Vorwort

Mit dem bevorstehenden Zeitalter des Internet of Things (IoT) werden die Grenzen zwischen dem physischen und dem virtuellen Leben immer stärker verwischt werden. Angriffe gegen unsere Onlinepräsenzen werden dann auch Risiken für unsere Sicherheit im »wirklichen« Leben darstellen. In der Vergangenheit waren für Angriffe auf unsere Güter physische Handlungen erforderlich, was daran lag, dass der Zugriff auf die betreffende Infrastruktur über das Internet beschränkt war. Dies ändert sich gerade, denn die Zukunft mit Milliarden vernetzter Dinge stellt einen dramatischen Wechsel dar.

Im vorliegenden Buch werden wir einen neugierigen Blick auf die Möglichkeiten des Missbrauchs einiger sehr beliebter IoT-Geräte werfen, die bereits heute erhältlich sind. Wir werden uns ansehen, wie sich mit einem einfachen Angriff gegen LED-Leuchten ein umfassender und anhaltender Stromausfall verursachen lässt, warum physische Sicherheit und Privatsphäre durch falsche Entscheidungen im Sicherheitsbereich erheblich beeinträchtigt sind und inwieweit Ihr Leben durch Sicherheitsmängel bei leistungsfähigen Elektrofahrzeugen gefährdet ist.

Ich möchte mit diesem Buch zeigen, welche spürbaren Risiken durch die IoT-Geräte entstehen, von denen wir in Zukunft immer stärker abhängig sein werden. Wenn wir beginnen, die Ursachen für die Schwachstellen bei bereits erhältlichen Geräten zu verstehen, können wir einen neuen Weg aufzeigen, solche Geräte in Zukunft sicherer zu machen und unser Leben mit ihnen zu bereichern.

Allerdings widmen sich gewiefte Angreifer bereits heute der Entdeckung und Anwendung solcher Schwachstellen, und sie werden auch in Zukunft Mittel und Wege finden, ihr Wissen auf jede nur denkbare Weise zu missbrauchen. Das Spektrum dieser Personen reicht vom neugierigen Oberstufenschüler bis hin zu teils privaten, teils auch staatlich unterstützten Verbrecherbanden, deren Ziel die Terrorisierung Einzelner wie auch ganzer Bevölkerungsgruppen ist. Die Schwachstellen bei IoT-Systemen können die Privatsphäre der Menschen in großem Stile zerstören und auch physische Schäden hervorrufen. Es steht einiges auf dem Spiel.

Zielgruppe

Dieses Buch ist für all jene Leser gedacht, die daran interessiert sind, in den derzeit erhältlichen IoT-Geräten Sicherheitslücken zu entdecken. Hierbei werden Sie mit der Denkweise von Angreifern vertraut gemacht, die ebenfalls eifrig nach Wegen suchen, solche Geräte zu ihrem Vorteil zu nutzen. Indem Sie sich mit den hinterhältigen Taktiken jener beschäftigen, die es auf die Welt des Internet of Things abgesehen haben, erhalten Sie einen umfassenden Einblick in die Vorgehensweise und die Psychologie der Angreifer. Auf diese Weise lernen Sie nicht nur, wie Sie sich schützen können, sondern können auch zur Entwicklung sicherer IoT-Produkte beitragen.

Aufbau

Dieses Buch ist in folgende Kapitel untergliedert:

Kapitel 1: Licht aus! – Angriff auf drahtlose LED-Leuchten

Am Anfang dieses Buches steht eine umfassende Abhandlung zu Aufbau und Architektur eines der beliebtesten IoT-Produkte, die derzeit auf dem Markt erhältlich sind: das Beleuchtungssystem Philips Hue (http://meethue.com). In diesem Kapitel schildern wir verschiedene Schwachstellen des Systems. Hierzu gehören grundlegende Aspekte wie die Passwortsicherheit und die Möglichkeit, mithilfe von Malware schwache Autorisierungsmechanismen zu umgehen und auf diese Weise dauerhafte Ausfälle zu verursachen. Ferner werden wir über die Komplexität der Vernetzung unserer Onlineprofile (z.B. auf Facebook) mit IoT-Geräten sprechen, denn hierdurch können plattformübergreifende Sicherheitslücken entstehen.

Kapitel 2: Wie man sich elektronisch Zutritt verschafft –Türschlösser manipulieren

In diesem Kapitel werfen wir einen Blick auf Sicherheitslücken bei marktüblichen elektronischen Türsperren, ihre Funkmechanismen und die Integration mit Mobilgeräten. Außerdem präsentieren wir aktuelle Fallstudien von Angreifern, die diese Lücken ausgenutzt haben, um Einbrüche zu begehen.

Kapitel 3: Funkverkehr im Fadenkreuz – Babyfone und andere Geräte kapern

Sicherheitsmängel bei ferngesteuerten Babyfonen sind Gegenstand dieses Kapitels. Wir werden uns echte Schwachstellen, die von Angreifern tatsächlich genutzt wurden, genauer ansehen und feststellen, wie einfache Konstruktionsfehler die ganze Familie unnötig in Gefahr bringen.

Kapitel 4: Verschwommene Grenzen – wo physischer und virtueller Raum sich treffen

Unternehmen wie SmartThings bieten zahlreiche IoT-Geräte und Sensoren zum Schutz der eigenen Wohnung an. So können Sie beispielsweise eine Benachrichtigung erhalten, wenn Ihre Haustüre nach Mitternacht geöffnet wird. Die Tatsache, dass solche Geräte für ihren Betrieb auf das Internet angewiesen sind, hat unsere Abhängigkeit von Netzwerkverbindungen erhöht – die Grenzen zwischen physischer Welt und Cyberspace verschwimmen. In diesem Kapitel sehen wir uns an, wie es um die Sicherheit von SmartThings-Produkten bestellt ist und wie sich mit ihrer Hilfe Geräte anderer Hersteller sicher bedienen lassen.

Kapitel 5: Angriff auf die Mattscheibe – über die Anfälligkeit von Smart-TVs

Moderne Fernsehgeräte sind im Grunde genommen nichts anderes als Computer mit leistungsfähigen Betriebssystemen wie Linux. Sie verbinden sich mit dem heimischen WLAN und unterstützen Dienste wie etwa Videostreams, Videokonferenzen, soziale Netzwerke und Instant Messaging. In diesem Kapitel widmen wir uns den Sicherheitslücken am Beispiel von Samsung-Fernsehgeräten, um die Hauptursachen von Schwachstellen und mögliche Auswirkungen auf Datenschutz und persönliche Sicherheit zu identifizieren.

Kapitel 6: Strom statt Benzin – Sicherheitsanalyse von vernetzten Fahrzeugen

Auch Autos sind »Dinge«, die heutzutage der Fernkommunikation und Fernsteuerung offenstehen. Anders als bei vielen anderen Geräten kann die Vernetzung des Autos wichtige Sicherheitsfunktionen erfüllen; Sicherheitslücken in Fahrzeugen hingegen können lebensgefährlich sein. In diesem Kapitel lernen wir ein drahtloses System mit geringer Reichweite kennen und beurteilen umfangreiche Forschungen führender Fachexperten. Schließlich analysieren und bewerten wir Funktionen der Model-S-Limousine von Tesla sowie mögliche Verbesserungspotenziale in Sachen Sicherheit bei diesem Fahrzeugtyp.

Kapitel 7: Sicheres Prototyping – littleBits und cloudBit

Beim Entwerfen eines IoT-Produkts besteht der erste wichtige Schritt darin, einen Prototyp zu erstellen. Auf diese Weise soll sichergestellt werden, dass die Idee konzeptionell umgesetzt werden kann, alternative Entwurfskonzepte untersucht werden können und Spezifikationen ermittelt werden, um eine belastbare Geschäftsentscheidung finden zu können. Extrem wichtig ist dabei die Implementierung von Sicherheitsfunktionen bereits im ersten Prototyp und in allen nachfolgenden Varianten bis hin zum finalen Produkt. Macht man sich über Sicherheit erst dann Gedanken, wenn das Produkt fertig ist, dann geht man in puncto Verbrauchersicherheit und Datenschutz ein hohes Risiko ein. In diesem Kapitel erstellen wir einen Prototyp für eine Türklingel mit SMS-Funktionalität mithilfe der Proto-

typentwicklungsplattform littleBits. Dabei hilft uns das cloudBit-Modul dabei, Fernsteuerungsmöglichkeiten per Funk einzubauen. Am Ende steht der Prototyp eines IoT-Konzepts für eine Türklingel, bei deren Betätigung eine SMS an den Benutzer versandt wird. Die Beschreibung der Schritte bei der Prototypentwicklung berücksichtigt auch Sicherheitsfragen und -anforderungen ebenso wie wichtige Sicherheitsaspekte, die von Produktentwicklern zu beachten sind.

Kapitel 8: Zukunftssicherheit – ein Dialog über künftige Angriffsvarianten

Im Laufe der kommenden Jahre wird unsere Abhängigkeit von IoT-Geräten einen massiven Höhenflug erleben. In diesem Kapitel skizzieren wir realistische Szenarios für Angriffe, die wir für die Zukunft erwarten.

Kapitel 9: Zwei Szenarios – Absichten und ihre Folgen

In diesem Kapitel betrachten wir zwei verschiedene hypothetische Szenarios, um darauf basierend einschätzen zu können, inwieweit Menschen sicherheitsrelevante Vorfälle beeinflussen können. Zunächst untersuchen wir den Versuch eines leitenden Mitarbeiters in einem großen Unternehmen, mithilfe von »Buzzwords« aus dem Bereich der IoT-Sicherheit den Unternehmensvorstand zu beeindrucken. Im zweiten Szenario sehen wir uns an, wie ein aufstrebender IoT-Provider mit Forschern und Journalisten zu interagieren versucht, um die Integrität seines Unternehmens aufrechtzuerhalten. Das Kapitel soll vor allem veranschaulichen, dass die Auswirkungen sicherheitsrelevanter Szenarios auch und gerade von den Absichten und Handlungen der beteiligten Personen beeinflusst werden.