9 Zwei Szenarios – Absichten und ihre Folgen

Wir verfügen nun über genug Wissen, um Sicherheitsprobleme im Zusammenhang mit bereits heute erhältlichen IoT-Geräten verstehen zu können sowie auch die Folgen, die Schwachstellen sowohl für die Hersteller solcher Geräte als auch für deren Nutzer haben können. Außerdem haben wir uns angesehen, wie man überhaupt ein Konzept für ein IoT-Produkt entwickelt und dabei bereits in der Prototypphase die erforderlichen Sicherheitsfunktionen implementiert. Wir wissen, wie wir mit unseren Kenntnissen über Lücken im Sicherheitsgefüge Risiken bewerten können und wie Gefährder solche Lücken nutzen.

Wichtig ist jedoch nicht nur, Sicherheitsfunktionen zu kennen und zu verstehen, sondern Sie sollten sich auch im Klaren darüber sein, dass sicherheitsrelevante Vorfälle – ganzheitlich betrachtet – auch und vor allem von den beteiligten Personen und von ihrem Handeln in den jeweiligen Situationen beeinflusst werden.

Wir werden in diesem Kapitel einen Blick auf zwei unterschiedliche Szenarios werfen, um ein Gefühl dafür zu entwickeln, wie derartige Vorfälle von den Beteiligten beeinflusst werden können. Im ersten Szenario werden wir sehen, wie ein leitender Mitarbeiter eines Konzerns versucht, sich den derzeitigen Hype um das Thema IoT-Sicherheit zunutze zu machen, um den Unternehmensvorstand zu beeindrucken. Das zweite Szenario beschreibt, wie ein aufstrebender IoT-Dienstleister auf Fragen von Sicherheitsfachleuten und Journalisten reagiert, um die Integrität seines Unternehmens aufrechtzuerhalten. Dieses Kapitel soll in erster Linie veranschaulichen, dass die Folgen, die in sicherheitsrelevanten Szenarios auftreten können, letztendlich vor allem durch die Ziele und Handlungen der beteiligten Personen beeinflusst werden.

9.1 Die wahren Kosten von Freigetränken

Auf dem Gebiet der Cybersecurity gibt es leider immer wieder Anbieter, deren Softwaretools alles andere als wirksam sind und Unternehmen deswegen in falscher Sicherheit wiegen. Das liegt vor allem daran, dass es zeitaufwendig ist, Feedback und neueste Erkenntnisse zu technischen Entwicklungen und Angriffsvektoren in Tools umzusetzen, die neu entstehende Technologien schützen sollen.

Auf der anderen Seite war die Bedeutung des Chief Information Security Officer (CISO) in den Unternehmen nie so groß wie heute, ist man dort doch besorgt, dass Angreifer unterschiedlichster Herkunft Schwachstellen ausnutzen und so finanzielle Einbußen verursachen und den guten Ruf der Firma beschädigen. Mitarbeiter, die in der Lage sind, die CISO-Funktion in großen und komplexen Infrastrukturen auszufüllen, sind gesucht und können mit einem Jahresgehalt von 1 Mio. US-Dollar[1] und mehr rechnen.

Die große Nachfrage nach erfahrenen Mitarbeitern führt in Kombination mit dem geringen Fachkräfteangebot dazu, dass für Unternehmen das Risiko besteht, in wirkungslose Sicherheitstools zu investieren. Im nachfolgend beschriebenen Szenario werden wir uns ansehen, wie durch das Aufkommen des Internet of Things Gefahren für ein Unternehmen entstehen, weil dort keine umfassende Sicherheitsstrategie entwickelt wurde.

9.1.1 Party im Ruby Skye

Die RSA-Konferenz, die alljährlich in San Francisco stattfindet, ist die größte Cybersecurity-Konferenz der Welt. Es gibt dort nicht nur Keynotes und Vorträge, sondern die Konferenz bietet auch eine großartige Möglichkeit, Sicherheitsexperten zu treffen und sich mit ihnen zu vernetzen.

John Smith, unlängst ernannter Vizepräsident und CISO bei Acme Inc., hatte sich besonders auf diese Konferenz gefreut. Er hatte seine Stelle bei Acme Inc. gerade erst angetreten, und der Vorstand des Unternehmens hatte bereits die Einstellung von 30 zusätzlichen Vollzeitmitarbeitern genehmigt, die ihm unterstellt sein sollten. John Smith wollte seine Begeisterung über seinen neuen Job mit seinen Freunden teilen, die an der Konferenz teilnahmen.

Auch Sam Cronin, Geschäftsführer und Vertriebsleiter bei Plunk, freute sich auf die RSA-Konferenz. Es war ihm gelungen, den gesamten Clubbereich des Ruby Skye, einer beliebten Diskothek in San Francisco, auf Geschäftskosten für einen Abend zu mieten. (Es ist während solcher Konferenzen durchaus üblich, dass Unternehmen beliebte Restaurants und Bars mieten, um kostenlose Partys für die Konferenzbesucher zu organisieren. Dies tun sie in der Hoffnung, dass ihre Gäste sich von der Party so sehr beeindrucken lassen, dass sie zu Kunden werden.)

Das Unternehmen Plunk, bei dem Cronin arbeitet, stellt ein populäres Tool zur Erfassung und Korrelierung großer Mengen von Logdaten her, die sich dann auf Anomalien prüfen lassen. Dies soll die Erkennung verdächtiger Ereignisse ermöglichen, die mit einem Angriff in Zusammenhang stehen könnten.

Auch John Smith war zur Party eingeladen worden und hatte gerne zugesagt. Er kannte nicht nur das Produkt, sondern wusste auch, dass im Ruby Skye eine Menge Spaß auf ihn wartete. Als er abends am Eingang des Clubs erschien und

1. *http://bit.ly/soaring_ciso_pay*

sein RSA-Namensschild vorzeigte, erkannte der Vertreter von Plunk darauf den Titel »Vice-President« und lotste ihn deswegen in den VIP-Bereich, wo es nicht nur die ganz teuren Getränke umsonst gab, sondern auch einige abgeteilte Zonen, die für Führungskräfte potenzieller Kunden reserviert waren.

Cronin stellte sich Smith gegenüber als Leiter der Vertriebsabteilung vor, und schnell verstrickten sich die beiden in ein Gespräch über die Sicherheit von IoT-Geräten. Smith sprach auch über seine neue Tätigkeit und darüber, wie spannend er die Aussicht fand, beim Vorstand von Acme Inc. ein höheres Betriebsbudget für sein Team herauszuschlagen, zusätzliche Mitarbeiter einzustellen und weitere Sicherheitsprodukte einzukaufen. Daraufhin bot Cronin Smith eine kostenlose Beratung an, um ihn auf das Treffen mit dem Vorstand vorzubereiten. Im Gegenzug ließ Smith die Bemerkung fallen, dass er Lizenzen für das Plunk-Sicherheitstool erwerben würde, sofern seine Vorgesetzten seinem Vorschlag folgten. Die beiden verabschiedeten sich voneinander, nicht ohne ein weiteres Gespräch in wenigen Tagen zu verabreden.

9.1.2 Buzzwords und wie man sie gewinnbringend nutzt

Eine Woche nach der RSA-Konferenz telefonierten Smith und Cronin miteinander. Smiths Absicht war es, den Vorstand von Acme Inc. zu beeindrucken, damit sein Plan, 55 zusätzliche Vollzeitmitarbeiter einzustellen, ebenso genehmigt würde wie ein Budget in Höhe von 100 Mio. US-Dollar für Investitionen und Betriebsausgaben in den kommenden drei Jahren.

Cronin war vor Kurzem damit beauftragt worden, das Plunk-Tool mit einer zusätzlichen Funktion zu verkaufen, die Logdaten von IoT-Produkten im Unternehmen erfasst. Diese Funktion ermöglicht es den Kunden, ihr Hardwareinventar im Blick zu behalten, was sicherheitstechnisch auch durchaus sinnvoll ist: Geräte wie Laptops, Mobiltelefone und IoT-Produkte, die nicht berücksichtigt werden, stellen ein gigantisches Sicherheitsrisiko dar, und wenn die Organisation keinen Überblick über die vorhandenen Geräte hat, ist es unmöglich, dieses Risiko zu reduzieren oder auch nur einzuschätzen.

Smith fragte Cronin, ob dieser das eine oder andere Thema vorschlagen könnte, das den Vorstand vielleicht interessieren würde. Daraufhin empfahl Cronin, den Schwerpunkt bei der Präsentation auf das gerade angesagteste Thema zu legen: das Aufkommen des Internet of Things und die damit einhergehenden Risiken. Im vorangegangenen Jahr hatte die Nutzung von Machine Learning und Big Data zur Korrelierung von Logdaten mit dem Ziel, Angriffe zu erkennen, zu den wichtigsten Themen auf der RSA-Veranstaltung gehört. In diesem Jahr war es vor allem um die Auswirkungen von IoT-Produkten auf die Sicherheit gegangen. Insofern stimmte Smith dem Vorschlag zu, sich vor allem auf dieses Thema zu konzentrieren. Er war der Ansicht, dass die Vorstandsmitglieder dies interessant finden würden und er sie mit seinem topaktuellen Wissen beeindrucken könnte.

9.1.3 Die Vorstandssitzung

Smiths Vortrag war für 10:40 Uhr angesetzt, und er hatte genau 10 Minuten Zeit. Er hatte eine PowerPoint-Präsentation vorbereitet, doch wurde ihm mitgeteilt, dass die Vorstandsmitglieder keine Zeit dafür hätten. Er musste sein Anliegen also kurz zusammengefasst und auf den Punkt gebracht vortragen. Und dann geschah Folgendes:

Smith: *Vielen Dank dafür, dass Sie sich Zeit für meine Ausführungen zum Thema Sicherheit nehmen. Als neu ernannter Chief Information Security Officer ist es meine vordringlichste Aufgabe, …*

Vorstandsmitglied 1: *Entschuldigen Sie, wenn ich Sie unterbreche. Worum genau geht es bei dem von Ihnen präsentierten Punkt?*

Smith: *Ich möchte über die wichtigsten Sicherheitsrisiken sprechen, deren Bekämpfung entscheidend sein wird.*

Vorstandsmitglied 1: *Okay, lassen Sie die Einleitung weg und kommen Sie bitte sofort zum Wesentlichen. Wir wissen, dass Sie unser CISO sind. Wir haben Sie eingestellt. Wir wissen auch über Ihre Tätigkeit Bescheid. Fahren Sie also fort.*

Smith: *Gut. Ich bin überzeugt, dass der Vorstand mit den IoT-Geräten am Markt vertraut ist, und dass bei vielen derartigen Geräten Sicherheitsrisiken festgestellt wurden. Wir sollten deswegen eine Partnerschaft mit einem führenden Hersteller von Sicherheitstools eingehen. Ich schlage das Unternehmen Plunk vor, denn …*

Vorstandsmitglied 2: *Einen Moment. Wir sind ein Krankenversicherungsunternehmen. Welche Arten von IoT-Geräten in unseren Einrichtungen betrifft dies? Vertreten Sie die Ansicht, dass die Risiken, die IoT-Geräte heute für unser Unternehmen darstellen, wichtiger sind als die Mittel, die wir bereitstellen, um die Einhaltung gesetzlicher Gesundheitsvorschriften zu unterstützen? Oder sprechen Sie von IoT-Geräten, die Ihrer persönlichen Ansicht nach in der Zukunft Risiken für uns darstellen könnten?*

Smith: *Mein Beitrag ist in der Tat auf die Zukunft gerichtet. Ich weiß nicht genau, welche IoT-Geräte uns heute Sorgen machen müssen, aber ich habe die RSA-Konferenz besucht, und alle Keynote Speaker erwähnten die Auswirkungen des Internet of Things auf die Sicherheit. Deswegen wollte ich …*

Vorstandsmitglied 2: *Bitte kommen Sie wieder, wenn Sie in der Lage sind, unsere Geschäftsstrategie technisch umzusetzen, und wir über handfeste Probleme sprechen können, die auf einem sachbezogenen Verständnis unserer Technologielandschaft basieren. Vielen Dank, Smith, Sie können gehen. Die nächste Präsentation, bitte.*

Smith wurde aus dem Sitzungszimmer geleitet. Er hatte angenommen, dass der Vorstand seine Kenntnisse zu aktuellen Sicherheitsfragen zu schätzen wissen würde, aber sein Vortrag hatte gerade einmal 1 Minute und 15 Sekunden gedauert. Er war vollkommen perplex.

Am nächsten Tag rief die Personalabteilung bei ihm an und bat um seine sofortige Kündigung. Seine im Arbeitsvertrag festgelegte Abfindung in Höhe von sechs Monatsgehältern würde er selbstverständlich erhalten.

9.1.4 Was war schief gelaufen?

In der Rückschau lässt sich feststellen, dass eine ganze Reihe von Faktoren zu Smiths Scheitern beigetragen hat. Sam Cronins Rolle als Vertriebsleiter beim Hersteller eines Sicherheitstools machte ihn zu einem voreingenommenen Berater. Ihm war es schließlich nur darum gegangen, Lizenzen für sein aktualisiertes Produkt zu verkaufen, was nicht im Einklang mit den Zielen des Vorstands von Acme Inc. stand.

Smith hätte sich stattdessen besser mit seinen Kollegen und anderen objektiven Personen beraten sollen, deren Unterstützung er in der Vergangenheit bereits in Anspruch genommen hatte – schließlich hatte er überhaupt keine Erfahrung mit Präsentationen bei Vorstandssitzungen. Vorstände brauchen eine kurze und knappe Aussage zu aktuellen Problemen und deren Auswirkungen auf die Geschäftstätigkeit des Unternehmens. Statt den Schwerpunkt ausschließlich auf die mit IoT-Geräten verbundenen Gefährdungen zu legen, hätte Smith eine nach Prioritäten sortierte Liste der Sicherheitsrisiken vorlegen sollen, die den Geschäftsbetrieb von Acme Inc. potenziell beeinflussen könnten: Zugang für Unbefugte, Verstöße gegen die Vertraulichkeit geistigen Eigentums usw. Diese Liste hätte dann auch IoT-spezifische Punkte sowie eine Roadmap für die in absehbarer Zeit zunehmende Verbreitung des Internet of Things enthalten können. Weil Smith sich ausschließlich auf die IoT-Geräte konzentrierte, war für den Vorstand sofort offensichtlich, dass er nicht die gesamte Risikolandschaft in Betracht gezogen hatte.

Die Bedeutung des Internet of Things und die Tatsache, dass es unser Leben privat wie auch bei der Arbeit in Zukunft bereichern wird, stehen außer Frage. Je stärker IoT-Geräte in unsere Welt vordringen, desto häufiger werden wir über ihre Sicherheit reden. Wie fast immer wollen Menschen und Medien das mit dem Aufkommen neuer Technologien verbundene Aufsehen nutzen, um Aufmerksamkeit zu erzielen. In vielen Fällen ist das auch gut und richtig, denn auf diese Weise gelangen Informationen an die Öffentlichkeit, und man spricht über das Thema. Hier jedoch hat Smith nicht nur die Zeit des Vorstands vergeudet, sondern durch sein Unvermögen, eine durchdachte und ganzheitliche Sicherheitsstrategie für Acme Inc. zu präsentieren, würde die Vorgehensweise im Sicherheitsbereich des Unternehmens unklar bleiben, solange der Vorstand keinen neuen CISO gefunden und eingestellt hat.

9.2 Lüge, Zorn und Selbstzerstörung

Zu Hause und auf der Arbeit nutzen die Menschen immer häufiger IoT-Geräte, die von unterschiedlichsten Unternehmen wie Philips, Belkin und Samsung hergestellt werden. Anbieter wie Apple, Microsoft, SmartThings oder IFTTT wetteifern darum, vereinheitlichte Plattformen zu entwickeln, die eine Integration dieser verschiedenen Geräte gestatten und eine nahtlose Benutzererfahrung gewährleisten sollen.

Wie wir aber in den vorangegangenen Kapiteln dieses Buchs bereits gesehen haben, weisen viele zurzeit erhältliche IoT-Geräte erhebliche Sicherheitslücken auf. Trotzdem werden diese Produkte schon eingesetzt und schaffen so Schwachstellen, durch die ganze IoT-Ökosysteme gefährdet werden. In der Vergangenheit konnten Softwareanbieter kritische Sicherheitslücken durch die schnelle Bereitstellung von Patches schließen. Dabei beschränkten sich die negativen Auswirkungen auf Endbenutzer normalerweise auf das Durchführen eines Computerneustarts, um die nervtötenden Updatehinweise loszuwerden.

Plattformen, die einen vereinheitlichten Zugang zu IoT-Geräten von unterschiedlichen Herstellern mit jeweils eigenen Protokollen gewähren sollen, tragen ein hohes Maß an Verantwortung dafür, das Schließen von Sicherheitslücken zu ermöglichen und gleichzeitig ihre eigene Infrastruktur vor Angriffen und Missbrauch zu schützen – sei es durch externe Gefährder oder die eigenen Mitarbeiter. Anders als bei Betriebssystemen und Anwendungen haben Anbieter von IoT-Plattformen oft nicht die Möglichkeit, eine bekannt gewordene Sicherheitslücke schnell zu schließen, ohne Dienste zu unterbrechen, die die Benutzer im täglichen Leben benötigen. Im folgenden hypothetischen Szenario wird genau eine solche Situation beschrieben. Wir müssen uns also der Tatsache bewusst sein, dass Dienste aufgrund von Versäumnissen im Sicherheitsbereich möglicherweise vorübergehend nicht zur Verfügung stehen.

9.2.1 Die Vorteile von LifeThings

Eine Sache, die LifeThings so großartig machte, war die fantastische Arbeitskultur. Obwohl das Start-up innerhalb von nur neun Monaten von 20 auf 1000 Mitarbeiter angewachsen war, hielt sich der Geschäftsführer an das Versprechen, flache Hierarchien zu pflegen, in denen der Wert eines Mitarbeiters nicht an seiner Stellenbezeichnung gemessen wurde, sondern an seinem persönlichen Beitrag.

Die Geschäftsstrategie von LifeThings bestand darin, im eigenen Heim eingesetzte IoT-Geräte miteinander zu integrieren, damit die Benutzer nicht mehr für jedes einzelne gekaufte Gerät eine separate App herunterladen mussten. Das Produkt von LifeThings war ein Hub, der mit dem WLAN verbunden werden musste und dann IoT-Geräte im Netzwerk autark erkennen konnte. LifeThings hatte Partnerschaften mit den Big Playern wie SmartThings, Philips, Foscam und vielen

anderen geschlossen, um Produkte wie funkgesteuerte Türschlösser, Autos, Beleuchtungseinrichtungen und Babyfone mithilfe des LifeThings-Hubs zu steuern.

Im Zuge des Immobilienbooms wurden in San Francisco und Seattle Komplexe mit Eigentumswohnungen gebaut, deren Bewohnern LifeThings sein Produkt kostenfrei zur lebenslangen Nutzung anbot. Die Vertriebsabteilung schloss mit den Bauträgern Verträge über den Einbau der Hubs in die neuen Wohnungen, sodass die Bewohner diese sofort nach dem Einzug nutzen konnten. Das Vorhandensein der LifeThings-Hubs sorgte dann dafür, dass viele Wohnungseigentümer drahtlose Beleuchtungssysteme, vernetzte Türschlösser und Videomonitore installierten, um den von LifeThings angebotenen kostenfreien Service nutzen zu können. Die Menschen waren von der transparenten Interoperabilität der Plattform begeistert: Sie konnten Rezepte zur Steuerung ihrer Lampen erstellen, elektronische Haustürschlüssel an ihre Freunde verteilen usw. Mundpropaganda und positive Bewertungen führten rasch dazu, dass LifeThings ein gängiger Name wurde – und die Umsätze des Unternehmens schossen geradezu in die Höhe.

Simin Powell leitete das LifeThings-Kundendienstteam. Nach einer aktuellen Umfrage lag die Zufriedenheit der LifeThings-Kunden mit dem Kundendienst bei 99,8 Prozent und damit deutlich über den Werten anderer Technologieunternehmen. Powell äußerte öffentlich das Versprechen, dass jedes Kundenproblem innerhalb von fünf Minuten nach Beginn des Kundenanrufs gelöst sein würde. Und dieses Versprechen konnte zum größten Teil auch eingehalten werden. Eltern riefen beim Kundendienst an, um ihre Kinder in die Wohnung zu lassen, wenn sie von der Schule nach Hause kamen, oder um den Status des Wohnungstürschlosses zu erfragen, wenn sie unsicher waren, ob sie abgeschlossen hatten oder nicht. Die meisten derartigen Aufgaben konnten mithilfe der LifeThings-App erledigt werden, aber trotzdem erfüllte das Unternehmen telefonische Kundenwünsche prompt, da es einen Rundumservice bieten wollte, um seinen Kunden im Problemfall optimal zur Seite zu stehen.

9.2.2 Social Engineering mit gefälschter Rufnummernübertragung

Ein paar Sicherheitsfachleute, die auch LifeThings-Benutzer waren, stellten irgendwann fest, dass die Kundendienstmitarbeiter sie automatisch mit Namen ansprachen. Während die meisten Kunden dies als angenehm empfanden, bemerkten die Sicherheitsexperten bald, dass LifeThings zu diesem Zweck auf die übermittelten Rufnummern zurückgriff, d.h., diese Rufnummern wurden zur Identifizierung des Kunden mit den entsprechenden Datensätzen verknüpft. Sie versuchten daraufhin, den Kundendienst telefonisch über das Problem zu informieren, doch waren die Servicemitarbeiter nicht in der Lage, die Tragweite zu erfassen, und bestanden darauf, dass die Dienste von LifeThings zuverlässig vor Hackern geschützt seien. Da sie keine Chance sahen, den Vorfall zu melden, veröffentlichten die Forscher ihre Erkenntnisse zur Sicherheitslücke in einem Blogpost

und demonstrierten, wie einfach sich eine übermittelte Rufnummer mit einem kommerziellen Dienst wie SpoofCard (Abb. 9–1) fälschen lässt.

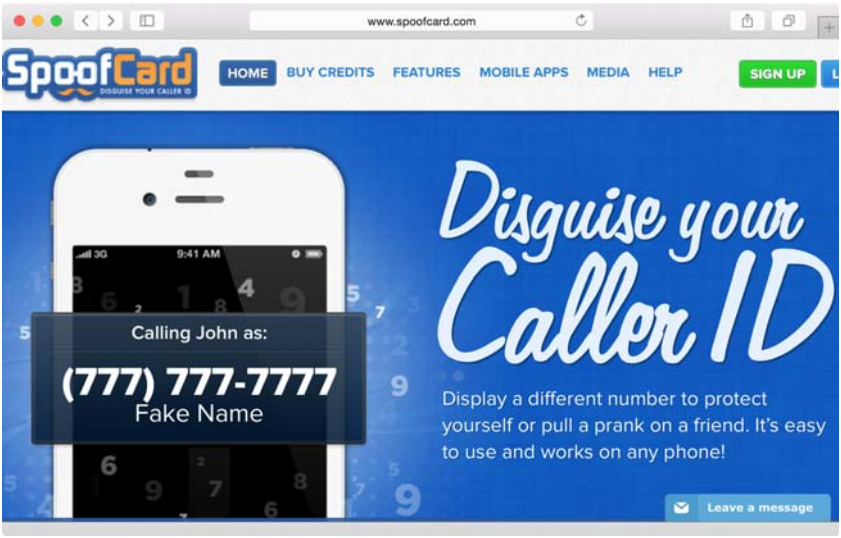

Abb. 9–1 *Mit SpoofCard kann jeder die von ihm übermittelte Rufnummer fälschen.*

Die Experten veröffentlichten sogar Audiomitschnitte von Telefongesprächen, die sie mit dem LifeThings-Kundendienst unter Verwendung einer gefälschten übermittelten Rufnummer geführt und in denen sie den jeweiligen Mitarbeiter dazu aufgefordert hatten, ihnen beim Öffnen ihrer Haustüre zu helfen. Daraufhin gab Simin Powell eine Pressemeldung folgenden Inhalts heraus:

> *Sicherheit und Privatsphäre unserer Kunden haben für uns oberste Priorität. Unserer Ansicht nach beweist die Tatsache, dass diese Personen Informationen darüber veröffentlicht haben, wie sich unser Kundendienst via Social Engineering hintergehen lässt, einen offensichtlichen Mangel an Professionalität. Ferner glauben wir, dass Hackerdienste wie SpoofCard verboten werden sollten, weil sie die beschriebenen Handlungen erst ermöglichen. Nichtsdestoweniger entwickeln wir fortlaufend neue Wege, um unseren Kunden einen möglichst sicheren und effizienten Service zu bieten.*

Das Problem bei Powells Antwort bestand darin, dass seine Reaktion zum einen rein emotional und gegen die Sicherheitsfachleute gerichtet war und zum anderen keine praktische Lösung für das Risiko bot, dem die Kunden ausgesetzt waren. Ein solches Verhalten ist häufig dann zu beobachten, wenn Unternehmen die Risiken für sich und ihre Kunden nicht richtig einschätzen können oder wenn sie unter Druck stehen, Leistungen für ihre Kunden erbringen zu müssen, während sie noch nicht genügend Zeit hatten, sich mit Sicherheitsaspekten umfassend auseinanderzusetzen. Darüber hinaus fand die Tatsache, dass die Experten tatsäch-

lich versucht hatten, das Problem zu melden, in Powells Statement keinerlei Erwähnung. Ein solcher Mangel an Transparenz kann aufseiten der Kunden zu einem erheblichen Vertrauensverlust führen und schwerwiegende Folgen für die Marke des Unternehmens haben.

9.2.3 Das (un)sichere Token

Da die Mitarbeiter vom LifeThings-Kundendienst ihr Bestes geben, um die Probleme ihrer Kunden innerhalb von fünf Minuten zu lösen, versuchen sie in den ersten beiden Minuten eines Anrufs einzuschätzen, ob es sich um ein nicht technisches Problem oder eine häufig gestellte Frage handelt, die zügig beantwortet werden kann. Andernfalls können die Kundendienstmitarbeiter sich remote beim LifeThings-Hub am Kundenstandort anmelden, um die Anfrage zu bearbeiten. Zu diesem Zweck gibt der jeweilige Mitarbeiter den folgenden Befehl auf seinem Terminal ein (hierbei wird vorausgesetzt, dass die E-Mail-Adresse des Kunden *customer@email.com* lautet):

```
$ create-secure-token customer@email.com
secure-token: a7144596f20fe4daf3a3c75f7011c4c5
```

Der Wert von `secure-token` wurde dann für den Zugriff auf den Hub des Kunden verwendet. Danach meldete sich der Mitarbeiter via `ssh` beim Server *secure.lifethings.com* an und benutzte hierzu `secure-token` als Passwort:

```
$ ssh -l customer@email.com secure.lifethings.com
Password: a7144596f20fe4daf3a3c75f7011c4c5
```

Nun konnte der Mitarbeiter mithilfe des Befehls `hub` die Geräte erfragen, die mit dem Hub verbunden waren:

```
$ hub -l
1. [Thermostat] [Status: 69F]
2. [Lock: Main door] [Status: Locked]
3. [Lock: Garage door] [Status: Locked]
4. [Light switch: Living room lamp] [Status: Off]
5. [Baby monitor: Bedroom 2] [Status: Inactive]
```

Als Nächstes sehen wir ein Beispiel dafür, wie sich die Temperatureinstellung eines Thermostats beim Kunden ändern ließ:

```
$ hub "Thermostat" -s "80"
[Thermostat] [Status: 80F]
```

Die Haustür des Kunden ließ sich wie folgt aufsperren:

```
$ hub "Lock: Main door" -s "Unlocked"
[Lock: Main door] [Status: Unlocked]
```

Schließlich war es auch möglich, sich durch Wiedergabe der Datei *audio1.mp3* mit dem folgenden Befehl eine zweiminütige Audioaufnahme anzuhören, die mit einem angeschlossenen Babyfon aufgezeichnet worden war:

```
$ hub "Baby monitor: Bedroom 2" -s "2m" -o audio1.mp3
[Baby monitor: Bedroom 2] [Status: Capturing audio to audio1.mp3 for 120s.
Press ^C to abort]
```

Das auf *secure.lifethings.com* vorhandene *hub*-Tool gestattete den Kundendienstmitarbeitern das einfache Abfragen und Ändern des Status aller Geräte, die mit einem LifeThings-Hub verbunden waren. Dies vereinfachte die schnelle Unterstützung von Benutzern, die Probleme mit bestimmten Geräten hatten, ganz erheblich. Außerdem konnte so sogar Kunden geholfen werden, die sich versehentlich aus ihren Wohnungen oder Häusern ausgesperrt hatten.

9.2.4 Vollzugriff

Genau ein Jahr nach der Enthüllung der oben beschriebenen Sicherheitslücke wurden die Forscher eingeladen, auf einer Sicherheitskonferenz einen Vortrag zu halten. Sie fragten sich, ob sie das LifeThings-System noch eingehender analysieren konnten. Sie schraubten also den LifeThings-Hub auf und entdeckten dort eine Micro-SD-Karte, auf der sich eine Datei namens */etc/config* mit folgendem Inhalt befand:

```
SSH_REMOTE=secure.lifethings.com
USER=researchers@email.com
MD5=93a4c0c0da435f4434f828c95cf70d6a
```

Schnell fanden sie heraus, dass unter der Adresse *secure.lifethings.com* ein SSH-Dienst ausgeführt wurde, mit dem sie sich am Server anmelden konnten. Sie nahmen an, dass als Benutzername *researchers@email.com* verwendet werden musste, da dieser dem String `USER` in der Datei */etc/config* zugeordnet war; hierbei handelte es sich um ihre eigene E-Mail-Adresse, mit der sie seinerzeit ihr LifeThings-Konto registriert hatten. Zu diesem Zeitpunkt kamen sie allerdings noch nicht auf die Idee, dass der MD5-Hashwert tatsächlich das Passwort sein könnte. Sie probierten einen Abend lang herum, setzten die Karte dann wieder ein und beschlossen, ihre Untersuchungen am nächsten Tag fortzusetzen.

Am darauffolgenden Morgen zogen sie die SD-Karte erneut heraus und sahen sich die Datei */etc/config* noch einmal an:

```
SSH_REMOTE=secure.lifethings.com
USER=researchers@email.com
MD5=a0536156e0267d5ed71a59cca90f2692
```

Der Wert von `MD5` hatte sich geändert. Sie setzten die Karte erneut für einige Stunden in den Hub ein und entnahmen sie später am selben Tag noch einmal. Noch immer lautete der Wert von `MD5` `a0536156e0267d5ed71a59cca90f2692`. Das bedeu-

tete, dass dieser Wert sich täglich änderte und deswegen wahrscheinlich auf irgendeine Weise mit dem Datum verknüpft war. Dieses Datum war der 10. Juni 2015. Sie probierten also verschiedene Datumszeichenfolgen aus, um den Hash auf diese Weise zu replizieren:

```
$ md5 -s "June 10, 2015"
MD5 ("June 10, 2015") = 21c0f5e21aea63e9c1e3055a3eda6cb9
$ md5 -s "06102015"
MD5 ("06102015") = 14e2234a4c2d9ba4490b548972d6b794
$ md5 -s "06-10-2015"
MD5 ("06-10-2015") = 579949533abab20c4b07f5ed7d56b70d
```

Keiner der Hashwerte passte. Dann dämmerte ihnen, dass es sich bei dem Wert um eine Aneinanderreihung von `USER`-Wert und Datum handeln könnte, und schon nach wenigen Versuchen hatten sie das Prinzip durchschaut:

```
$ md5 -s 'resear-chers@email.com06102015'
MD5 ("researchers@email.com06102015") = a0536156e0267d5ed71a59cca90f2692
```

Zur Verifizierung ihrer Feststellungen überprüften sie, ob sie mit dem Datum des Vortages auch den vorherigen MD5-Wert erhalten würden. Und siehe da:

```
$ md5 -s 'resear-chers@email.com06092015'
MD5 ("researchers@email.com06092015") = 93a4c0c0da435f4434f828c95cf70d6a
```

Geschafft! Die Forscher bemerkten dann etwas, das ihnen zuvor entgangen war – dass nämlich der Wert von `MD5` nichts anderes als das Passwort war, mit dem sie sich am Server *secure.lifethings.com* anmelden konnten:

```
$ ssh -l researchers@email.com secure.lifethings.com
Password: a0536156e0267d5ed71a59cca90f2692
```

Nach der Anmeldung und dem Auffinden des Befehls `hub` fanden sie heraus, dass sie Zugang zu ihrem eigenen Hub hatten. Da ein Freund von ihnen ebenfalls einen LifeThings-Hub einsetzte, hatten sie nun nichts Besseres zu tun, als dessen Passwort zu berechnen:

```
$ md5 -s 'friend@email.com06102015'
MD5 ("friend@email.com06102015") = b6ebb2b704bc66c2d50b5d5ed2425e5c
```

Auf diese Weise konnten sie sich mit der Identität dieses Freundes anmelden und seine Geräte remote steuern – ganz genau so, wie es auch ein Kundendienstmitarbeiter von LifeThings tun würde. Nachdem sie früher bereits versucht hatten, das Problem der gefälschten Rufnummer bei LifeThings zu melden, und daraufhin ihnen unprofessionelles Verhalten vorgeworfen worden war, entschieden die Forscher, diese Sicherheitslücke bei der Konferenz vorzustellen, um zu zeigen, wie Angreifer remote auf alle mit einem LifeThings-Hub verbundenen Geräte zugreifen konnten, sofern ihnen die E-Mail-Adresse des Opfers bekannt war.

9.2.5 Das Ende von LifeThings

Eine Woche, nachdem die Forscher ihre Entdeckungen präsentiert hatten, verfasste der bekannte investigative Journalist Stan Goodin einen Artikel, in dem er diese Erkenntnisse mit mehreren Vorfällen in Verbindung brachte, in denen die unsichere Architektur der LifeThings-Infrastruktur in letzter Zeit missbraucht worden war:

- Polizeiliche Statistiken zeigten eine ungewöhnlich hohe Anzahl von Einbrüchen in den erwähnten Wohnkomplexen, in denen LifeThings-Hubs zuvor eingebaut worden waren.
- Audioaufnahmen von Gesprächen, in denen hochrangige Politiker geheime Details zu Kampagnen zu Hause mit ihren Partnern besprochen hatten, gelangten ins Internet. Die betreffenden vier Politiker wohnten alle in Häusern, die mit LifeThings-Systemen ausgestattet waren.

Goodins Artikel wurde von verschiedenen Medien weltweit übernommen und veröffentlicht. Folgende Reaktion kam von LifeThings, wiederum geäußert von Simin Powell:

> *Die Geschäftsführung von LifeThings nimmt Sicherheit und Privatsphäre ihrer Kunden sehr ernst. Der kürzlich von Stan Goodin veröffentlichte Artikel entbehrt jeder Grundlage, basiert er doch ausschließlich auf unzuverlässigen Statistiken und Gerüchten. Kunden, die verdächtige Aktivitäten melden wollen, sollten sich direkt mit dem LifeThings-Kundendienst in Verbindung setzen.*

Auch diesmal enthielt die Äußerung von LifeThings keinerlei Angaben zu den Maßnahmen, die das Unternehmen ergriffen hatte, um die Angelegenheit zu untersuchen. Zum betreffenden Zeitpunkt gab es noch keine bekannte Möglichkeit, zur Meldung eines Sicherheitsproblems mit LifeThings Kontakt aufzunehmen.

Einige Wochen nach der Veröffentlichung von Goodins Artikel verfassten die erwähnten Sicherheitsforscher, die das Problem des unzuverlässigen Tokens veröffentlicht hatten, einen Blogpost, in dem sie behaupteten, über Beweise zu verfügen, dass sowohl die US-amerikanische als auch die chinesische Regierung in den Server *secure.lifethings.com* eingedrungen waren. Allerdings blieben sie sowohl den konkreten Nachweis als auch jede weitere Information zu der Frage schuldig, wofür die beiden Regierungen den Server ihrer Ansicht nach verwendet hatten.

Zwei Tage später setzte eine Hacktivistengruppe unter dem Twitter-Namen *@against_world_gov* folgenden Tweet ab:

> *Legt euch nicht mit uns an, LifeThings! Wir wissen, dass ihr mit der NSA die Privatsphäre der Menschen verletzt. Dieser DoS geht auf uns.*

Zum gleichen Zeitpunkt startete diese Gruppe einen Denial-of-Service-Angriff auf *secure.lifethings.com*, der dafür sorgte, dass kein einziges Gerät mehr über die LifeThings-Hubs bedient werden konnte. Die Reaktion von LifeThings erfolgte noch am gleichen Tag:

> *Wir untersuchen gegenwärtig eine laufende Denial-of-Service-Attacke gegen unser Netzwerk. Der Angriff hat dazu geführt, dass die LifeThings-Hubs nicht mehr reagieren. Wir sind entschlossen, die Täter zu finden und die Verfügbarkeit des Dienstes schnellstmöglich wiederherzustellen.*

Doch wie sehr sich LifeThings auch gemeinsam mit seinem Internetprovider bemühte, den Angriff abzuwehren, die Hacktivisten setzten ihn mit immer neuen Botnet-Armeen von unterschiedlichsten Standorten aus fort. Zwei Tage nach obiger Mitteilung gab LifeThings folgende Meldung heraus:

> *Wir bemühen uns, die Verfügbarkeit unserer Dienste wiederherzustellen. Unseren Kunden haben wir via E-Mail eine Anleitung zukommen lassen, in der Schritt für Schritt beschrieben wird, wie sie ihren LifeThings-Hub durch ein neues Gerät (»LifeThings2«) ersetzen, das für die gegenwärtigen Probleme nicht anfällig ist. Wir danken Ihnen für Ihre Geduld.*

Diese Äußerung von LifeThings veranschaulicht, dass das Unternehmen keine Möglichkeit vorgesehen hatte, seine Serverarchitektur zu ändern oder die Firmware auf bereits installierten Hubs zu aktualisieren und den laufenden Angriff auf diese Weise zu beenden. Die einzige Methode bestand darin, die alten Hubs gegen neue zu ersetzen. Zu diesem Zeitpunkt war nicht klar, welche zusätzlichen Sicherheitsmaßnahmen implementiert und welche Veränderungen an der Sicherheitsarchitektur des neuen Hubs vorgenommen worden waren.

Nur die wenigsten Kunden nahmen den Aufwand in Kauf, ihre Hubs per Post zurückzuschicken. Viele – darunter auch zahlreiche Prominente – zogen einfach buchstäblich den Stecker und beendeten ihr LifeThings-Abonnement. Schließlich wurde der Server *secure.lifethings.com* offline genommen, und die Geldgeber, die LifeThings bislang unterstützt hatten, weigerten sich, weitere Mittel in das Unternehmen zu investieren. Am Ende meldete LifeThings Insolvenz an.

Im Rückblick wird klar, dass die Entwickler der Architektur, in deren Mittelpunkt der Server *secure.lifethings.com* stand, eine Reihe bewährter Sicherheitsmethoden schlicht nicht beachtet hatten. Das Unternehmen bot Fachleuten keine Möglichkeit, Sicherheitslücken zu melden. Sogar nachdem die Sicherheitsexperten die Schwachstelle mit der gefälschten Rufnummer enthüllt hatten, richtete man bei LifeThings keinen konkreten Mechanismus ein, der den Empfang von Mitteilungen über Sicherheitslücken ermöglichte. Selbst die Analyse, mit der Stan Goodin nachwies, dass LifeThings entweder keine Ahnung oder aber kein Interesse daran hatte, Privatsphäre und Sicherheit seiner Kunden zu schützen, wurde einfach abgetan. Zudem war das Produkt nicht so entwickelt, dass es einen

Denial-of-Service-Angriff abwehren konnte; deswegen bestand die einzige Lösung in der Bereitstellung eines neuen physischen Hubs für jeden einzelnen Kunden. Die Kosten dafür wurden natürlich von LifeThings übernommen, das seine Kunden aufforderte, die alten Hubs zurückzusenden und neue einzubauen.

Aus dieser Geschichte lässt sich eine Menge lernen:

- Hersteller von IoT-Geräten und Plattformanbieter sind maßgeblich dafür verantwortlich, dass sich ihre Geräte remote aktualisieren lassen, um ggf. simple, aber effektive Angriffe abzuwehren.
- Wörter wie *secure* (oder *Sicherheit*) in Produkt- oder Servernamen sind keinesfalls ein Hinweis darauf, dass die zuständigen Techniker Erfahrung mit dem Entwickeln oder Implementieren sicherer Produkte und Konzepte haben. Alle Vorschläge für eine Architektur müssen von einer unabhängigen und qualifizierten externen Stelle geprüft und bewertet werden.
- Für Fachleute, die Sicherheitslücken und Schwachstellen melden wollen, muss ein eindeutig definierter Kommunikationsprozess vorhanden sein.
- Sicherheitsfragen, die von Experten aufgeworfen werden, müssen in jedem Fall beachtet und überprüft werden. Andernfalls kann nämlich eine einzige Schwachstelle – oder wie in diesem Fall eine ganze Reihe davon – zu schwerwiegenden geschäftlichen Einbußen führen und am Ende auch den Schutz zunichtemachen, der den Kunden versprochen wurde.

Jedes IoT-Gerät und jeder Plattformanbieter wird sich früher oder später in einer Situation wiederfinden, in der sich seine Architektur auf die eine oder andere Weise als unsicher erweist. Das oben beschriebene Szenario veranschaulicht in drastischer Form, wie ein dauerhaftes Vernachlässigen der notwendigen Sorgfalt dazu führen kann (und wird), dass die Kunden das Vertrauen verlieren und das Unternehmen deswegen vom Markt verschwindet.

9.3 Fazit

Die Behauptung, dass Situationen, die sich aus Sicherheitsproblemen ergeben, aufgrund der Absichten und Handlungen von Schlüsselpersonen einen bestimmten Verlauf nehmen können, haben wir anhand der beiden in diesem Kapitel beschriebenen Szenarios unterstrichen.

Im ersten Szenario wollte John Smith die Vorstandsmitglieder in seinem Unternehmen dadurch beeindrucken, dass er den Schwerpunkt auf Sicherheitsfragen im Zusammenhang mit IoT-Geräten legte. Allerdings lief dieser Ansatz den Interessen seines Arbeitgebers zuwider. Statt ein grundlegendes Verständnis für die Geschäftsinteressen und die technischen Risiken im Zusammenhang mit der Vision seines Unternehmens zu zeigen, wollte Smith nur über IoT reden, weil dies ein aktuelles Schlagwort war. Und auch wenn es in seiner Absicht lag, das Thema

vor allem zu nutzen, um vom Vorstand weitere Unterstützung und letztendlich auch die finanziellen Mittel zu erhalten, um ein noch besseres Team aufzubauen, wirkte er eher wie ein Mitarbeiter mit Selbstbedienungsmentalität, der sich ausschließlich auf seine eigenen Interessen und sein Fortkommen konzentriert, statt für das Unternehmen das Optimum herausholen zu wollen. Angesichts des gegenwärtigen Interesses am Internet of Things lohnt es sich sicher, über ein so wichtiges Szenario nachzudenken und daraus zu lernen. Natürlich empfiehlt es sich stets, über neue Technologien zu sprechen und für die Zukunft gerüstet zu sein, aber gleichermaßen wichtig – wenn nicht *noch* wichtiger – ist es, niemals das Unternehmen aus dem Blick zu verlieren, das man zu schützen versucht, und bei Bedarf eine ordentliche Sicherheitsstrategie vorzulegen, die mit den Zielen der Organisation im Einklang steht.

Im zweiten Szenario war der Firma LifeThings mit ihrer IoT-Plattform ein Coup gelungen, indem sie klug in neu gebaute Wohnkomplexe investierte. Allerdings hatte das Versprechen des Unternehmens, einen möglichst schnellen Kundendienst anzubieten, seinen Preis: Mit einer gefälschten übertragenen Rufnummer konnte ein Angreifer problemlos die Identität eines Kunden annehmen. Die Reaktion von LifeThings auf die Erkenntnisse von Sicherheitsfachleuten und Journalisten zeigte, dass das Unternehmen vor allem emotional reagierte. Das lag höchstwahrscheinlich daran, dass es dort niemanden gab, der in der Lage war, den Mitarbeitern die Wichtigkeit von Sicherheit und die hohe Bedeutung der kritischen Prozesse zu vermitteln, die für die Kommunikation mit Fachexperten, Journalisten und Kunden genau definiert sein müssen. Die Sicherheitsarchitektur der Plattform war zudem vollkommen unausgereift, und das Unternehmen zeigte sich weitgehend unfähig, bekannt gewordene Probleme zu beheben. Aufgrund des mangelnden Verständnisses und der fehlerhaften Entscheidungen aufseiten der Geschäftsführung von LifeThings wurde die Privatsphäre der Kunden beeinträchtigt, und es kam zu Diebstählen physischer Güter. All dies führte am Ende aufgrund finanzieller Schwierigkeiten zum Untergang des Unternehmens.

Anhand dieser beiden Szenarios lässt sich besser verstehen, warum sicherheitsrelevante Situationen mit den handelnden Personen stehen und fallen. Unternehmen müssen dafür Sorge tragen, dass sie geeignete Mitarbeiter beschäftigen – nämlich solche, die in der Lage sind, positive Ergebnisse sowohl für die Unternehmen selbst als auch für die Kunden zu erzielen.

Wir haben in diesem Buch eine ganze Reihe von bereits erhältlichen IoT-Produkten und die mit ihnen verbundenen Sicherheitsrisiken behandelt. Des Weiteren haben wir uns mit den Details der Entwicklung und des Prototypings neuer IoT-Geräte auseinandergesetzt und uns damit befasst, welche Arten von Angriffen für die verschiedenen Gefährder interessant sein könnten. Wir haben außerdem potenzielle zukünftige Angriffsvektoren beschrieben, die wir bei Entwicklung und Verwendung von IoT-Produkten berücksichtigen müssen. Abschließend haben wir nun gesehen, welchen Einfluss menschliches Handeln mit seinen Zie-

len, Absichten und Vorgehensweisen im Umgang mit sicherheitsrelevanten Vorfällen auf deren tatsächliche Folgen haben kann. Ich hoffe, dass ich Ihnen in diesem Buch ein grundlegendes Verständnis für die im Zusammenhang mit dem Internet of Things entstandene Bedrohungslandschaft vermitteln konnte und Sie nun in der Lage sind, unser aller Leben durch dieses Wissen sicherer zu gestalten, damit wir alle künftig von dieser Technologie profitieren und sie gewinnbringend nutzen können.