Risiko Smart Home – Angriff auf ein Babymonitorsystem

Gregor Bonney · Stefan Nagel · Marko Schuba

FH Aachen
gregor.bonney@alumni.fh-aachen.de
{nagel | schuba}@fh-aachen.de

Zusammenfassung

Unser Zuhause wird zunehmend intelligenter. Smart Homes bieten uns die Steuerung von Haus- oder Unterhaltungstechnik bequem vom Smartphone aus. Junge Familien nutzen die Technologie, um mittels vernetzten Babymonitorsystemen ihren Nachwuchs von überall aus im Blick zu haben. Davon auszugehen, dass solche Systeme mit einem Fokus auf Sicherheit entwickelt wurden, um die sehr persönlichen Daten zu schützen, ist jedoch ein Trugschluss. Die Untersuchung eines handelsüblichen und keineswegs billigen Systems zeigt, dass die Geräte sehr einfach kompromittiert und missbraucht werden können.

1 Einleitung

In den letzten Jahrzehnten ist eine nachhaltige Wandlung technischer Systeme zu beobachten. Während vor 30 Jahren fast ausschließlich isolierte Geräte betrieben wurden, die bestenfalls nur für spezifische Kommunikationsdienste oder Einwahlleitungen verbunden wurden, ist heute der Begriff „always-on" in vielen Bereichen schon in die Realität umgesetzt. Dabei geht es nicht nur um Menschen, die kommunizieren, sondern zunehmend um Systeme, die untereinander Daten austauschen. Dies wird durch den Begriff Internet der Dinge (Internet of Things, IoT) beschrieben, bei dem Objekte durch Internet-ähnliche Strukturen verknüpft und Informationen ausgetauscht werden [Asht09].

Die zunehmende Vernetzung und Automatisierung vieler Teilbereiche unseres Lebens führt zu einer steigenden Abhängigkeit von der Verfügbarkeit und Integrität der Systeme und Daten. Und nicht nur im beruflichen sondern auch im privaten Bereich ist die Authentizität und Vertraulichkeit wichtiger Informationen von hoher Bedeutung. Ein Bereich der für Privatpersonen gleichzeitig attraktiv wie auch risikoreich ist, ist die Heimautomatisierung, häufig mit dem Begriff Smart Home bezeichnet [Harp03]. Hierbei geht es insbesondere um die Steuerung und Überwachung von Haustechnik, aber auch um Unterhaltungs- und Komfortfunktionen. Viele der Anwendungen bzw. Systeme werden dabei bequem über die App eines Smartphones gesteuert. Die zunehmende Komplexität und Vernetzung der Systeme in unserem Zuhause erhöht das Gefährdungspotential für unsere Informationen, sei es durch gezielte Angriffe oder durch technische Ausfälle. Weiterhin führt die vernetzte Gewinnung, Speicherung und Verarbeitung personenbezogener Daten zu einer stetig wachsenden Bedrohung der Privatsphäre.

In diesem Paper wird beispielhaft gezeigt, wie einfach der Angriff auf eine Anwendung (konkret ein Babymonitorsystem) innerhalb eines Smart Homes sein kann. Dabei wird deutlich, dass Systeme, die viele Anwender bedenkenlos in ihr Smart Home integrieren, durch die Vernetzung

P. Schartner (Hrsg.) · D•A•CH Security 2016 · syssec (2016) 371-378.

mit dem Internet ein Risiko für sehr intime Informationen sowie einen Einstiegspunkt für die weitere Kompromittierung des Smart Homes darstellen.

2 Monitorsysteme für Babies

Eine der vielen Anwendungen, die sich heutzutage in vielen Haushalten mit kleinen Kindern findet, ist ein Monitorsystem. Das Babyfon früherer Jahre hat sich zu einem High-Tech-System entwickelt [CHIP15]. Neben der Übertragung des Tons erlauben moderne Systeme das Gegensprechen, die Videoübertragung von Bildern mehrerer Kameras, die entfernte Steuerung der Kameras, die Aufnahme von Videos und Bildern, die Einbindung in das heimische Netzwerk via WLAN oder Powerline, die Messung der Raumtemperatur oder das Abspielen von Audiodateien wie z.B. Schlafliedern. Die Anzeige und Steuerung erfolgt dabei entweder über proprietäre Geräte oder über eine Smartphone-App. Je nach System ist eine solche Steuerung auch von außen, d.h. vom Internet aus möglich. Der allgemeine Trend, nützliche Dinge unseres Alltages mit IT-Funktionalität zu erweitern, führt vor allem auch dazu, dass das Internet immer mehr Einfluss auch auf die Geschäftsmodelle großer Firmen nimmt [FlWe14]. Um langfristig wettbewerbsfähig zu bleiben, werden immer mehr Firmen IoT-Produkte herstellen, was die Angriffsfläche auf die IT-Geräte in unserem alltäglichen Umfeld erweitern wird.

Dass Babymonitorsysteme Schwachstellen aufweisen, die von Angreifern ausgenutzt werden können, ist nicht neu. In einer Studie zeigte die Firma Rapid7 im vergangenen Jahr Schwachstellen verschiedener Systeme, die zum Teil entfernt, d.h. über das Internet ausgenutzt werden können [StBe15]. Das Aufdecken der Schwachstellen war dabei in vielen Fällen trivial. Die gezeigten Angriffe waren meist darauf zurückzuführen, dass der Zugriff auf das Gerät entweder über ein unverschlüsseltes Protokoll erfolgte, bzw. die auf den Geräten vorhandenen Passwörter entweder nicht geändert wurden bzw. leicht zu erraten waren. Einige Sicherheitsprobleme basierten auch auf Schwachstellen zugekaufter Software, deren Existenz schon länger bekannt war. Insgesamt offenbart die Untersuchung, dass die Handhabung von Sicherheit bei Babymonitorsystemen, obwohl dies ein sehr sensibler Bereich ist, bei vielen Herstellern noch keine hohe Priorität hat.

Die Konsequenzen eines Angriffs auf ein Babymonitorsystem können vielfältiger Natur sein. Zum einen kann ein Angreifer Video- und Audio-Informationen abgreifen. Unterstützt das Gerät Gegensprechen oder das Abspielen von Audio-Dateien, kann ein Angreifer direkt in das entsprechende (Kinder-)Zimmer kommunizieren, was sehr beängstigend sein kann. Im schlimmsten Fall kann der Benutzer die komplette Kontrolle des Geräts übernehmen und somit weitere Angriffe innerhalb des Heimnetzwerks starten. Dass die Sicherheit zunehmend schlechter wird bzw. es immer mehr angreifbare Geräte gibt, zeigt sich auch auf Webseiten wie „shodan.io“ [Shod16], auf der seit Anfang des Jahres eine Sektion existiert, in der man sich Bilder von schlecht gesicherten Kameras anschauen kann. Darunter zu finden sind auch Bilder von Babykameras [Poru16].

3 Das Babymoov-System

Das Babymoov-System besteht aus zwei Komponenten: Eine Netzwerkkamera, die im Kinderzimmer angebracht wird, und eine iOS- oder Android-App zum Betrachten des Videostreams [Baby16]. Angeschlossen wird die Kamera mit einem USB3.0 Kabel, das gleichzeitig der

Stromversorgung dient und eine integrierte Netzwerkverbindung bietet. Dieses Kabel wird direkt mit einem Powerline Adapter verbunden. Ein weiterer Powerline Adapter bietet einen Netzwerkanschluss zum direkten Anbinden an das Heimnetzwerk (vgl. Abbildung 1).

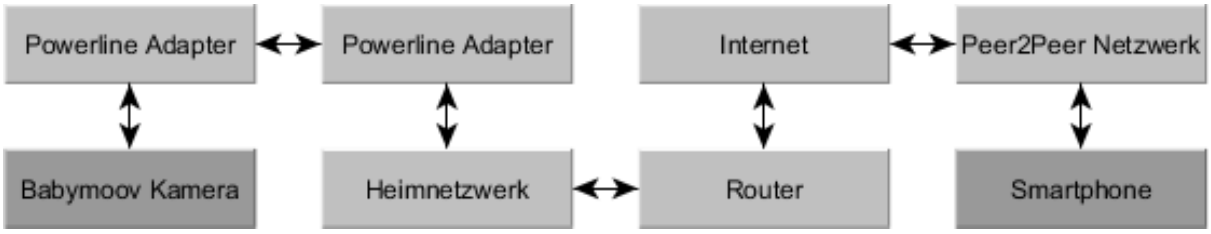

Abb. 1: Der Netzaufbau des Babymoov-Systems

Die Kamera verfügt neben der Möglichkeit, Video- und Tonsignale per App zu empfangen, über zahlreiche weitere Features, wie z.B. einen Sensor zur Überwachung der Raumtemperatur, ein RGB-Nachtlicht, eine Gegensprechfunktion, einen MP3-Upload und automatische Benachrichtigungen anhand konfigurierbarer Bewegungs- oder Ton-Events.

Die Hardware der Kamera ist ein von Elansat produzierter Chipsatz, auf dem GNU/Linux mit Busybox als Betriebssystem zum Einsatz kommt. Die Smartphone-App wird ebenfalls durch den Technologiezulieferer bereitgestellt.

3.1 Verbindungsaufbau zwischen App und Kamera

Der erste Verbindungsaufbau zwischen Kamera und Smartphone-App erfolgt durch das Einscannen eines auf der Kamera befestigten QR-Codes. Der QR-Code kodiert eine 20 Zeichen lange „UID“ gefolgt von einem Semikolon und einem Leerzeichen sowie der Zeichenkette „12345678“. Letztere repräsentiert das Passwort. Nach erfolgreichem Aufruf des QR-Codes wird das Video- und Audiosignal über einen Peer-to-Peer Cloud-Service zum Smartphone übertragen. Das Passwort lässt sich zwar über Optionen der App ändern, der entsprechende Hinweis wird aber nur einmalig und unscheinbar am unteren Bildschirmrand eingeblendet (siehe Abbildung 2). Dies erfolgt zudem zu einem Zeitpunkt, an dem der Kunde gerade darauf fokussiert ist, den QR-Code einzuscannen, weshalb der Hinweis sehr leicht übersehen werden kann.

3.2 Freigabefunktion der Kamera

Damit Verwandte und Bekannte ebenfalls das Kind betrachten können, bietet die App die Möglichkeit, für einen zeitlich beschränkten Zeitraum den Zugriff auf die Kamera freizugeben. Hierzu wird eine E-Mail mit einem speziellen Link vorformuliert, sodass diese lediglich an den ausgesuchten Empfänger versandt werden muss. Erhält dieser anschließend den Link auf sein Smartphone und ist die App ebenfalls installiert, so wird die Kamera in der App eingerichtet, sobald der Nutzer den Link anklickt.

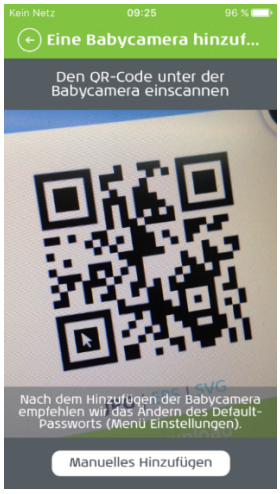

Abb. 2: Für Benutzer leicht zu übersehen: Aufforderung das Verbindungsaufbau-Passwort zu ändern

4 Analyse des Babymoov-Systems

4.1 Portscan und Services

Da die Kamera „Cloud-Services“ nutzt, ist eine Netzanbindung mit IP-Adresse Grundvoraussetzung. Ein Portscan des Geräts zeigt vier offene Ports, darunter ein Webserver auf Port 80, Telnet auf Port 23 und zwei offene UDP Ports: 48206 und 32761. Hier werden zunächst der Webserver- und der Telnet-Port betrachtet.

4.1.1 Webserver mit verstecktem Admin-Interface

Der Webserver auf Port 80 antwortet auf der Index-Seite mit einem „HTTP 200 OK“. Der Inhalt erscheint zunächst harmlos als „nicht gefunden“-Fehlerseite. Eine genauere Betrachtung zeigt jedoch, dass ein in der Seite versteckter Link zur Kamera-Administrationsoberfläche des Herstellers führt (Abbildung 3).

Die Administrationsoberfläche bietet verschiedene Optionen der Parametrisierung und ein Live-Bild der Kamera an. Ein dort vorhandener Link namens „Show all parameters“ offenbart eine Liste aller Einstellungen und zeigt hierbei unter anderem die URL zur Geräte-Firmware an.

Abb. 3: Versteckter Link unter dem Punkt in "File not fond [sic!]."

4.1.2 Telnet

Der Telnet-Dienst ermöglicht dem Benutzer „root“ bei Kenntnis des Passworts den Zugang zum Gerät. Bedingt durch uneingeschränkte Rechte dieses Benutzers sind Manipulationen aller

Art möglich. In dem Benutzerhandbuch zur Kamera ist kein Hinweis auf einen laufenden Telnet-Dienst vorhanden, stattdessen wird der Funktionsumfang der Kamera beschrieben. Das root-Kennwort lässt sich durch einen versierten Benutzer zwar mit dem Befehl „passwd“ ändern, wird nach einem Neustart jedoch auf das ursprüngliche zurückgesetzt.

4.2 Firmware

Als nächstes wird die Firmware der Kamera betrachtet. Mit dem Analyse-Tool Binwalk können Binärdateien (z.B. einer Firmware) auf ihre Zusammensetzung hin untersucht werden [Binw16]. Angewendet auf die Firmware der Kamera findet das Tool ein ZLIB-komprimiertes Archiv und kann es entpacken. Die Analyse des entpackten Archivs zeigt weitere versteckte Webseiten des Kamera-Webservers sowie den Inhalt der Passwortdatei „/etc/shadow“ des GNU/Linux Betriebssystems. Interessant ist die Tatsache, dass keinerlei Verschlüsselungsbibliotheken enthalten sind. Aus dem in der Passwortdatei enthaltenen MD5-Passworthash (vgl. Abbildung 4) kann mit dem Tool hashcat das zum Benutzer „root“ gehörende Klartextpasswort „ipad“ ermittelt werden [Hash16].

```
[root@WiCam]# cat /etc/shadow
root:$1$QJU2u3Iz$w6r6WdTmNL7Va5155QmD81:0:0:99999:7:::
[…]
```

Abb. 4: Gekürzte Ausgabe des Dateiinhalts der „/etc/shadow“.

4.3 Google Cloud Messaging

Der Server, über den die Firmware bezogen werden kann, erlaubt das Anzeigen von Verzeichnisinhalten. Durch gezieltes Browsen auf eine höhere Ebene, wird ein Interface zur Kommunikation mit Endgeräten über „Google Cloud Messaging“-Dienste angezeigt (vgl. Abbildung 5).

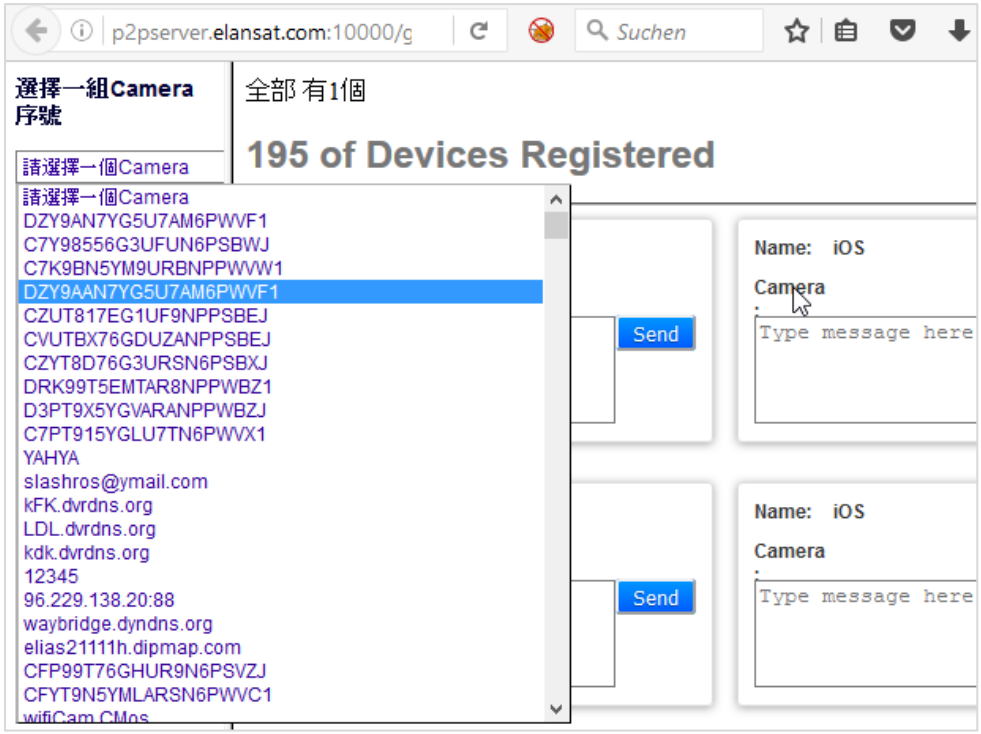

Abb. 5: Mehrere tausend UIDs sind aufgelistet.

Auf der linken Seite des Interfaces kann – wie in der Abbildung markiert – eine Kamera über ihre UID ausgewählt werden. Nach Selektion kann über die rechte Seite des Framesets eine Nachricht zum verbundenen Smartphone gesandt werden. Zum Zeitpunkt der Untersuchung wurden ca. 3600 UIDs auf dieser Seite aufgelistet. Ein Login ist nicht nötig.

4.4 Peer-to-Peer Netzwerk

Damit der Nutzer des Kamerasystems den Funktionsumfang der Kamera ohne Änderungen an Router- bzw. Firewall-Freigaben über jeden freien Internetzugang nutzen kann, verbindet die Kamera sich mit einem Peer-to-Peer Netzwerk, welches den Audio- und Videostream zur App auf dem Smartphone des Nutzers weiterleitet. Die Streams werden hierbei per UDP auf den Zielport 10001 versandt. Interaktionen auf dem Smartphone, wie das Setzen einer neuen Nachtlichtfarbe oder aber das Ändern des Zugangskennworts werden ebenfalls über das Netzwerk transportiert.

5 Angriffsmöglichkeiten

Bedingt durch die Liste der UIDs auf der Herstellerwebseite, den laufenden Telnet-Dienst und die „Kamerafreigabe“-Funktion, bietet das Babymoov-System mehrere Angriffsvektoren (vgl. Abbildung 6).

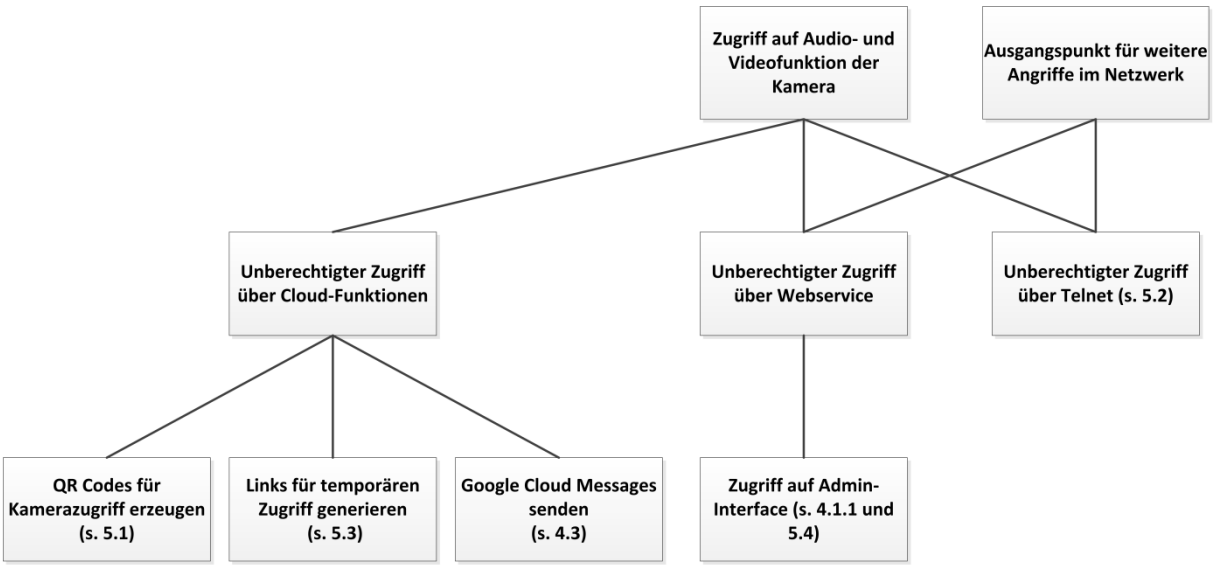

Abb. 6: Angriffsbaum für Babymoov Kamera.

5.1 Erstellen eines eigenen QR-Codes

Wird ein QR-Code durch einen Generator mit einer UID aus der Liste und dem Standard-Kennwort „12345678“ generiert, so ist es möglich auf fremde Kameras Zugriff zu erhalten, sofern das Kennwort nicht verändert wurde.

5.2 Telnet kann Kamera kompromittieren

Ist die Kamera direkt an das Internet angeschlossen, so ist der Telnet-Zugang öffentlich erreichbar. Diverse Geräte werden unter anderem auf Shodan gelistet und erlauben das Einloggen mit dem Benutzer „root“ und dem Kennwort „ipad“ [Shod16].

5.3 Kamerafreigabe nutzt symmetrischen AES Schlüssel

Die „Kamerafreigabe“-Funktion erlaubt den Zugriff durch andere für einen eingeschränkten Zeitraum. Der in der vorformulierten E-Mail erzeugte Link enthält hierbei einen Parameter, der mittels dem symmetrischen Schlüssel „BaByMoOvMissKeY9“ zurückberechnet werden kann. Hierbei werden die UID und das Verbindungspasswort sowie der Zeitstempel, an dem der Zugang ablaufen soll, in Klartext angezeigt. Die zeitliche Einschränkung lässt sich dadurch umgehen, dass mittels der gewonnenen Information ein QR-Code generiert und anschließend per App eingescannt wird.

5.4 Den Besitzer aussperren

Die Kamera bietet gemäß dem Benutzerhandbuch keine Option an, das einmal vergessene Kennwort wiederherzustellen oder zurückzusetzen. Ob ein Firmware-Update die Konfiguration auf die Werkseinstellung zurücksetzt, ist unklar. Sobald ein Angreifer das Kamerasignal erfolgreich per App erlangt hat, kann dieser das Zugangskennwort abändern und somit die legitimen Nutzer aussperren. Über das versteckte Administrationsinterface ist ein Neusetzen des Kennwortes jedoch möglich.

6 Zusammenfassung

Babymonitorsysteme stehen beispielhaft für einen sensiblen Anwendungsbereich im Smart Home, oder noch allgemeiner, im Internet of Things. Sicherheitstechnisch sind viele der Systeme jedoch nicht ausreichend gut aufgestellt. In diesem Beitrag wurde gezeigt, wie einfach eine moderne Kamera des Herstellers Babymoov erfolgreich angegriffen werden kann. Als Resultat können bei Systemen, die mit dem Internet verbunden sind, nicht nur Bilder und Töne der Systeme von jedermann abgegriffen werden, sondern es wird auch der Zugriff auf das Gerät und so eine Vielzahl von Manipulationen möglich. Der Hersteller des Systems wurde auf Basis eines Responsible Disclosure Prozesses informiert.

Grundsätzlich sollten Hersteller von IoT-Geräten keine unsicheren oder veralteten Techniken oder Protokolle einsetzen. Die Verbindung zwischen den Geräten sollte immer verschlüsselt erfolgen. Weiterhin sollten nur aktuell sichere Verschlüsselungs- und Hashwertverfahren eingesetzt werden. Jeder Zugriff auf andere Geräte sollte nur authentifiziert erfolgen, um unberechtigten Zugriff zu erschweren. Hier kann beispielsweise eine PKI (Public Key Infrastructure) sinnvoll eingesetzt werden [KeeL15]. Von fest einprogrammierten Passwörtern oder Service-Zugängen ist grundsätzlich abzuraten, da es immer nur eine Frage der Zeit ist, bis diese bekannt werden. Letztendlich müssen sich die Hersteller auch Gedanken machen, wie eine einfache und dennoch zuverlässige Verteilung von Updates für IoT-Geräte erfolgen kann.

Literatur

[Asht09] K. Ashton: That 'Internet of Things' Thing, Online (2016), http://www.rfidjournal.com/articles/view?4986, (abgerufen am 28. März 2016).

[Harp03] R. Harper: Inside the Smart Home, Springer-Verlag London (2003).

[CHIP15] CHIP Test & Kaufberatung: Live-Stream aus dem Kinderzimmer – Babyphone mit Kamera: Systeme im Vergleich, Online (2016), http://www.chip.de/artikel/Babyphone-mit-Kamera-Systeme-im-Vergleich_80715236.html, (abgerufen am 28. März 2016).

[StBe15] M. Stanislav, T. Beardsley: HACKING IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities, Rapid7 Report (2015).

[FlWe14] E. Fleisch, M. Weinberg, F. Wortmann: Geschäftsmodelle im Internet der Dinge, Online (2014), http://www.iot-lab.ch/wp-content/uploads/2014/09/GM-im-IOT_Bosch-Lab-White-Paper.pdf, (abgerufen am 13.06.2016).

[Poru16] J. M. Porup: "Internet of Things" security is hilariously broken and getting worse, Online (2016), http://arstechnica.com/security/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies/, (abgerufen am 13.06.2016).

[Baby16] Babymoov: Babycamera 0% Emission, Online 2016, http://produkte.babymoov.de/baby-camera-0-emission.html#descriptifproduit, (abgerufen am 28. März 2016).

[Binw16] Binwalk: Firmware Analysis Tool, Online 2016. http://binwalk.org (abgerufen am 28. März 2016).

[Hash16] hashcat: advanced password recovery, Online 2016. http://hashcat.net/oclhashcat (abgerufen am 28. März 2016).

[Shod16] Shodan: The search engine fort the Internet of Things, Online 2016. https://www.shodan.io (abgerufen am 28. März 2016).

[KeeL15] Lila Kee: IT-Sicherheit 2016 – PKI wird zu der Sicherheitstechnologie im IoT-Markt, AP-Verlag, Online 2015, http://ap-verlag.de/it-sicherheit-2016-pki-wird-zu-der-allgegenwaertigen-sicherheitstechnologie-im-iot-markt/15467/, (abgerufen am 04. Juni 2016).