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.