ein alter Hut. Die Problematik ist vergleichbar mit dem Unterschied zwischen Einbrüchen und Bränden einerseits, von denen einzelne Häuser in einer bestimmten Gegend im Laufe eines Jahres gelegentlich betroffen sind, und Überschwemmungen und Erdbeben andererseits, die entweder alle oder niemanden in einem bestimmten Gebiet treffen. Für Computer gilt nicht nur beides gleichzeitig, sie sind auch von Aspekten des Risikomodells für das Gesundheitswesen betroffen.

Die Art und Weise, wie Computer gefährdet sind, hat Auswirkungen auf das Wesen der Sicherheitsprobleme und stellt die Methoden, mit denen wir uns dagegen wehren müssen, völlig auf den Kopf. Die von einem durchschnittlichen Angreifer ausgehende Bedrohung bereitet uns kein Kopfzerbrechen. Sorgen machen müssen wir uns um extremistische Einzeltäter, die alle mit in den Abgrund reißen können.

Die Angriffe werden immer besser, schneller und einfacher

Der Verschlüsselungsalgorithmus DES (Data Encryption Standard) stammt aus den 1970er-Jahren. Im Hinblick auf die Sicherheit war DES bewusst so ausgelegt, dass es den damals machbaren Angriffen gerade so standhielt. 1976 schätzen Kryptografieexperten, dass es 20 Millionen Dollar kosten würde, einen Computer zu bauen, der DES knacken könnte. In meinem 1995 erschienenen Buch *Applied Cryptography* (dt. Titel *Angewandte Kryptographie*) habe ich geschätzt, dass die Kosten auf eine Million Dollar gesunken sind. 1998 hat die Electronic Frontier Foundation (EFF) für 250.000 Dollar einen Rechner gebaut, der die DES-Verschlüsselung in weniger als einem Tag knacken konnte. Heutzutage können Sie das mit Ihrem Laptop erledigen.

In den 1990er-Jahren waren Mobiltelefone dafür ausgelegt, sich ohne irgendeine Authentifizierung automatisch mit Mobilfunkzellen zu verbinden, denn die Authentifizierung war damals schwierig und es war kaum möglich, eine gefälschte Funkzelle zu betreiben. Ein halbes Jahrzehnt später setzte das FBI ein geheimes System namens Stingray ein, um zu Überwachungszwecken Funkzellen zu simulieren. Ein weiteres halbes Jahrzehnt später war es so einfach geworden, Funkzellen nachzubilden, dass Hacker es bei ihren Konferenzen auf der Bühne vorführten.

Auch die zunehmende Geschwindigkeit von Computern hat dazu beigetragen, dass sie beim Knacken von Kennwörtern durch Brute-Force-Attacken (dem Ausprobieren aller möglichen Kennwörter) exponentiell schneller geworden sind. Unterdessen hat sich die Länge und Komplexität der Kennwörter, die ein durchschnittlicher Anwender benutzt und sich merken kann, nicht verändert. Deshalb sind Kennwörter, die vor zehn Jahren noch sicher waren, heutzutage unsicher.

Den folgenden Aphorismus habe ich erstmals von einem NSA-Mitarbeiter gehört: »Angriffe werden immer besser; niemals schlechter.« Angriffe werden schneller, preiswerter und einfacher. Was heute nur theoretisch möglich ist, wird schon morgen in die Tat umgesetzt. Und weil unsere Informationssysteme viel länger als ursprünglich geplant im Einsatz bleiben, müssen wir schon jetzt auch an die Angreifer denken, die die Technologien der Zukunft verwenden.

Die Angreifer lernen ebenfalls dazu und passen sich an. Das unterscheidet die Computersicherheit von den Maßnahmen, mit denen man sich zum Beispiel vor einem Tornado schützt. Tornados stellen eine Bedrohung dar. Wir könnten nun verschiedene Vorsichtsmaßnahmen und deren Wirksamkeit erörtern und uns fragen, ob zukünftige technische Fortschritte uns helfen können, uns besser vor der zerstörerischen Kraft dieser Wirbelstürme zu schützen. Aber was auch immer wir unternehmen oder unterlassen, wir wissen genau, dass Tornados sich nicht an unsere Schutzmaßnahmen anpassen und ihr Verhalten ändern werden. Es sind schließlich nur Tornados.

Menschliche Gegenspieler sind da anders. Sie sind einfallsreich und intelligent. Sie ändern ihre Taktik, erfinden Neues und passen sich kontinuierlich an. Angreifer inspizieren unsere Systeme und suchen nach möglichen Class Breaks. Und sobald jemand eine solche Sicherheitslücke findet, wird sie so lange immer wieder ausgenutzt, bis sie geschlossen wird. Eine

Sicherheitsmaßnahme, die Netzwerke heute noch schützt, könnte schon morgen nicht mehr funktionieren, weil die Angreifer herausgefunden haben, wie sie sich umgehen lässt.

All das hat zur Folge, dass der Wert von Expertenwissen schnell verfällt. Was gestern noch eine streng geheime Fähigkeit des Militärs war, ist heute das Thema einer Doktorarbeit und wird morgen zu den Hackertools gehören. Ein Beispiel dafür ist die differenzielle Kryptoanalyse, die irgendwann vor 1970 von der NSA entdeckt wurde. In den 1970er-Jahren entdeckten Mathematiker bei IBM sie bei der Entwicklung von DES ebenfalls. Die NSA stufte IBMs Entdeckung als geheim ein, aber das Verfahren wurde Ende der 1980er-Jahre ein weiteres Mal von Kryptografen wiederentdeckt.

Die Verteidiger müssen ständig in Bewegung bleiben. Was gestern noch funktionierte, ist vielleicht schon heute unbrauchbar und wird morgen fast mit Sicherheit nutzlos sein.

Stichwortverzeichnis

C

D

E

F

G

H

I

Y

Z