Alexander Straßheim, Sebastian Schreiber

IoT-Penetrationstest

Dieser Artikel befasst sich mit Schwachstellen in IT-Netzen, die durch unsichere IoT-Geräte verursacht werden. Er zeigt, wie IoT-Sicherheitstests zur Verbesserung der Anwendungssicherheit speziell im Internet beitragen können. Eine neu entdeckte Sicherheitslücke in einer Waschmaschine etwa erlaubt Zugriff auf den darauf laufenden Webserver. Das Problem ist dabei weniger die Lücke, als der Umgang des Herstellers damit.

Es wird nicht mehr lange dauern, bis tatsächlich alle unsere elektronischen Geräte im Haushalt über das Internet miteinander verknüpft werden können. Bluetooth, WLAN und Mobilfunk sind bereits in fast jedem Haushalt vorhanden. Das Internet der Dinge gewinnt immer mehr an Bedeutung und schleicht sich zunehmend in unseren Alltag ein. Unsere Haushaltsgeräte sollen Informationen nicht nur austauschen, sondern auch verarbeiten können. Unser Leben soll dadurch einfacher, schneller, komfortabler, vernetzbar und smarter werden. Analysten gehen davon aus, dass bis 2020 über 30 Milliarden Geräte mit dem Internet verbunden sein werden.

Entwickler von IoT-Geräten stehen vor der Entscheidung: Sollen sie vorhandene Geräte mit älteren Mikrocontrollern erweitern und so eine Internetverbindung und cloudbasierte Anwendungen ermöglichen, aber damit möglicherweise Sicherheitsrisiken in Kauf nehmen? Oder sollen sie neu entwickelte Mikrocontroller einsetzen, die eigens für IoT-Geräte ausgelegt sind? Denn an IoT-Geräte werden verschiedene Anforderungen gestellt. Hierzu gehören eine niedrige Energieaufnahme, hohe Rechenleistung, unterschiedliche Schnittstellen sowie – mit zunehmender Bedeutung – auch die Sicherheit.

Viele IoT-Geräte werden mit Akkus betrieben. Dabei wird viel Wert auf eine lange Betriebszeit zwischen den Ladevorgängen gelegt. Aber auch bei netzbetriebenen Geräten möchte man eine geringe Energieaufnahme erreichen. Dies erlaubt den Entwicklern, die Größe des Gesamtgeräts und von Bauteilen – beispielsweise Kühlkörper – gering zu halten. Zahlreiche Sensoren und Eingabegeräte, etwa Berührungserkennung und Grafikdisplays, setzen eine enorme Rechenleistung voraus. Neben USB und Ethernet verwenden viele neue IoT-Geräte Funkverbindungen. Hierzu gehören vor allem Bluetooth Low Energie (BLW) und WiFi. Zu guter Letzt sollen IoT-Geräte auch die Privatsphäre des Benutzers wahren und gleichzeitig vor digitalen Angriffen, unbefugten Zugriffen oder Datenänderungen geschützt sein. Generell sind hierbei die Sicherheitsanforderungen an IoT-Geräte höher als an solche Geräte, die nicht mit dem Internet verbunden sind.

In jüngster Zeit sind vermehrt Meldungen zu lesen, bei denen Internet of Things (IoT)-Geräte für digitale Attacken missbraucht wurden. So nutzten Angreifer im Jahr 2016 tausende IoT-Geräte für Distributed Denial-of-Service (DDoS)-Angriffe aus und legten dadurch große Teile des Internets lahm. Von diesem Angriff waren auch Firmen wie Amazon, Netflix, Spotify, und Twitter betroffen, um nur einige größere Unternehmen zu nennen [1]. Für Hersteller und Dienstleister bedeuten derartige Angriffe und Ausfälle nicht nur einen Image-, sondern auch einen immensen wirtschaftlichen Schaden. IT-Sicherheitsforscher gehen davon aus, dass in Zukunft vergleichbare Distributed Denial-of-Service (DDoS)-Angriffe unter Ausnutzung von IoT-Geräten zunehmen werden [2].

1 Was ist das Internet of Things?

Die Kommunikation zwischen elektronischen Geräten hat sich längst etabliert, wenn auch meist nur in vereinfachter Form. Bestellen wir beispielsweise etwas über das Internet, so verfolgen wir unser Paket auf dem Smartphone und können zu jedem Zeitpunkt feststellen, wo es sich gerade befindet. Wird der Füllstand unserer Druckerpatrone unterschritten, kann der Drucker automatisch eine Nachbestellung auslösen. Bei den aufgezeigten Fällen ist noch immer eine menschliche Interaktion notwendig. Durch das Internet of Things (IoT) soll dieser Aufwand entfallen. IoT ist nicht nur in aller Munde, sondern umgibt uns mittlerwei-

Sebastian Schreiber

studierte Informatik, Physik, Mathematik und BWL an der Universität Tübingen. Noch während seines Studiums gründete er 1998 das IT-Sicherheitsunternehmen SySS GmbH in Tübingen. Als Sicherheitsexperte und Live-Hacker tritt er häufig öffentlich auf und zeigt, wie IT-Netze übernommen, Passwörter geknackt und Daten abgezogen werden können.
E-Mail: Sebastian.Schreiber@syss.de

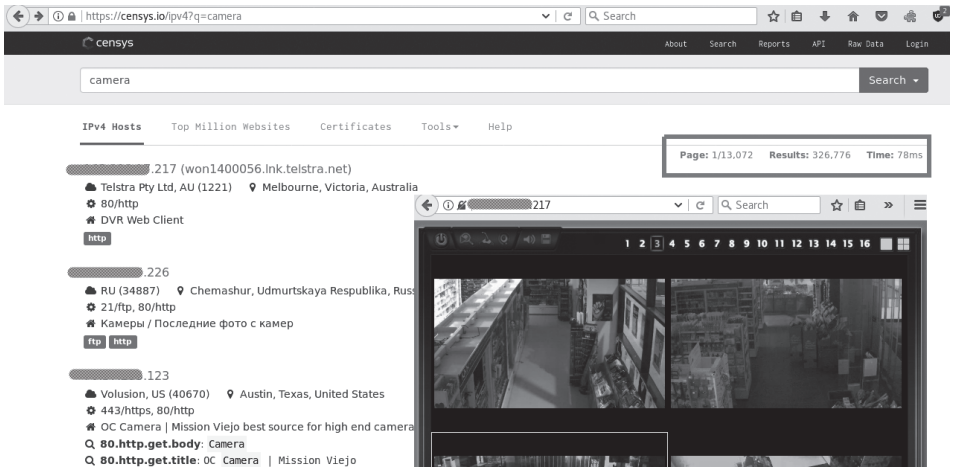
Alexander Straßheim

ist seit 2015 IT Security Consultant und Penetrationstester bei der SySS GmbH in Tübingen und auf Sicherheit von mobilen Apps und IoT-Geräten spezialisiert.

E-Mail: alexander.strassheim@syss.de

le auch im täglichen Leben. Sucht man gezielt nach einer Definition des Begriffs, so stellt man schnell fest, dass es mehr als eine Definition für IoT gibt [3]. Verschiedene Institutionen fassen diesen Begriff unterschiedlich auf, und man stolpert schnell von einem Schlagwort zum nächsten. Begriffe wie IoT, Industrie 4.0, M2M – die Vernetzung von Maschinen und Systemen kennt viele Bezeichnungen, die letztlich auf dieselbe Sache zielen: IoT bezeichnet die Kommunikation zwischen intelligenten Geräten ohne aktives Zutun des Menschen. Dabei ist anzunehmen, dass IoT-Geräte häufig eine IP-Adresse besitzen und als eigenständiges Gerät im lokalen Netz oder auch im Internet erreichbar sind. Das Internet of Things ist nicht nur eine Technologie, sondern es kombiniert eine ganze Reihe unterschiedlicher Technologien. Diese Geräte sind somit in der Lage, Daten zu erfassen, auszuwerten, auszutauschen und für weitere Aktionen zu verwenden. Diese Fülle an Möglichkeiten soll uns im Alltag begleiten und uns Arbeit abnehmen. Dies bedeutet aber zugleich, dass auch eine Reihe neuer digitaler Angriffsszenarien mit der raffinierten Technologieentwicklung einhergehen.

Abbildung 1 | Censys: IoT-Suchmaschine mit Gefahrenpotenzial



2 Verkannte Risiken des IoT

Dieser Artikel beschäftigt sich im Wortsinne mit IoT-Geräten, also „intelligenten" Geräten, die mit dem Internet verbunden sind und damit potenziell auch „von außen", sprich nicht nur innerhalb eines geschlossenen Firmennetzes angesprochen werden können. Dadurch entstehen neue Wertschöpfungsnetze, allerdings auch neue digitale Risiken. Mögliche Gefahren entstehen auf vier verschiedenen Ebenen [4]. Die erste Ebene ist die Hardwareebene. Sie bezieht sich auf die Interaktion des IoT-Geräts mit seiner Umgebung. Die Interaktion geschieht meist über Sensoren. So besteht die Möglichkeit, bestimmte Signalarten so zu manipulieren, dass Sensoren gestört werden und es zu Fehlfunktionen kommt [5]. Nicht auszuschließen ist, dass Angreifer bei Hardwarezugriff eventuell sensible Daten von dem Gerät entwenden können. Gefahren der zweiten Ebene, der Netzwerkebene, beziehen sich auf den Informationsaustausch zwischen den Komponenten. Es besteht die Möglichkeit, dass Angreifer die verwendete Software dazu bringen, ungewollte Aktionen auszulösen. Die Gefahren der dritten Ebene betreffen die Back-End- oder Cloud-Lösung, auf der unterschiedliche Dienste bereitgestellt werden. So können neben Vorgaben auch Daten gespeichert werden, die für das Funktionieren des IoT-Produkts notwendig sind. Diese können Schwachstellen enthalten, z. B. durch den Einsatz veralteter Software, durch die das IoT-Gerät für bösartige Aktionen missbraucht werden könnte. Die Applikationsebene bezeichnet die vierte Ebene und bezieht sich auf Schwachstellen in der Bedienung einer Webanwendung oder eines mobilen Geräts.

2.1 Verdeckte und offensichtliche Gefahren

Besitzer eines IoT-Geräts können sich schnell mit Malware infizieren. So waren zuletzt IP-Kameras von einer Schwachstelle betroffen, bei der die Infizierung nicht einmal zwei Minuten dauerte [6]. Die meisten dieser durch die in diesem Fall eingesetzte Malware „Mirai" verwundbaren Geräte besitzen keinen persistenten Speicher, sodass die Geräte nach Unterbrechen der Stromversorgung von der Malware befreit werden. Dies bietet jedoch auch keine dauerhafte Lösung, da diese Geräte nach kurzer Zeit wieder reinfiziert werden. Es ist prinzipiell sinnvoll, voreingestellte Passwörter der Geräte generell zu ändern.

So wurden Kunden der Deutschen Telekom erst kürzlich – im November 2016 – Opfer eines Botnetz-Angriffs und wären in diesem Zuge beinahe Bestandteil eines noch größeren Botnetzes geworden. Es wurde versucht, die Router über Port 7547 anzugreifen und sie mit dem Mirai-Botnetz zu verbinden. Wartungsserver können über diesen Fernwartungsport den Router kontaktieren und diesem mitteilen, dass ein Softwareupdate bereitsteht. Über diesen Weg wurde versucht, weitere Schadsoftware auf das Gerät zu bringen. Glücklicherweise funktionierte der Angriff nicht einwandfrei, sodass die ca. 900.000 angegriffenen Router der Telekom nicht für ein größeres Botnetz missbraucht werden konnten, sondern teilweise nur ausfielen [7]. Trotzdem entstand ein enormer wirtschaftlicher Schaden aufseiten der Telekom, für den der verantwortliche 29jährige Hacker aus Großbritannien Ende Juli 2017 vom Kölner Landgericht zu einem Jahr und acht Monaten auf Bewährung verurteilt wurde. Diese Attacke verdeutlicht, dass viele Angriffe für den einzelnen Benutzer nicht offensichtlich sind.

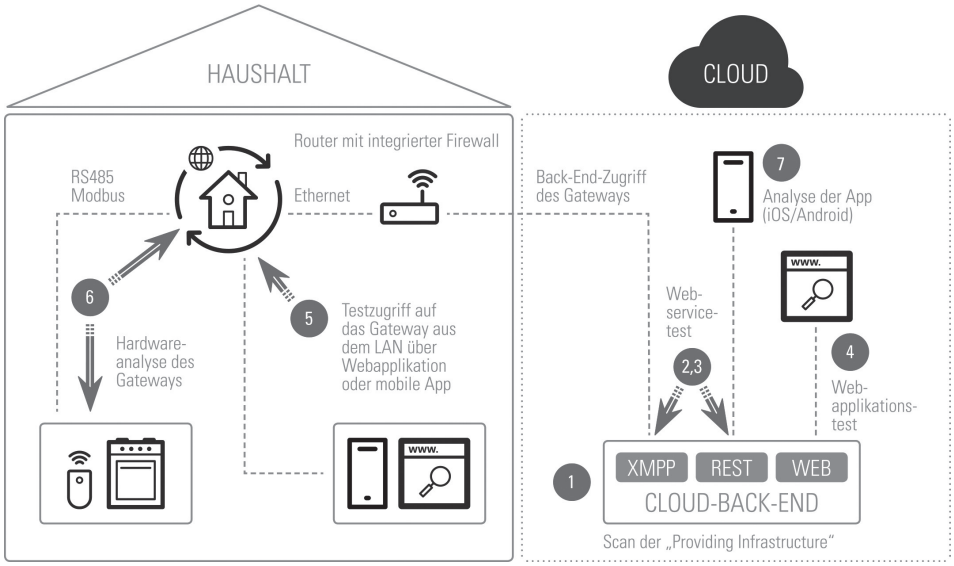
Mit den Suchmaschinen Shodan und Censys können viele IoT-Systeme gefunden werden. Es lassen sich sogar private Kameras, Wetterstationen, ja selbst Einrichtungen der öffentlichen Strom- und Wasserversorgung ansteuern.

Abbildung 1 zeigt die Suchmaschine Censys mit einer Suchanfrage zu IP-Kameras. Unzureichend geschützte Kameras können detailliert Einblick in die Privatsphäre geben. Jedoch lassen sich nicht nur IP-Kameras erkunden, sondern auch kritische Anlagensteuerungen, was ein immenses Sicherheitsrisiko darstellt. Gelangen solche Systeme in unbefugte Hände, kann dies erhebliche Folgen haben. Die Betreiber kritischer Infrastrukturen müs-

sen in Bezug auf die IT-Sicherheit insbesondere die Risiken der Vernetzung von Geräten beachten.

Die mit „Vault 7: CIA Hacking Tools Revealed" betitelte Wikileaks-Pressemitteilung beschreibt den Alptraum von Sicherheitsexperten: So sollen vernetzte Autos als potenzielles Mordwerkzeug verwendet werden [8]. In den geleakten Unterlagen der CIA stach besonders folgender Satz hervor: „Im Oktober 2014 wollte die CIA auch eine Fahrzeugsteuerung infizieren, wie sie moderne Autos und Lkw verwenden". Der Zweck einer solchen Kontrolle wird nicht genannt, aber sie würde es der CIA erlauben, nahezu nicht erkennbare Mordanschläge zu begehen [9]. In dem Dokument, das Wikileak als Quelle angibt, finden sich Überlegungen der CIA zu Angriffszielen bei IoT-Geräten. Es geht aus den Unterlagen jedoch nicht hervor, dass es dem Geheimdienst bereits gelungen ist, ein vernetztes Fahrzeug zu manipulieren und in die Steuerung einzugreifen. Dass dies jedoch möglich ist, zeigten die Sicherheitsexperten Charlie Miller und Chris Valasek beim Hack des Jeeps Cherokee von Chrysler im Jahr 2015. Interessant sind auch Angriffe auf das Unterhaltungssystem im Fahrzeug. So könnte beispielsweise der Standort des Fahrzeugs überwacht werden, ohne einen eigenen Sender anbringen zu müssen. Auch Mikrofone im Fahrzeug könnten angezapft und Gespräche der Insassen abgehört werden. Autobesitzer können sich selbst aktuell kaum gegen Angriffe schützen oder die IT-Sicherheit ihrer Autos verbessern. Jedoch ist es empfehlenswert, über ODBII laufende Diagnosesysteme nach Möglichkeit abzustecken, da über ODBII betriebene Stecker ein Einfallstor für Angriffe gegen das Fahrzeug darstellen.

Abbildung 2 | Komponenten des Internet of Things



Doch nicht immer benötigen Angreifer hochkomplexes Wissen über mögliche Angriffsvektoren. So staunte ein Smart Lock-Benutzer nicht schlecht, als plötzlich sein Nachbar auch ohne Schlüssel in der Wohnung stand. Mit Smart Lock lässt sich beispielsweise die Haustür über eine Smartphone-App steuern. Befindet sich nun das Smartphone (oder Tablet) im Haus und ist zusätzlich ein Sprachassistent aktiv, reicht ein gekipptes Fenster aus, um sich die Haustüre öffnen zu lassen. So verschaffte sich der Nachbar durch den Ruf „Hey Siri, unlock the front door" („Hey Siri, öffne die Haustüre") [10] Zutritt zur fremden Wohnung. Hierbei ist allein der Befehl ausschlaggebend, der Sprachassistent ist nicht fähig, Menschen anhand ihrer Stimme zu unterscheiden.

2.2 Testplan und simulierte Angriffe

Die Smart Home-Hersteller bemühen sich um eine leichte Handhabung der Geräte, auch ohne IT-Kenntnisse und auf Knopfdruck. Zudem sollen IoT-Geräte von überall steuerbar sein. Die Sicherheit bleibt da meist auf der Strecke. Die Gebrauchsanleitungen weisen nicht darauf hin, dass die notwendigen Einstellungen für die Geräte Löcher in die Firewall reißen, die uns eigentlich vor Angreifern aus dem Internet schützen soll, oder dass sensible Daten unverschlüsselt über das Internet übertragen werden.

Abbildung 2 zeigt das typische Set-up einer IoT-Hardware. Die dargestellten nummerierten Pfeile bezeichnen die Tests, die auch im Projektplan eines Penetrationstests verankert sind (vgl. Abbildung 3).

Die genaue Auswahl an Tests und Tools wird passend zum IoT-Gerät und dessen Anforderungen getroffen, da ein Penetrationstester seine Testzeit optimal ausschöpfen und möglichst viele Erkenntnisse gewinnen möchte. Es ist zudem wichtig, die Funde und erzielten Testergebnisse für den Auftraggeber genau zu dokumentieren und Empfehlungen für die Behebung von Schwachstellen auszusprechen, sodass der Auftraggeber das IT-Sicherheitsniveau nachhaltig steigern kann. Ist die Sicherheit des Gerätes auf einen Stand gebracht worden, die entsprechend der oben exemplarisch genannten oder anderer vergleichbarer Spezifikationen ausreichend ist, kann die Markteinführung beginnen.

Auf dem Back-End (1) laufen üblicherweise verschiedene Dienste. Diese können je nach Konfiguration Schwachstellen aufweisen oder auf veralteter Software basieren. Sind Schwachstellen vorhanden, besteht die Gefahr einer möglichen Rechteausweitung des Angreifers, die zur Kompromittierung des Systems führt. In der Folge ließe sich ein entsprechendes IoT-Gerät für bösartige Aktionen missbrauchen.

Die Interaktion von IoT-Geräten erfolgt meist in unterschiedliche Richtungen. So werden die Geräte häufig über Webapplikationen oder mobile Apps für Smartphones und Tablets bedient. Somit können der dahinterliegende Webservice sowie der Datenverkehr zum Back-End (2,3), aber auch die Applikation (4,5,7) selbst verwundbar sein und Schwachstellen aufweisen. Prinzipiell besteht die Gefahr, dass ein Angreifer mittels entsprechender Manipulation des Datenverkehrs in der Lage ist, die Software zu ungewollten Aktionen zu bringen. Ist das IoT-Gerät nicht in der Lage, die Legitimität einer Anfrage zu prüfen, steht das IoT-Gerät in der Folge unter der Kontrolle des Angreifers.

Auch die Herstellung und etwaige Implementierungsfehler in der Hardware (6) dürfen nicht außer Acht gelassen werden. Das denkbar schlimmste Szenario für Hersteller besteht in Angriffs-

Abbildung 3 | Testmodule

Teilprojekt	Modul	Zeitbedarf (in Personentagen)
Kick-off-Workshop (telefonisch)	KICKOFF	
1) Analyse Cloudsysteme (Infrastrukturtest) Alle an der Lösung beteiligten und über das Internet erreichbaren Serversysteme werden einer Sicherheitsanalyse unterzogen. Dazu setzt der Pentester sowohl unterschiedliche Securityscanner (z. B. Nessus, MaxPatrol, Saint) als auch Verwundbarkeitsscanner/Exploit-Sammlungen (wie z. B. Metasploit Framework) ein. Zudem werden bei Sicherheitstests im entsprechenden Kontext selbst entwickelte Softwaretools eingesetzt, wie beispielsweise Active Directory-Scanner, ShCoLo, FirePeek/FirePoke, Windows File System-Scanner, Windows Registry-Scanner und Wolpertinger. Manuelle und teilmanuelle Tests sind ebenfalls Bestandteil dieser Prüfung.	INTERNET	0,5
2) und 3) Prüfung des Webservice für a) App und b) Gateway Der Fokus dieses Tests liegt auf einer Sicherheitsanalyse des über XMPP kommunizierenden Webservice des Kunden, wie sie in den zur Verfügung gestellten Dokumenten dargestellt sind. Primäre Prüfgegenstände sind: 1) Schwächen in der Transportsicherung und Man-in-the-Middle-Manipulation legitimer Anfragen, insbesondere Überprüfung auf Anfälligkeit für einen Downgrade-Angriff 2) Eingabefilterung (z. B. auf SQL oder XPath Injection) 3) Autorisierung (Rechteausweitung, Zugriff auf fremde Daten,...) 4) XML-Parser (External Entities, XML Bomb, ...) Zwei Methoden kommen zum Einsatz: **1) Direkte Analyse der API** Der Kunde stellt eine Schnittstellendefinition zur Verfügung. Über direkte Zugriffe auf den Webservice werden Schwachstellen identifiziert. Ggf. wird hierzu ein eigener Client geschrieben. **2) Traffic Interception** Die Kommunikation zwischen Client und Webservice wird unter Anwendung eines Angriffsproxys aufgebrochen und so manipulierbar gemacht.	WEB-SERVICE	1,5
4) Analyse der Webapplikation: Einerseits wird die Existenz von Webschwachstellen (unter anderem die OWASP Top 10) aus der Perspektive eines unangemeldeten Angreifers sowie eines angemeldeten Nutzers geprüft. Andererseits wird ein Nachweis einer sicher verschlüsselten Datenübertragung erstellt. Zum Einsatz kommen Browsererweiterungen, spezielle Angriffsproxys sowie manuelle Prüfmethoden. Die Aufwände ergeben sich aus unserer Kalkulationsgrundlage Webapplikationstests (siehe nächster Abschnitt). **Bewertung der Applikation:** Schutzbedarf: hoch (im Internet exponiert) Komplexität: niedrig-mittel (wenig Funktionalitäten, kein Rechte- und Rollenkonzept)	WEBAPP	2
5) Analyse der Webapplikation auf dem Gateway: Einerseits wird die Existenz von Webschwachstellen (unter anderem die OWASP Top 10) aus der Perspektive eines unangemeldeten Angreifers sowie eines angemeldeten Nutzers geprüft. Andererseits wird ein Nachweis einer sicher verschlüsselten Datenübertragung erstellt. Zum Einsatz kommen Browsererweiterungen, spezielle Angriffsproxys sowie manuelle Prüfmethoden. Die Aufwände ergeben sich aus unserer Kalkulationsgrundlage Webapplikationstests. **Bewertung der Applikation:** Schutzbedarf: mittel Komplexität: niedrig	WEBAPP/ WEB-SERVICE	2
6) Hardwareanalyse des Gateways: Der Pentester wird die eingesetzte Hardware des Produkts analysieren. Neben weiteren werden die folgenden Aspekte beleuchtet: ▪ Hardwareinventarisierung (Identifikation eingesetzter Bauteile und vorhandener Schnittstellen wie JTAG, serielle Konsole/UART) ▪ Hardware-Debugging über die identifizierten Schnittstellen (z. B. Memory Dumps) ▪ Identifizierung und Analyse des Betriebssystems, eingesetzter Anwendungen, Dienstekonfigurationen und des Dateisystems ▪ Analyse auf Extraktionsmöglichkeiten eingesetzter Speicherkomponenten (z. B. Flash/SPI) Mögliche Tools für diese Testphase sind Bus Pirate, JTAGulator, Minicom/Screen, flashrom oder Logic Analyzer. ▪ Fahndung nach hinterlegten Credentials	PRODUCT	2
Dokumentation inkl. Executive Summary, Bewertung der Schwachstellen; zweistufige Qualitätssicherung	DOCU	2,5
Summe der Personentage:		**10,5**

szenarien, durch die sich Angreifer unautorisierte Zugriffsrechte auf dem Gerät verschaffen und eigenständigen Code auf dem Gerät zur Ausführung bringen. Auch die im Gerät verbauten Sensoren können angegriffen und manipuliert werden. In der Folge kommt es zu Fehlmessungen und Funktionsstörungen. So können nicht nur Signale zwischen Sensor und Gateway, sondern auch zwischen Gateway und Back-End angegriffen werden. Dies hätte zur Folge, dass das IoT-Gerät ungewollte Aktionen durchführt.

3 Maßnahmen & Konzeption

Angriffe wie die aus dem Jahr 2016, bei denen eine enorme Anzahl an verwundbaren IoT-Geräten für DDoS-Angriffe ausgenutzt wurden, zeigen einen deutlichen Handlungsbedarf, wenn es um IoT-Sicherheitslösungen geht. Häufig fehlt den Herstellern das Bewusstsein, dass neben der Funktionalität der Geräte auch die Sicherheit einen enormen Stellenwert hat. Eine Analyse unterschiedlicher Geräte zeigt, dass Produkte teilweise nur begrenzte oder sogar überhaupt keine Sicherheitsmechanismen besitzen. In der Regel benötigen Angreifer nur eine einzige Lücke, um ein verwundbares System zu kompromittieren [11]. Es ist essenziell wichtig, dass die Hersteller ein ausgeprägtes Sicherheitsbewusstsein entwickeln. Erst wenn diese Voraussetzung geschaffen worden ist, können im nächsten Schritt konkrete Maßnahmen umgesetzt werden.

IT-Sicherheit sollte fester Bestandteil der Planungs- und Entwicklungsphase sein. Passende Architekturen und geeignete sicherheitsbezogene Entwurfsentscheidungen müssen schon frühzeitig in den Entwicklungsprozess einfließen, um eventuelle Folgekosten zu minimieren.

Angriffsflächen lassen sich beispielsweise minimieren, indem vor dem Entwicklungsprozess entschieden wird, welche Komponenten für den tatsächlichen Betrieb des Geräts benötigt werden. Kostendruck bei der Entwicklung und Produktion ist ein entscheidender Faktor. Bietet ein Hersteller mehrere Ausstattungsvarianten an, so wird mit hoher Wahrscheinlichkeit nicht für jede Variante eine eigene Platine entwickelt und bestückt. Alle Erweiterungsmodule sind mit zusätzlichen Kosten verbunden. So sind beispielsweise Steckverbinder sehr teuer, ganz zu schweigen von aufwendigerer Fertigung, Montage und Wartung [12]. Der Hersteller ist meist in erster Linie bemüht, einheitliche Bauteile in großer Stückzahl zu fertigen, um Kosten zu sparen. Die Ausstattung unterscheidet sich oft in der Firmware, die in den günstigen Varianten einige Funktionen ungenutzt lässt.

Bereits während der Konzeptionsphase eines IoT-Geräts sollten die grundlegenden Funktionsbestandteile auf deren Sicherheit hin befragt werden. Gerade die Kommunikation zwischen den beteiligten Schnittstellen und deren Absicherung ist hier ein neuralgischer Punkt. Dabei ist etwa zu beachten, dass Signale und

Anfragen manipuliert sein könnten oder dass diese eventuell aus einer anderen, nicht zum Gerät gehörenden Quelle stammen.

Es sollte soweit wie möglich sichergestellt werden, dass unautorisierte Daten zurückgewiesen werden.

4 Markteinführung

Es ist wichtig, das Produkt vor der Markteinführung einem Sicherheitstest durch einen unabhängigen Dienstleister zu unterziehen. Ziel eines Sicherheitstests ist es, mögliche Schwachstellen aufzudecken und Wege zur Behebung aufzuzeigen. Führende Sicherheitsorganisationen haben spezifiziert, wie ein Sicherheitstest und die Dokumentation zu gestalten sind. Ist vor der Markteinführung kein Sicherheitstest durchgeführt worden, sollte dieser unbedingt nachgeholt werden. Auch wenn bei der Entwicklung die zum Zeitpunkt gängigen Sicherheitsvorkehrungen getroffen wurden, gibt es letztlich keine hundertprozentige Garantie, dass das Endprodukt frei von Sicherheitsproblemen ist. Neue Sicherheitslücken werden regelmäßig entdeckt und veröffentlicht. Möchte der Hersteller das Vertrauen der Kunden gewinnen, so ist es wichtig, offen mit aufgedeckten Schwachstellen umzugehen. Werden öffentlich bekannte Lücken behoben und Sicherheitsupdates zur Verfügung gestellt, ist es weniger wahrscheinlich, dass Angreifer eine Schwachstelle erfolgreich ausnutzen können.

So hat beispielsweise auch das Unternehmen Somfy, das Antriebs- und Steuerungstechnik für Rolläden, Sonnenschutz, Garagen- und Hoftore entwickelt und vertreibt, sich einer Sicherheitsprüfung unterzogen. Gestetet wurde das Produkt TaHoma® Connect. So konnten noch vor Produkteinführung einige Schwachstellen aufgezeigt werden, die dann zur eigentlichen Markteinführung bereits behoben waren. Dem Unternehmen Somfy konnte nach der IoT-Sicherheitsprüfung für TaHoma® Connect ein Zertifikat ausgestellt werden, das eine hohe Datensicherheit bescheinigt.

5 Fazit

Noch immer ist das Bewusstsein für potenzielle Gefahren bei Internet of Things (IoT)-Geräten nicht groß genug. Hersteller verschweigen zum Teil die Risiken, die der Kunde durch den Einsatz von IoT-Geräten eingeht. In Bedienungsanleitungen und auf Verpackungen wird in der Regel nicht auf versteckte Funktionen, Dienste und womöglich vorhandene Sensoren hingewiesen. Ein IoT-Gerät ist für den Kunden eine Blackbox, deren exakte Funktionen und Sicherheit er nicht überblicken kann. IoT-Geräte sollten grundsätzlich in einem separaten Netzwerk isoliert werden, da sie eine nicht einzuschätzende Gefahr für das lokale Netzwerk darstellen, in dem sich private Dokumente, Videos und Bilder befinden.

Arne Schönbohm, der Chef des Bundesamts für Sicherheit in der Informationstechnik, regt an, ein Mindesthaltbarkeitsdatum für IT einzuführen. So sollen Hersteller von Soft- und Hardware einen einwandfreien Zustand garantieren und bei Mängeln haften. Somit stünden Hersteller in der Pflicht, die Sicherheit der bereitgestellten Produkte für einen bestimmten Zeitraum zu gewährleisten. Dem Kunden soll damit verdeutlicht werden, dass das eingesetzte Produkt ein Verfallsdatum hat und er nach Ablauf dessen selbst für die Sicherheit sorgen muss [13]. Es stellt sich die Frage, wie die Installation von Sicherheitsupdates auszusehen hat und wer die Verantwortlichkeit übernimmt. Soll der Haushalt, sprich der Nutzer eines solchen IoT-Geräts das Sicherheitsupdate selbst installieren? Übernimmt diesen Prozess der Hersteller oder der Verkäufer?

Zwar wäre ein solcher Vorschlag wünschenswert, jedoch nur schwer umsetzbar, da der Markt global und intransparent ist.

IoT-Sicherheit hat nach dem IoT-Botnetz Mirai oder dem Chrysler-Hack an Bedeutung gewonnen. Hersteller namhafter Produkte geben der Sicherheit ihrer Geräte eine höhere Priorität, da ein erfolgreicher Angriff nicht nur einen immensen wirtschaftlichen, sondern auch einen erheblichen Imageschaden für das entsprechende Unternehmen bedeutet.

Literatur

[1] B. Chacos, "Major DDoS attack on dyn DNS knocks spotify, twitter, github, PayPal, and more offline. PCWorld," 21-Oct-2016. [Online]. http://www.pcworld.com/article/3133847/internet/ddos-attack-on-dyn-knocks-spotify-twitter-github-etsy-and-more-offline.html. [Accessed: 11-Jul-2017].

[2] M. Orcutt, „Lebensgefährliches Internet der Dinge? Technology Review," 7-Dec-2017. [Online]. https://www.heise.de/tr/artikel/Lebensgefaehrliches-Internet-der-Dinge-3562468.html. [Accessed: 11-Jul-2017].

[3] F. Lindner, „IoT Definitionen: Was ist eigentlich das Internet der Dinge?" [Online]. https://www.expertenderit.de/blog/iot-definitionen-was-ist-eigentlich-das-internet-der-dinge. [Accessed: 11-Jul-2017].

[4] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: A review," in 2012 international conference on computer science and electronics engineering, 2012, vol. 3, pp. 648–651. [Auch online]. https://www.researchgate.net/publication/254029342_Security_in_the_Internet_of_Things_A_Review. [Accessed: 11-Jul-2017].

[5] Y. Son et al., "Rocking drones with intentional sound noise on gyroscopic sensors," in Proceedings of the 24th USENIX conference on security symposium, 2015, pp. 881–896. [Auch online]. https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-son.pdf. [Accessed: 11-Jul-2017]

[6] H. Gierow, „Mirai-IoT-Botnet: IP-Kamera nach 98 Sekunden mit Malware infiziert", golem.de, 21-Nov-2016. [Online]. https://www.golem.de/news/mirai-iot-botnet-ip-kamera-nach-98-sekunden-mit-malware-infiziert-1611-124602.html. [Accessed: 11-Jul-2017]

[7] „Telekommunikation: BSI: Bei Angriff auf Telekom 'noch einmal Glück gehabt'," Die Welt, 29-Nov-2016. [Online]. https://www.welt.de/newsticker/dpa_nt/afxline/topthemen/article159833020/Bei-Angriff-auf-Telekom-noch-einmal-Glueck-gehabt.html [Accessed: 11-Jul-2017].

[8] F. Greis, "Vault 7: CIA hacking tools revealed" [Online]. https://www.wikileaks.org/ciav7p1/. [Accessed: 11-Jul-2017].

[9] „Vault 7: Was macht die CIA mit gehackten Autos?", golem.de, 9-Mar-2017. [Online]. https://www.golem.de/news/vault-7-was-macht-die-cia-mit-gehackten-autos-1703-126639.html. [Accessed: 11-Jul-2017].

[10] C. Wisniewski, "Siri opens 'smart' lock to let neighbor walk into a locked house," 22-Sep-2016. [Online]. https://nakedsecurity.sophos.com/2016/09/22/siri-opens-smart-lock-to-let-neighbor-walk-into-a-locked-house/. [Accessed: 11-Jul-2017].

[11] S. Schreiber, "Der Penetrationstest als Instrument 7 der Internen Revision", in A. Sowa, P. Duscha, and S. Schreiber, IT-Revision, IT-Audit und IT-Compli- ance. Wiesbaden: Springer Fachmedien Wiesbaden, 2015, S. 151–183

[12] M. Dölle, J. v. Malottki, „Digitaler D-Day – Installationswege und versteckte Funktionen gefährden Privatsphäre und Sicherheit", c't, 31-Mar-2017. [Online]. https://www.heise.de/ct/ausgabe/2017-8-Installationswege-und-versteckte-Funktionen-gefaehrden-Privatsphaere-und-Sicherheit-3665522.html. [Accessed: 11-Jul-2017].

[13] „BSI-Chef: IT-Mindesthaltbarkeitsdatum würde wichtige Signale setzen," 21-May-2017. [Online]. http://winfuture.de/news,97748.html.