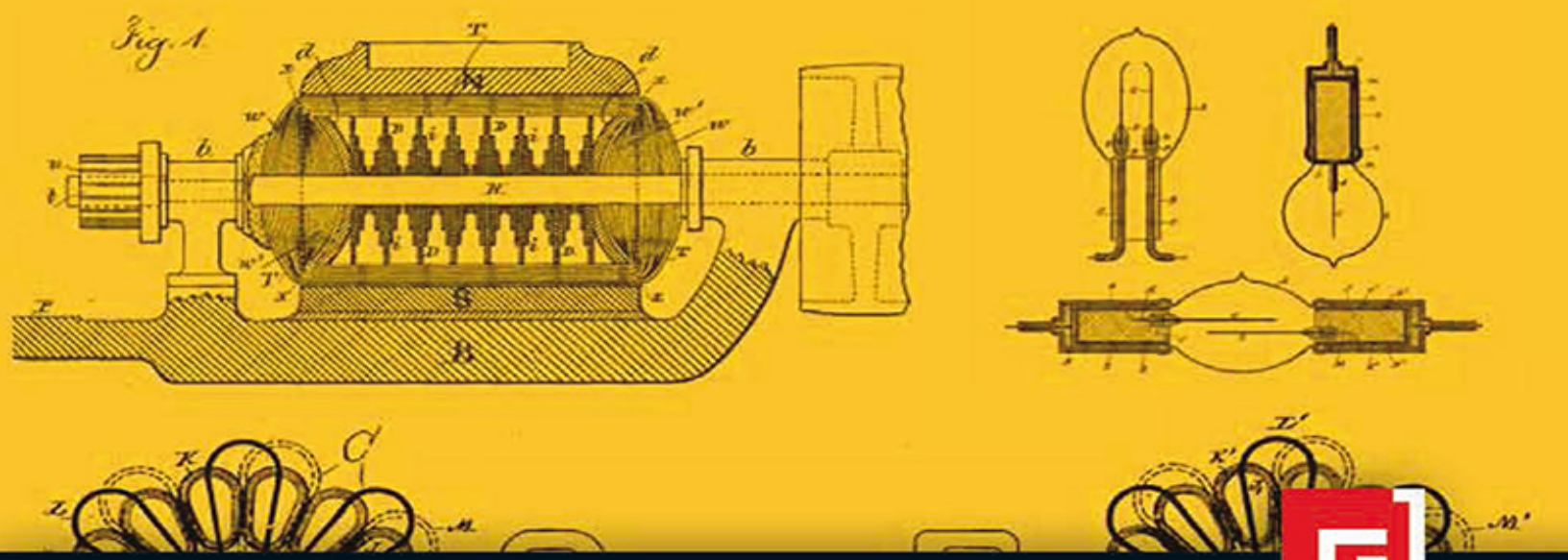

Nitesh Dhanjani

IoT-Hacking

Sicherheitslücken im Internet der Dinge erkennen und schließen

dpunkt.verlag

Nitesh Dhanjani ist bekannt als Forscher, Autor und Redner aus dem Security-Bereich. Er hat unter anderem die Bücher *Hacking: The Next Generation* (O'Reilly), *Network Security Tools* (O'Reilly) und *HackNotes: Linux and Unix Security* (Osborne McGraw-Hill) verfasst. Über seine Arbeit wurde in den Medien bereits ausführlich berichtet, so etwa bei CNN, Reuters, MSNBC und Forbes.

IoT-Hacking

Sicherheitslücken im Internet der Dinge erkennen und schließen

Nitesh Dhanjani

Lektorat: René Schönfeldt
Übersetzung: Christian Alkemper, Rheinstetten
Copy-Editing: Ursula Zimpfer, Herrenberg
Satz: Nadine Thiele
Herstellung: Susanne Bröckelmann
Umschlaggestaltung: Helmut Kraus, www.exclam.de
Druck und Bindung: M.P. Media-Print Informationstechnologie GmbH, 33100 Paderborn

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN:
Buch 978-3-86490-343-4
PDF 978-3-86491-927-5
ePub 978-3-86491-928-2
mobi 978-3-86491-929-9

Wieblinger Weg 17
69123 Heidelberg

Authorized German translation of the English edition of Abusing the Internet of Things
ISBN 9781491902332 © 2015 Nitesh Dhanjani

5 4 3 2 1 0

Leserstimmen zur englischen Originalausgabe

»Nitesh Dhanjani präsentiert das IoT-Sicherheitsparadox in knappen Beispielen, die dem Leser die realistischen Probleme vernetzter Geräte und die damit verbundenen Herausforderungen eindrucksvoll veranschaulichen.« – *Brian Hanson, Führungskraft im Sicherheitsbereich*

»Dieses Buch enthüllt Sicherheitslücken, mit denen schon in naher Zukunft Milliarden vernetzter Geräte infiziert sein werden. Es bietet praktische Anleitungen zur Bewältigung aufkommender Sicherheitsrisiken für Verbraucher, Entwickler und Studierende gleichermaßen.« – *Prof. em. Elias Houstis, Purdue University und Universität Thessalien (Griechenland)*

»In seiner gesamten Laufbahn hat sich Dhanjani hervorgetan, indem er stets an vorderster Front stand, wenn es um technisch anspruchsvolle Entwicklungen in der Informationssicherheit und deren Auswirkungen auf Unternehmen und Verbraucher ging. In seinem Buch präsentiert er eindrucksvoll mögliche Auswirkungen unzureichender Sicherheitsfunktionen auf die Gesellschaft, sofern die Risiken nicht vom ersten Moment an berücksichtigt werden.« – *Lee J. Kushner, President LJ Kushner & Associates*

»Angriffe gegen das Internet of Things werden die Schlagzeilen in den kommenden Jahren beherrschen. Einige dieser Angriffe werden in den Medien vollkommen übertrieben dargestellt werden, andere hingegen sehr viel schlimmer sein, als die Leute glauben wollen. Dieses Buch ist ein absolut sachlicher Einstieg in eine Welt, in der Menschen IoT-Profile erstellen und die Geräte dann angreifen.« – *Haroon Meer, Gründer von Thinkst Applied Research*

»Während sich die Gesellschaft noch über die Auswirkungen der Verbreitung von vernetzten Geräten austauscht, präsentiert uns Nitesh Dhanjani Beispiele aus dem echten Leben für die Herausforderungen, denen wir in der Welt solcher Geräte begegnen werden. Ein ernüchternder Ausblick auf das, was uns bevorsteht, und auf die Geräte, von denen wir über kurz oder lang abhängig sein werden.« – *Billy Rios, Gründer von Whitescope.io*

»In diesem Buch vermittelt uns Nitesh Dhanjani auf sehr detaillierte Weise, wie Angriffe gegen das Internet of Things ausgeführt werden können. Er zeigt uns, warum wir die Fehler der Vergangenheit vermeiden müssen. Da IoT-Geräte mit der physischen Welt verbunden sind, können die Auswirkungen von Sicherheitslücken gigantisch sein.« – *Gustavo Rodriguez-Rivera, Weiterbildungsdozent am Computer Science Department der Purdue University*

»[Dieses Buch] ist ein hervorragender Ausgangspunkt für alle, die sich für Bedrohungen und Angriffe auf vernetzte Geräte der nächsten Generation interessieren. Dhanjani beschreibt eine Vielzahl von Anwendungen – von der Möglichkeit, mit ›intelligenten‹ Beleuchtungssystemen einen Stromausfall zu verursachen, bis hin zum Aufspüren und Entsperren eines Elektroautos von Tesla. Dabei kommen zum Teil auch Tricks und Techniken zum Einsatz, die schon in den Neunzigern bekannt waren. Dhanjani erweist sich in seinem gesamten Buch als Meister darin, sowohl grundsätzliche Konstruktionsfehler als auch Mängel bei der konkreten technischen Implementierung auf ebenso einfache wie klare Weise zu erläutern. Für mich ist das Werk aufs Neue eine Bestätigung eines der aus meiner Sicht wichtigsten Grundsätze aus der Informationssicherheit: Je mehr sich ändert, desto weniger ändert sich.« – *Saumil Shah, CEO von Net-Square*

Geleitwort

Als ich erfuhr, dass mein Freund Nitesh Dhanjani ein Buch über das Internet of Things (IoT) verfasst, war ich überaus erfreut. Schließlich ist dies ein Fachgebiet, das zumindest für mich gleichermaßen aufregende wie erschreckende Aspekte aufweist.

Wir hören heutzutage in den Nachrichten Tag für Tag von Hackern, die Sicherheitsfunktionen erfolgreich überwunden haben. Aufgrund der Häufigkeit und des Ausmaßes solcher Vorfälle sind wir mittlerweile ein wenig abgestumpft. Moderne Gesellschaften wie die unsere haben mittlerweile erkannt, dass der Nutzen, den wir durch die Akzeptanz innovativer Technologien erhalten, deren Kosten und Risiken – zumindest kurzfristig – übersteigen. Unser kollektives Versagen dabei, dieses Unsicherheitsmuster endlich wirkungsvoll in Angriff zu nehmen, sollte Beweis genug dafür sein, dass wir den Nutzen höher bewerten als die Risiken.

Ein wesentlicher Aspekt dieser Nutzen-Risiko-Analyse ist die Tatsache, dass die Risiken, die in der Vergangenheit aufgetreten sind, vor allem immaterielle Güter betreffen: Daten und Geld.

Stellen wir uns aber nun einmal vor, welche Auswirkungen es hätte, wenn die Risiken physisch erfahrbar würden: Städte liegen tagelang im Dunkeln, medizinische Geräte töten Patienten, in Kühlschränken verdirbt das Essen, Fahrer verlieren die Kontrolle über ihre Autos, Flugzeuge fallen vom Himmel usw. Ob wir in solchen Fällen weiterhin so tolerant gegenüber technischen Ausfällen bleiben würden, darf bezweifelt werden.

Ich nehme an, dass unser Konzept des Begriffs »Risiko« den Schwerpunkt vor allem auf physische Auswirkungen legt und abstrakte Risiken eher vernachlässigt. Dies ist vielleicht einer der Gründe dafür, dass Risiken im Bereich der Informationssicherheit für viele Menschen schwer zu erfassen sind. Ferner gehe ich davon aus, dass, sobald Vorfälle in diesem Bereich auch physische Konsequenzen haben, wir die Risiken des Internet of Things gewiss überdenken werden.

In der »realen« Welt gibt es zahlreiche Bauvorschriften, die Anforderungen an physische Infrastrukturen definieren, und ihre Einhaltung wird von zertifizierten Technikern oder diplomierten Ingenieuren streng überwacht. Wann endlich werden wir uns Gedanken darüber machen, was Sicherheit in einer Welt bedeutet, in der Millionen und Abermillionen vernetzter Geräte vorhanden sind?

Ich kann nur hoffen, dass die Leser dieses Buches erkennen, dass die technologischen Investitionszyklen, die heute eine fortlaufende Innovation gewährleisten sollen, in Bezug auf IoT-Geräte überdacht werden müssen. Wenn wir die aktuellen Entwicklungs- und Qualitätssteuerungsprozesse, die vor allem auf schnelle Innovation, niedrige Kosten und kurze Produktlebenszyklen ausgelegt sind, auf das Internet of Things anwenden, werden Sicherheit und Datenschutz zweifellos noch stärker unter die Räder kommen.

Patrick Heim

Mit über 20 Jahren Erfahrung ist Patrick Heim ein Veteran der Informationssicherheit.

Er hat bereits eine Vielzahl unterschiedlicher Positionen in den Bereichen Auditing, Consulting und Penetration Testing sowie als Chief Trust Officer und Chief Information Security Officer bekleidet.

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 IoTGeräte 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 IoTGeräten 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 Prototypentwicklungsplattform 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.

Inhaltsverzeichnis

1 Licht aus! – Angriff auf drahtlose LED-Leuchten

1.1 Warum Hue?

1.2 Leuchten über die Website-Oberfläche steuern

1.3 Beleuchtungsregelung mit der iOS-App

1.4 Den Zustand von Leuchtkörpern ändern

1.5 IFTTT

1.6 Fazit

2 Wie man sich elektronisch Zutritt verschafft – Türschlösser manipulieren

2.1 Hoteltürschlösser und Magnetkarten

2.2 Z-Wave-fähige Türschlösser

2.3 Bluetooth Low Energy oder: Wie sich Türen mit Mobile-Apps öffnen lassen

2.4 Fazit

3 Funkverkehr im Fadenkreuz – Babyfone und andere Geräte kapern

3.1 Der Fall Foscam

3.2 Das Belkin-WeMo-Babyfon

3.3 WeMo Switch oder: Manche Dinge ändern sich nie

3.4 Fazit

4 Verschwommene Grenzen – wo physischer und virtueller Raum sich treffen

4.1 SmartThings

4.2 Noch mehr Unsicherheit durch Interoperabilität

4.3 Fazit

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

5.1 Die TOCTTOU-Attacke
5.2 Das nennen Sie Verschlüsselung?
5.3 Apps verstehen und missbrauchen
5.4 So überprüfen Sie Ihr eigenes Smart-TV (und andere IoT-Geräte)
5.5 Fazit

6 Strom statt Benzin – Sicherheitsanalyse von vernetzten Fahrzeugen

6.1 Das Reifendruckkontrollsystem (RDKS)
6.2 Funkkonnektivität ausnutzen
6.3 Das Tesla Model S
6.4 Fazit

7 Sicheres Prototyping – littleBits und cloudBit

7.1 Einführung in das cloudBit Starter Kit
7.2 Sicherheitsevaluation
7.3 Die Gefährder
7.4 Bug-Bounty-Programme
7.5 Fazit

8 Zukunftssicherheit – ein Dialog über künftige Angriffsvarianten

8.1 Die Thingbots sind da!
8.2 Der Aufstieg der Drohnen
8.3 Geräteübergreifende Angriffe
8.4 Hörst du die Stimme?
8.5 Angriffe auf Cloud-Infrastrukturen

8.6 Durch die Hintertür
8.7 Es blutet mir das Herz
8.8 Verwässerte Patientendateien
8.9 Der Datentsunami
8.10 Angriffe auf Smart Cities
8.11 Hacking Major Tom
8.12 Die Gefahren der Superintelligenz
8.13 Fazit

9 Zwei Szenarios – Absichten und ihre Folgen

9.1 Die wahren Kosten von Freigetränken
9.2 Lüge, Zorn und Selbstzerstörung
9.3 Fazit

Index

1 Licht aus! – Angriff auf drahtlose LED-Leuchten

Der große Stromausfall des Jahres 2003[1] legte das Leben in Teilen des Mittleren Westens und des Nordostens der USA sowie in der kanadischen Provinz Ontario weitgehend lahm. Etwa 45 Millionen Menschen blieben zwei Tage ohne Strom. Allein in New York zählte die Feuerwehr 3000 Anrufe aufgrund des unsachgemäßen Umgangs mit Kerzen. 60 Feueralarme wurden ausgelöst, und es waren zwei Todesopfer zu beklagen, weil versucht worden war, das fehlende Licht mit offenem Feuer zu ersetzen. In Michigan führten brennende Kerzen während des »Blackouts« ebenfalls zu einem Großfeuer, ein Haus brannte bis auf die Grundmauern nieder.

Das Erschreckende daran war nicht das Auftreten des Stromausfalls an sich, sondern die Erkenntnis, in welchem Maße in den Industrieländern die Versorgung etwa mit Elektrizität als selbstverständlich betrachtet wird und wie groß die Abhängigkeit davon ist. In Momenten, in denen uns solche grundlegenden Versorgungsgüter weggenommen werden, sind wir gezwungen, über ihr ständiges Vorhandensein nachzudenken und dieses schätzen zu lernen. Wir drücken auf einen Schalter und erwarten das sofortige Aufleuchten des elektrischen Lichts. Wir öffnen den Kühlschrank und gehen davon aus, dass unsere Lebensmittel und Getränke dort angemessen gekühlt auf uns warten. Wir betreten unsere Wohnung und erwarten zu jeder Zeit eine angenehme Temperatur dank Heizung und Klimaanlage.

Dabei ist es gerade einmal knapp hundert Jahre her, seit wir herausgefunden haben, wie man Strom erzeugt. Davor wurden Häuser mit Petroleumlampen beleuchtet und mit Öfen beheizt. Unsere gegenwärtige Abhängigkeit von der Elektrizität dagegen ist schier unfassbar: Fällt der Strom aus, kommen unsere Städte und Unternehmen innerhalb von Sekunden zum Stillstand.

Die Vereinigten Staaten werden über insgesamt drei miteinander verbundene Stromnetze versorgt, die den Strom im Land verteilen: die Eastern Interconnection, die Western Interconnection und die Texas Interconnection.[2] Diese Systeme sind durch die Kommunikation zwischen den Versorgern und ihren Übertragungssystemen verbunden, um gemeinsam vom Bau größerer Generatoren und der Bereitstellung von Elektrizität zu niedrigeren Kosten profitieren zu können.

In den Industrieländern stehen und fallen die Volkswirtschaften und das Wohl der Bürger mit dem Vorhandensein funktionsfähiger Stromnetze. Immer häufiger wird die Technologie, die solchen Netzen zugrunde liegt (einschließlich Generatoren und Transformatoren), mithilfe von Computern bedient, und die Funktionalität kann über Computernetze ferngesteuert werden. Demzufolge ist es wohl nur allzu verständlich, dass die Sicherheit dieser Systeme vor Angriffen aus dem Cyberspace[3] ein Aspekt ist, über den viel nachgedacht wird.

Doch nicht nur die Sicherheit des Stromnetzes ist wichtig: In der aufkommenden Ära von IoT-Verbraucherprodukten muss noch ein anderes Technologieökosystem wirksam geschützt werden: die IoT-Produkte selbst. Es sind heute bereits verschiedene Produkte erhältlich, die die traditionelle Beleuchtung mit Glühlampen ersetzen sollen und drahtlos ferngesteuert werden können. Wenn wir derartige IoT-Geräte in unsere Wohnungen und Büros einbauen, müssen wir Gewissheit haben, dass nicht nur die zugrunde liegende Infrastruktur (wie etwa das Stromnetz), sondern auch diese Systeme selbst in puncto Sicherheit zuverlässig konstruiert sind.

In diesem Kapitel werden wir Konstruktion und Architektur eines der derzeit populärsten IoT-Produkte auf dem Markt unter die Lupe nehmen: das Beleuchtungssystem Hue des niederländischen Herstellers Philips (*http://meethue.com*). In unserer Gesellschaft ist Beleuchtung aus Gründen der Sicherheit und Bequemlichkeit unentbehrlich; deswegen ist es durchaus sinnvoll, den Schwerpunkt in diesem ersten Kapitel auf ein beliebtes IoT-Produkt dieser Kategorie zu legen. Wir werden Betrieb und Kommunikation des Produkts aus sicherheitstechnischer Sicht analysieren und versuchen, Schwachstellen ausfindig zumachen. Nur auf der Grundlage einer umfassenden Analyse können wir die

bestehenden Sicherheitslücken des Produkts seriös diskutieren und herausfinden, wie sich in Zukunft sichere IoT-Geräte entwickeln lassen.

1.1 Warum Hue?

Wir haben bereits gesehen, warum Beleuchtung für die Sicherheit und Bequemlichkeit in unserer Zivilisation eine so wichtige Rolle spielt. Zu Beginn unserer Analyse von IoT-Geräten in diesem Bereich werden wir uns konkret mit dem *Hue Personal Lighting System* von Philips auseinandersetzen, da es sich ausgesprochen großer Beliebtheit erfreut. Es ist einer der ersten IoT-Beleuchtungsartikel, die eine gewisse Popularität errungen haben, und wird sowohl hinsichtlich seiner Architektur wie auch seiner Konstruktion mit hoher Wahrscheinlichkeit ähnliche Produkte der Konkurrenz inspirieren. Aus diesem Grund kann uns eine Sicherheitsanalyse des Hue-Beleuchtungssystem das Verständnis dafür vermitteln, welche Sicherheitsmechanismen heutzutage bei IoT-Produkten in diesem Bereich zum Einsatz kommen, welche möglichen Schwachstellen vorhanden und welche Änderungen erforderlich sind, um solche Produkte in Zukunft sicher zu machen.

Das Hue-Beleuchtungssystem ist bei verschiedenen Onlinehändlern und Baumärkten erhältlich. Wie Abbildung 1–1 zeigt, umfasst das Starterpaket drei funksteuerbare Leuchtkörper und eine Bridge. Für die Lampen lässt sich über die Hue-Website oder eine iOS-App[4] eine von 16 Millionen Farben festlegen.

Abb. 1–1 *Hue-Starterpaket mit Bridge und drei funksteuerbaren Leuchtkörpern*

Die Bridge wird über ein Ethernetkabel an den Router des Nutzers angeschlossen. Hierdurch entsteht eine ausgehende Verbindung zur Hue-Internetinfrastruktur; wir werden darauf im Folgenden noch eingehen. Die Bridge kommuniziert nun über das auf dem Standard IEEE 802.15.4[5] aufbauende ZigBee-Protokoll[6] direkt mit den LED-Leuchten. ZigBee ist ein kostengünstiges Protokoll mit geringer Leistungsaufnahme, was es für die Kommunikation von IoT-Geräten untereinander prädestiniert.

Befindet sich der Nutzer im lokalen Netzwerk, dann stellt die iOS-App eine direkte Verbindung mit der Bridge her, und es können Befehle

zum Ändern des Leuchtzustands abgesetzt werden. Greift der Nutzer hingegen remote oder über die Hue-Website zu, dann werden die Anweisungen über die Hue-Internetinfrastruktur versendet.

Im weiteren Verlauf dieses Kapitels werden wir die zugrunde liegende Sicherheitsarchitektur untersuchen, um die Implementierung zu verstehen und Schwächen in der Konstruktion zu erkennen. Wir werden ein grundlegendes Verständnis der Sicherheitsmängel vermitteln, die beliebte IoT-basierte Beleuchtungssysteme, wie sie gegenwärtig auf dem Markt erhältlich sind, beeinträchtigen können.

1.2 Leuchten über die Website-Oberfläche steuern

Ein empfehlenswerter Ansatz zur Offenlegung von Sicherheitslücken besteht darin, sich mit der zugrunde liegenden technischen Architektur vertraut zu machen – am besten mithilfe einer Use-Case-Analyse (Analyse von Anwendungsfällen). Der einfachste Anwendungsfall des Hue-Systems besteht in der Onlineregistrierung eines Kontos auf der Hue-Website und der Verknüpfung der Bridge mit diesem Konto. Danach kann der Nutzer mithilfe seines Kontos die Leuchtkörper fernsteuern. In diesem Abschnitt werden wir uns anschauen, wie diese Verknüpfung der Bridge mit dem Benutzerkonto erfolgt und wie sich die Lampen über die Website steuern lassen. Nachdem wir gesehen haben, wie dieser Anwendungsfall technisch implementiert ist, werden wir die zugehörigen Sicherheitsprobleme und Möglichkeiten ihrer Ausnutzung genauer betrachten.

Zuallererst muss sich jeder Nutzer auf dem Hue-Portal über ein kostenloses Konto registrieren[7] (siehe Abb. 1–2). Er muss einen Benutzernamen auswählen, eine E-Mail-Adresse eingeben und ein mindestens sechsstelliges Passwort erstellen.

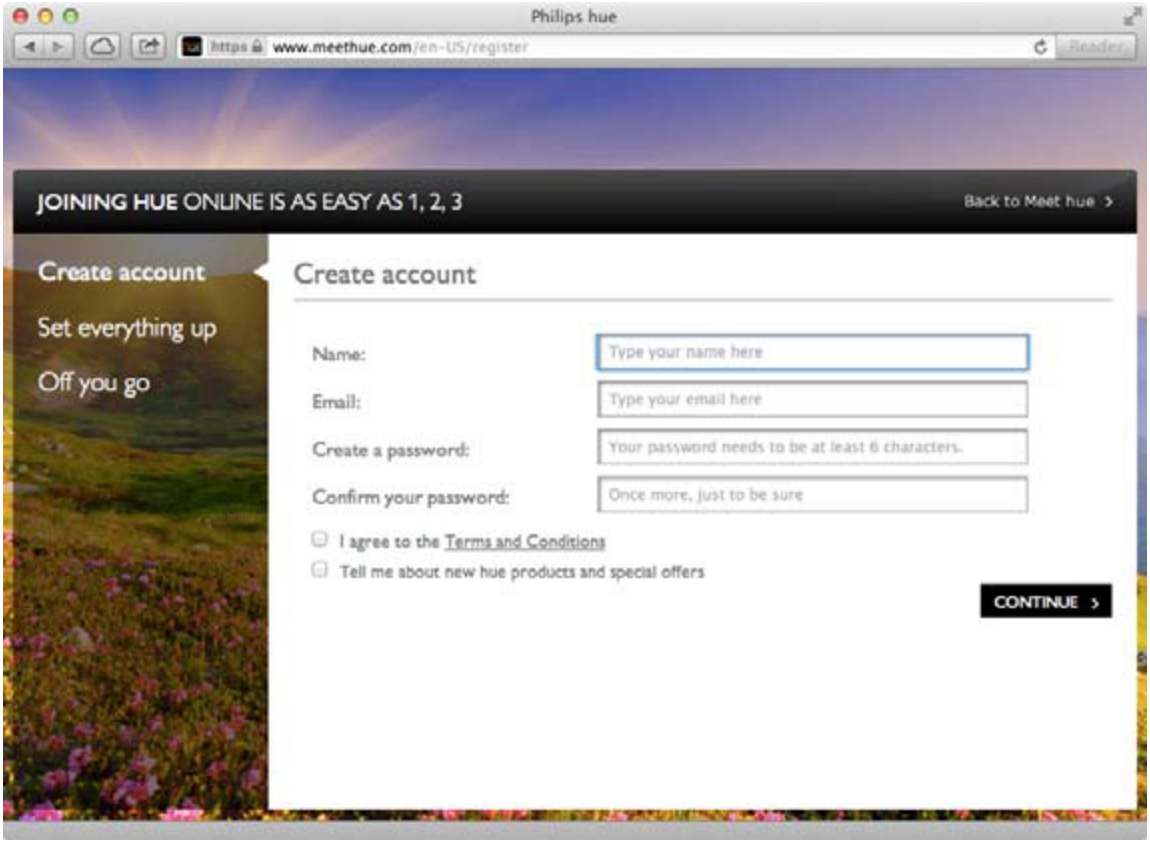

Abb. 1–2 *Registrierung auf der Hue-Website*

Im zweiten Schritt versucht die Website nun, die Bridge zu lokalisieren und sie mit dem vom Nutzer erstellten Konto zu verknüpfen. Wie Abbildung 1–3 zeigt, erscheint auf der Website dann die Meldung »We found your bridge« bzw. »Bridge gefunden« (in der deutschen Version).

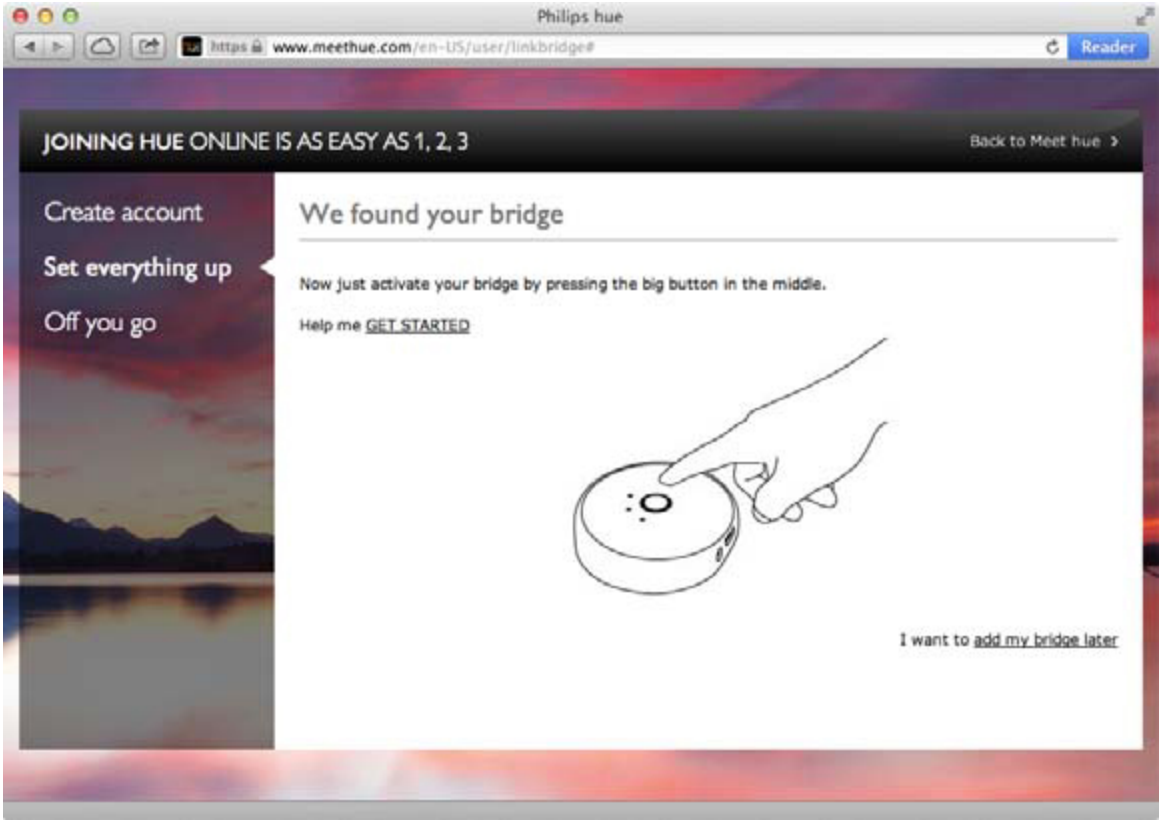

Abb. 1–3 *Bridge mit der Website verknüpfen*

Die Website erkennt, dass die Bridge gefunden wurde, weil die Bridge standardmäßig mit dem Hue-Backend eine Verbindung herstellt, um ihre ID (jeder physischen Bridge wird bei der Herstellung eine eindeutige ID zugewiesen), die interne IP-Adresse und die mit der ID identische MAC-Adresse als Broadcast zu versenden. Zu diesem Zweck sendet die Bridge eine `POST`-Anfrage `an` *dcs.cb.philips.com*:

```
POST /Dcs.ConnectionServiceHTTP/1.0
Host: dcs.cb.philips.com:8080
Authorization: CBAuth Type="SSO", Client="[DELETED]",
RequestNr="16",
Nonce="[DELETED]", SSOToken="[DELETED]", Authentication="
[DELETED]
Content-Type: application/CB-MessageStream;
boundary=ICPMimeBoundary
Transfer-Encoding: Chunked
304
--ICPMimeBoundary
Content-Type: application/CB-Encrypted; cipher=AES
```

```
Content-Length:0000000672
[DELETED]
```

Hierauf erhält die Bridge vom Server folgende Antwort:

```
HTTP/1.0 200 OK
WWW-Authenticate : CBAuth Nonce="[DELETED]"
Connection : close
Content-Type : application/CB-MessageStream;
boundary="ICPMimeBoundary"
Transfer-Encoding : Chunked
001
```

HINWEIS

Als [DELETED] gekennzeichnete Codeabschnitte sind Inhalte, die aus Gründen der Vertraulichkeit und Integrität der für die Tests verwendeten Hardware und Konten gelöscht wurden. Das Entfernen der entsprechenden Zeichen hat jedoch keine nennenswerten Auswirkungen auf die Nachvollziehbarkeit des Beispiels.

Die auf die `POST`-Anfrage erhaltene Antwort `001` zeigt an, dass die Hue-Infrastruktur die Bridge registriert hat, indem sie die zugehörige ID mit der Absender-IPAdresse der HTTP-Verbindung verknüpft hat.

Nach der Installation des Hue-Systems können Sie aus Ihrem Heimnetz heraus die Seite *https://www.meethue.com/api/nupnp besuchen, um festzustellen, welche Informationen von Ihrer Bridge an die Hue-Infrastruktur gemeldet wurden*. Wie Abbildung 1–4 zeigt, werden dort die ID der Bridge nebst ihrer MACund der internen IP-Adresse angezeigt. Die Hue-Website sammelt die relevanten Informationen zu den Bridges (IDs, interne IP-Adressen und MAC-Adressen) und ordnet diese jeweils der Absender-IP-Adresse der TCP-Verbindung zu, wenn Sie die Hue-Website besuchen. Aus diesem Grund meldet die Website wie oben gesehen brav »We found your bridge«.

Abb. 1–4 *ID, interne IP-Adresse und MAC-Adresse der Bridge*

Damit der Nutzer die Erlaubnis erhält, die Bridge fernzusteuern, muss er innerhalb von 30 Sekunden die Taste auf der Bridge betätigen. Der Nachweis des physischen Zugangs zur Bridge gegenüber dem Server stellt eine zusätzliche Sicherheitsebene dar.

Nach dem Anzeigen der Meldung in Abbildung 1–3 setzt der Webbrowser die folgende `GET-Anfrage ab:`

```
GET /en-US/user/isbuttonpressed HTTP/1.1
Host: www.meethue.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_3)
AppleWebKit/536.28.10
(KHTML, like Gecko) Version/6.0.3 Safari/536.28.10
Accept: */*
DNT: 1
X-Requested-With: XMLHttpRequest
Referer: https://www.meethue.com/en-US/user/linkbridge
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Cookie:[DELETED]
Connection: keep-alive
Proxy-Connection: keep-alive
```

Diese `GET-Anfrage wartet 30 Sekunden, damit der Nutzer genügend Zeit hat, die Taste auf der Bridge` zu betätigen. Tut er dies, dann sendet die Bridge zur Bestätigung eine `POST-Anfrage` an *dcp.cpp.philips.com*. Nun hat der Nutzer den physischen Besitz der Bridge nachgewiesen, woraufhin der Server die `POST`-Anfrage positiv beantwortet:

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Cache-Control: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Set-Cookie: PLAY_FLASH=;Path=/;Expires=Thu, 01 Jan 1970 00:00:00
GMT
Set-Cookie: PLAY_ERRORS=;Path=/;Expires=Thu, 01 Jan 1970
00:00:00 GMT
Set-Cookie: [DELETED]
Vary: Accept-Encoding
Date: Mon, 29 Apr 2013 23:30:06 GMT
Server: Google Frontend
Content-Length: 4
true
```

Diese Serverantwort zeigt an, dass die Taste tatsächlich gedrückt wurde. Daraufhin sendet der Browser die folgende `GET`-Anfrage, um die Einrichtung abzuschließen:

```
GET /en-US/user/setupcomplete HTTP/1.1
Host: www.meethue.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_3)
AppleWebKit/536.28.10
(KHTML, like Gecko) Version/6.0.3 Safari/536.28.10
Accept: text/html,application/xhtml+xml,application/xml;
DNT: 1
Referer: https://www.meethue.com/en-US/user/linkbridge
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Cookie: [DELETED]
Connection: keep-alive
Proxy-Connection: keep-alive
```

Auf diese `GET`-Anfrage hin übermittelt der Server viele verschiedene Details:

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8; char-set=utf-8
Cache-Control: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Set-Cookie: PLAY_FLASH=;Path=/;Expires=Thu, 01 Jan 1970 00:00:00
GMT
Set-Cookie: PLAY_ERRORS=;Path=/;Expires=Thu, 01 Jan 1970
00:00:00 GMT
Set-Cookie: PLAY_SESSION="[DELETED]-
%00ip_address%3A[DELETED]__[DELETED]
;Path=/
Vary: Accept-Encoding
```

Date: Mon, 29 Apr 2013 23:30:08 GMT
Server: Google Frontend
Content-Length: 47369
[DELETED]
app.data.bridge = {"clientMessageState":[DELETED],"config":
{"lights":{"15":
{"name":"Bathroom 2","state":
{"bri":254,"effect":"none","sat":144,"reachabl
e":true,"alert":"none","hue":14922,"colormode":"ct","on":false,"
ct":369,"xy
":
[0.4595,0.4105]},"modelid":"LCT001","swversion":"65003148","poin
tsymbol":
{"3":"none","2":"none","1":"none","7":"none","6":"none","5":"non
e","4":"non
e","8":"none"},"type":"Extended color light"},"13":
{"name":"Bathroom 4","st
ate":
{"bri":254,"effect":"none","sat":144,"reachable":true,"alert":"n
one","
hue":14922,"colormode":"ct","on":false,"ct":369,"xy":
[0.4595,0.4105]},"mode
lid":"LCT001","swversion":"65003148","pointsymbol":
{"3":"none","2":"none","
1":"none","7":"none","6":"none","5":"none","4":"none","8":"none"
},"type":"E
xtended color light"},"14":{"name":"Bathroom 3","state":
{"bri":254,"effect"
:"none","sat":144,"reachable":true,"alert":"none","hue":14922,"c
olormode":"
ct","on":false,"ct":369,"xy":
[0.4595,0.4105]},"modelid":"LCT001","swversion
":"65003148","pointsymbol":
{"3":"none","2":"none","1":"none","7":"none","6"
:"none","5":"none","4":"none","8":"none"},"type":"Extended color
light"},"1
1":{"name":"Hallway 2","state":
{"bri":123,"effect":"none","sat":254,"reacha
ble":true,"alert":"none","hue":17617,"colormode":"xy","on":false
,"ct":424,"
xy":
[0.492,0.4569]},"modelid":"LCT001","swversion":"65003148","point
symbol"
:
{"3":"none","2":"none","1":"none","7":"none","6":"none","5":"non
e","4":"no
ne","8":"none"},"type":"Extended color light"},"12":
{"name":"Bathroom 1","s
tate":
{"bri":254,"effect":"none","sat":144,"reachable":true,"alert":"n

```
one",
"hue":14922,"colormode":"ct","on":false,"ct":369,"xy":
[0.4595,0.4105]},"mod
elid":"LCT001","swversion":"65003148","pointsymbol":
{"3":"none","2":"none",
"1":"none","7":"none","6":"none","5":"none","4":"none","8":"none
"},"type":"
Extended color light"},"3":{"name":"Living room lamp 2","state":
{"bri":102,
"effect":"none","sat":234,"reachable":true,"alert":"none","hue":
687,"colorm
ode":"xy","on":false,"ct":500,"xy":
[0.6452,0.3312]},"modelid":"LCT001","swv
ersion":"65003148","pointsymbol":
{"3":"none","2":"none","1":"none","7":"non
e","6":"none","5":"none","4":"none","8":"none"},"type":"Extended
color ligh
t"},"2":{"name":"Living room lamp 1","state":
{"bri":119,"effect":"none","sa
t":180,"reachable":true,"alert":"none","hue":51616,"colormode":"
xy","on":fa
lse,"ct":158,"xy":
[0.3173,0.187]},"modelid":"LCT001","swversion":"65003148"
,"pointsymbol":
{"3":"none","2":"none","1":"none","7":"none","6":"none","5":
"none","4":"none","8":"none"},"type":"Extended color
light"},"1":{"name":"B
ookshelf 1","state":
{"bri":161,"effect":"none","sat":236,"reachable":true,"
alert":"none","hue":696,"colormode":"xy","on":false,"ct":500,"xy
":[0.6474,0
.3308]},"modelid":"LCT001","swversion":"65003148","pointsymbol":
{"3":"none"
,"2":"none","1":"none","7":"none","6":"none","5":"none","4":"non
e","8":"non
e"},"type":"Extended color light"},"10":{"name":"Bedroom
1","state":{"bri":
254,"effect":"none","sat":144,"reachable":true,"alert":"none","h
ue":14922,"
colormode":"ct","on":false,"ct":369,"xy":
[0.4595,0.4105]},"modelid":"LCT001
","swversion":"65003148","pointsymbol":
{"3":"none","2":"none","1":"none","7
":"none","6":"none","5":"none","4":"none","8":"none"},"type":"Ex
tended colo
r light"},"7":{"name":"Guest bedroom 1","state":
{"bri":115,"effect":"none",
"sat":144,"reachable":true,"alert":"none","hue":14922,"colormode
":"xy","on"
:false,"ct":369,"xy":
```

```
[0.2567,0.2172]},"modelid":"LCT001","swversion":"65003
148","pointsymbol":
{"3":"none","2":"none","1":"none","7":"none","6":"none",
"5":"none","4":"none","8":"none"},"type":"Extended color
light"},"6":{"name
":"Kitchen 3","state":
{"bri":74,"effect":"none","sat":253,"reachable":true,
"alert":"none","hue":37012,"colormode":"xy","on":false,"ct":153,
"xy":[0.281
,0.2648]},"modelid":"LCT001","swversion":"65003148","pointsymbol
":{"3":"non
e","2":"none","1":"none","7":"none","6":"none","5":"none","4":"n
one","8":"n
one"},"type":"Extended color light"},"5":{"name":"Kitchen
1","state":{"bri"
:106,"effect":"none","sat":254,"reachable":true,"alert":"none","
hue":25593,
"colormode":"xy","on":false,"ct":290,"xy":
[0.4091,0.518]},"modelid":"LCT001
","swversion":"65003148","pointsymbol":
{"3":"none","2":"none","1":"none","7
":"none","6":"none","5":"none","4":"none","8":"none"},"type":"Ex
tended colo
r light"},"4":{"name":"Bookshelf 2","state":
{"bri":16,"effect":"none","sat"
:247,"reachable":true,"alert":"none","hue":11901,"colormode":"xy
","on":fals
e,"ct":500,"xy":
[0.5466,0.4121]},"modelid":"LCT001","swversion":"65003148",
"pointsymbol":
{"3":"none","2":"none","1":"none","7":"none","6":"none","5":"
none","4":"none","8":"none"},"type":"Extended color light"},"9":
{"name":"Ki
tchen 2","state":
{"bri":246,"effect":"none","sat":216,"reachable":true,"ale
rt":"none","hue":58013,"colormode":"xy","on":false,"ct":359,"xy"
:[0.4546,0.
2323]},"modelid":"LCT001","swversion":"65003148","pointsymbol":
{"3":"none",
"2":"none","1":"none","7":"none","6":"none","5":"none","4":"none
","8":"none
"},"type":"Extended color light"},"8":{"name":"Hallway
1","state":{"bri":9,
"effect":"none","sat":254,"reachable":true,"alert":"none","hue":
25593,"colo
rmode":"xy","on":false,"ct":290,"xy":
[0.4091,0.518]},"modelid":"LCT001","sw
version":"65003148","pointsymbol":
{"3":"none","2":"none","1":"none","7":"no
ne","6":"none","5":"none","4":"none","8":"none"},"type":"Extende
```